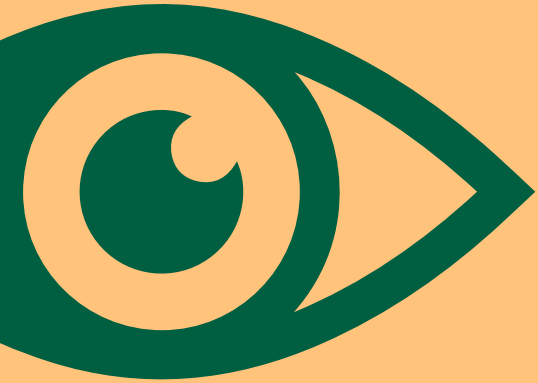
*Políticas públicas al derecho/* Editorial **Dejusticia**

# INTELIGENCIA ESTATAL EN INTERNET Y REDES SOCIALES: EL CASO COLOMBIANO



*Lucía Camacho Gutiérrez*
*Daniel Ospina Celis*
*Juan Carlos Upegui Mejía*

Dejusticia

# INTELIGENCIA ESTATAL EN INTERNET Y REDES SOCIALES: EL CASO COLOMBIANO

LUCÍA CAMACHO GUTIÉRREZ
DANIEL OSPINA CELIS
JUAN CARLOS UPEGUI MEJÍA

Financiado por Privacy International

*políticas públicas al derecho /* Editorial Dejusticia

Camacho Gutiérrez, Lucía.

Inteligencia estatal en internet y redes sociales: el caso colombiano / Lucía Camacho Gutiérrez, Daniel Ospina Celis, Juan Carlos Upegui Mejía. – Bogotá: Editorial Dejusticia, 2022.

56 páginas; 22 cm. – (Políticas públicas al derecho)
978-628-7517-58-5

1. Inteligencia 2. Internet 3. Redes sociales 4. Privacidad. I. Tít. II. Serie.

ISBN 978-628-7517-58-5 versión digital

Preparación editorial
Diego Alberto Valencia

Cubierta
Alejandro Ospina

Revisión de textos
María José Díaz Granados

Primera edición
Bogotá, D.C., Colombia, diciembre 2022

Este texto puede ser descargado gratuitamente en
https://www.dejusticia.org



Dejusticia
Calle 35 # 24-31, Bogotá, D.C., Colombia
Teléfono: (57) 601 608 3605
www.dejusticia.org

## Contenido

## Los Autores


### Lucía Camacho Gutiérrez

Abogada y máster en Derechos Humanos. Fellow del Media Democracy Fund en el Centro de Estudios de Derecho, Justicia y Sociedad - Dejusticia. Orcid: https://orcid.org/0000-0002-9831-0255

### Daniel Ospina Celis

Abogado y magíster en Historia de la Universidad de los Andes. Es investigador del Centro de Estudios de Derecho, Justicia y Sociedad - Dejusticia. Orcid: https://orcid.org/0000-0002-0688-9854

### Juan Carlos Upegui Mejía

Fue investigador del Centro de Estudios de Derecho, Justicia y Sociedad - Dejusticia. Es profesor de la Universidad Externado de Colombia. Orcid: https://orcid.org/0000-0002-4649-8217

## Introducción

VOLVER AL CONTENIDO

El Estado colombiano adelanta actividades de inteligencia en internet y en redes sociales. Por lo general, estas actividades pasan desapercibidas y es poco lo que conocemos sobre ellas. De vez en cuando, sin embargo, algunos casos salen a la luz pública. En 2020, la investigación periodística titulada "Las carpetas secretas", publicada por la revista *Semana*, reveló cómo algunas de las agencias de inteligencia del Estado habían empleado internet y las redes sociales para obtener información con el objetivo de perfilar a periodistas, opositores políticos del gobierno de turno y defensores de derechos humanos.

La inteligencia estatal, cuando se despliega como una actividad legítima, busca satisfacer al menos dos finalidades básicas: informar las políticas públicas en materia de seguridad, y apoyar la ejecución de las operaciones de inteligencia militar y policial dirigidas a la protección de la seguridad nacional y ciudadana (Bruneau y Boraz, 2007). Dado que las labores de inteligencia son fundamentales para los Estados, aspectos como la obtención rápida de información accionable y confiable permite llevar a cabo los objetivos que esta se propone y facilitar la toma de decisiones.

En Colombia, las actividades de inteligencia fueron reguladas a nivel legal en 2013 con la expedición de la Ley 1621. Según esta ley, los organismos especializados del Estado que desarrollan la función de inteligencia y contrainteligencia tienen como objetivo proteger los derechos humanos y prevenir las amenazas contra la vigencia del orden democrático (Ley 1621 de 2013, art. 2).

Para desarrollar esta función, los organismos de inteligencia acuden a distintas estrategias dirigidas a la recolección de información disponible en distintas fuentes, incluidas internet y las redes sociales. El despliegue de dichas actividades de recolección de información en línea no es reciente; según datos obtenidos en el curso de esta investigación, diversas agencias de inteligencia acuden a la consulta de fuentes abiertas de información en línea y redes sociales, de forma habitual y sistemática, al menos desde 2014 (en la Policía Nacional) y 2016 (en el Ejército Nacional).

Mientras los particulares que usan internet y redes sociales las emplean generalmente para comunicarse, estudiar, divertirse o buscar información, los organismos de inteligencia las emplean también para adelantar sus labores y, sobre todo, para recolectar información que permita apuntalar hipótesis de investigación a fin de identificar, contener y evitar posibles riesgos en contra de la seguridad. Internet y las redes sociales sirven, en ese sentido, como fuentes o entornos de fácil acceso y consulta de información, especialmente información personal, considerada de interés en materia de inteligencia.

El volumen de la información accesible en fuentes abiertas en internet crece de forma exponencial cada día. A su vez, la información personal que circula en las redes sociales permite conocer, con un especial nivel de detalle, datos sobre el círculo social, las actividades, los gustos y los lugares más frecuentados por las personas declaradas como objetivos de inteligencia. Actualmente, su uso constituye una de las modalidades de acceso a la información estratégica más atractivas y económicas para los Estados (Akghar, 2016; Marzell, 2016; Steele, 2007; Hassan, 2019).

La inteligencia en internet es un subtipo de la inteligencia en fuentes abiertas que consiste en la consulta, el acceso y el uso de información (gratuita o bajo pago) disponible en línea, y que no está restringida por leyes de privacidad o derechos de autor. Aquella información es recogida, procesada, analizada e interpretada en aras de dirigir la acción estatal en materia de seguridad nacional y ciudadana (Akghar, 2016; Gibson, 2016; Miller, 2018).

Por su parte, la inteligencia en redes sociales es una tipología de la inteligencia en línea que sucede exclusivamente en las plataformas que facilitan la interacción bidireccional y pública de las personas que, para tal efecto, publican constantemente información personal sobre sí mismas, lo que piensan, con quiénes se relacionan y lo que hacen, en tiempo real. Su acceso y uso en materia de inteligencia cobran valor en tanto que aportan a los esfuerzos de identificación de personas y grupos de interés, a la prevención de eventos de riesgo y al monitoreo de temas y situaciones relevantes en materia de seguridad (Omand *et al*., 2012; Omand, 2017).

Sin embargo, los problemas éticos y jurídicos en torno al acceso y uso de la información personal disponible en línea, en el caso colombiano, no han sido suficientemente estudiados hasta ahora. El propósito de esta investigación es aportar insumos para el diagnóstico y el abordaje de algunos de estos problemas, en especial, el relacionado con la visión compartida por algunas agencias de inteligencia colombianas según la cual, la información que es accesible en internet y en redes sociales, por el solo hecho de estar disponible en estos medios, puede ser usada sin límites ni restricciones en el contexto de las actividades de inteligencia.

No desconocemos que el uso de información disponible en internet o en las redes sociales puede tener un gran valor para la ciudadanía e incluso para el Estado bajo condiciones claras y situaciones específicas. Un uso legítimo y benéfico de dicha información es el que se da fruto del periodismo de investigación que busca nutrir los debates públicos u ofrecer evidencia que da cuenta de violaciones de los derechos humanos; o el uso de dicha información por los Estados puede resultar legítimo en aras de prevenir atentados terroristas, desarticular redes de trata de personas o prevenir la explotación y el abuso infantil.

Desde luego, existe una diferencia entre las tareas de investigación con fines académicos o periodísticos y las actividades de inteligencia estatal. Mientras que la tarea de investigación dirigida al estudio, escrutinio o control al ejercicio del poder debe ser compatible con los derechos de terceros, las segundas

deben, además, ajustarse al principio de legalidad, necesidad y proporcionalidad. Los servidores públicos y el Estado solo pueden ir tan lejos como lo permita la ley, en el marco de sus competencias y funciones legales. La vocación de estos principios es fijar límites necesarios para el actuar estatal a fin de evitar que el despliegue de una actividad con un alto potencial de incidencia en los derechos fundamentales se torne en una fuente de abusos.

Pensar en los límites a la inteligencia estatal, desplegada ahora en la internet y en las redes sociales, debe empezar por disolver la narrativa según la cual la posibilidad de encontrar y acceder a información personal en línea permite a los cuerpos de inteligencia hacer con ella prácticamente cualquier cosa. La información disponible en línea no pierde, por su publicación, su naturaleza de información personal privada o sensible. Por tal motivo, si se quiere consultar, procesar y almacenar dicha información se debe, entre otras cosas, seguir las normas que protegen la privacidad y los principios de la legislación concerniente al tratamiento de datos personales.

Para el desarrollo de esta investigación, que apunta a explorar los límites a la actividad estatal, empleamos diversas fuentes oficiales (leyes, decretos, resoluciones, decisiones de la Corte Constitucional, entre otras) y no oficiales (consulta de medios de comunicación, literatura sobre inteligencia en internet y redes sociales), y realizamos entrevistas a expertos que han sido asesores de algunos cuerpos de inteligencia, y con expertos en periodismo de investigación, cuya identidad hemos prometido preservar. Queremos agradecer su disposición y generosidad en los encuentros con nuestro equipo. En este punto también queremos indicar la especial dificultad para lograr las entrevistas. A pesar de que contactamos a una docena de expertos, solo el 20% de los contactados aceptó conceder entrevista y conversar con el equipo de investigación.

En el relevamiento de fuentes oficiales también elevamos una docena de solicitudes de acceso a la información a diversas agencias de inteligencia del Estado, con el objetivo de indagar sobre la incidencia del uso de internet y de las redes sociales en el ejercicio de sus funciones. Sobre este último punto, no que-

remos dejar de resaltar que algunas de las entidades indagadas aplicaron la Ley 1712 de 2014, sobre acceso a la información pública, y nos facilitaron valiosa información para la construcción de este informe. Aun cuando se trata de un avance en materia de transparencia en temas que, en el pasado, eran evacuados con respuestas desestimatorias sin mayores explicaciones, creemos que todavía queda un largo camino por recorrer.

El pleno acceso a la información sobre los aspectos básicos y generales de la inteligencia en fuentes abiertas y en redes sociales sigue siendo una tarea pendiente. Esto se ilustra, por ejemplo, con la oposición a la reserva sobre un mismo asunto, que resultó invocada de manera disímil por las diferentes autoridades que integran la comunidad de inteligencia, lo que genera dudas sobre la apropiación y correcta aplicación de la Ley de Acceso a la Información.

Desde luego, la inaplicación heterogénea de la ley obró a favor de nuestra investigación, pero creemos que si una entidad puede entregar información sobre un asunto acerca del cual otras alegan reserva, la reserva aplicada quizá podría levantarse para el resto, en atención al principio según el cual, en caso de dudas, debe preferirse la transparencia por encima de la reserva.

En este contexto, la presente investigación se desarrolla en cuatro partes. En la primera parte, retomamos el caso de "Las carpetas secretas" para ilustrar la narrativa detrás de las actividades de inteligencia en internet y en redes sociales en Colombia. En la segunda parte, describimos brevemente la regulación de las labores de inteligencia estatal en Colombia, con un énfasis en el marco normativo aplicable a la inteligencia en línea. En la tercera parte, mostramos los hallazgos sobre los límites que dicen aplicar algunas agencias de inteligencia, los problemas de vaguedad que existen en la materia, así como la posición que mantienen sobre el carácter de la información que obtienen a partir de actividades de inteligencia en internet y en las redes sociales. Por último, exponemos nuestra propuesta y formulamos algunas recomendaciones de política pública, a partir de una articulación entre los valores en juego: la garantía de la seguridad nacional y la vigencia del orden constitucional y democrático,

por un lado, y el respeto por los derechos fundamentales, incluido el de privacidad y protección de datos, por el otro.

## 1. Inteligencia en internet y redes sociales. El caso "Las carpetas secretas"

La investigación titulada "Las carpetas secretas" fue publicada en 2020 por la revista *Semana*. En esta investigación se describe cómo el Ejército Nacional recolectó información personal de más de 130 personas, entre periodistas, defensores de derechos humanos, miembros de sindicatos y congresistas, con el fin de crear perfiles detallados de cada una.

VOLVER AL CONTENIDO

La información recogida fue obtenida a través de diversos medios, incluida internet y las redes sociales. Según *Semana*, la creación de estos perfiles y el análisis de la información no seguía ningún fin legítimo, especialmente porque declarar a las personas como objetivos de las actividades de inteligencia en razón de su afiliación política, el trabajo en la defensa de los derechos humanos o su labor periodística resulta, cuando menos, discriminatorio.

Pero este caso va más allá de lo cuestionable en torno a los criterios de selección de los objetivos de inteligencia. Tal y como mostró la investigación de *Semana*, uno de los periodistas de quien se creó un perfil de inteligencia es corresponsal del *New York Times*. Gracias a sus publicaciones en Twitter se extrajo información relacionada con su actividad en línea, se determinó quiénes eran sus seguidores y de qué países lo seguían, cuál era su círculo social estrecho y con quiénes había interactuado de forma frecuente. De hecho, los investigadores de inteligencia también escarbaron en las publicaciones en redes sociales de algunos de sus seguidores.

Otra de las víctimas del perfilamiento ilegal fue una fotoperiodista, sobre quien el Ejército obtuvo grandes cantidades de información personal. Se recogió información sobre su actividad en Facebook, sus contactos más cercanos de la red social, y se elaboró un perfil de cada uno de acuerdo con lo que habían publicado en dicha plataforma. Asimismo, de su cuenta en Ins-

tagram se obtuvo la información de su geolocalización asociada a cada una de las fotos publicadas por ella en su red social.

*Semana* también destaca el caso de una periodista colombiana de quien se obtuvo su número único de identificación nacional (cédula de ciudadanía), lo que permitió consultar bases de datos públicas y accesibles por internet. Entre las bases de datos consultadas se encuentran las del lugar de votación, propiedad de vehículos e infracciones de tránsito, que dan cuenta de su lugar de domicilio, vehículos a su nombre y trayectos transitados.

Por su parte, algunas de las agencias de inteligencia y expertos que dieron su opinión para *Semana* sobre este caso sostuvieron:

> Algunos de los responsables directos, entre coroneles y generales, han tratado de justificar los perfiles argumentando que se trata de datos obtenidos por fuentes abiertas y redes sociales. (Semana, 2020a)

> Ellos [los militares] van a tratar de salirse por las ramas argumentando que la información recopilada de fuentes abiertas como tal no es inteligencia. El problema con eso es que el producto final, es decir, los informes que se hacen con base en esos datos, sí son inteligencia y tienen un fin específico, que en este caso no es claro. (Alto funcionario de la Dirección Nacional de Inteligencia entrevistado por la revista *Semana*, 2020a)

*El País*, otro medio que indagó en la opinión de expertos en seguridad sobre la obtención de información disponible en internet y redes sociales por parte del Ejército con la intención de perfilar a un grupo determinado de personas dijo que: "Todos esos datos están en fuentes abiertas de las redes sociales, por lo que "eso no es espionaje, no son 'chuzadas'. Seguimiento es cuando usted va detrás de la persona" (El País, 2020).

La constante en los tres casos relatados revela una posición de base que es problemática: el tratamiento de la información disponible en internet y en redes sociales, debido a su publicación y fácil acceso, no está sometido a límites jurídicos; dicha información es considerada, de hecho, pública y de libre acceso y consulta.

Como la información disponible en internet circula libremente, se podría pensar que su acceso y uso por las agencias de inteligencia no es susceptible de ser considerado una actividad de inteligencia propiamente dicha. Si cualquier persona puede acceder a esta información y utilizarla para distintos fines, su acceso es público. ¿Cuál es el problema de que las agencias de inteligencia accedan a información en internet y en redes sociales? ¿Por qué tendríamos que considerar que esta actividad está sujeta a límites jurídicos, incluso si es realizada por las agencias de inteligencia del Estado?

VOLVER AL CONTENIDO

## 2. Regulación de la inteligencia (en línea)

Las preguntas que suscita la exposición de los casos recogidos en la investigación "Las carpetas secretas", esto es, las que tienen que ver con el carácter aparentemente libre o discrecional de toda actividad relacionada con la recolección y el tratamiento de información disponible en fuentes abiertas, en especial en internet, nos llevan a su vez a preguntarnos por la regulación de las actividades de inteligencia cuando estas se adelantan ahora y de forma cada vez más intensa en los escenarios digitales: la internet y las redes sociales.

¿Cuál es la regulación sobre el tratamiento de la información, y en especial de la información personal, disponible en internet y en redes sociales a propósito de las tareas de inteligencia?, ¿cuáles (si los hay) son los límites aplicables?, ¿es cierto que existe una total discrecionalidad por parte de las agencias de inteligencia del Estado para recolectar, tratar y usar la información personal disponible en internet?

La legislación colombiana no ofrece respuestas categóricas. La regulación existente es escueta y parece no haber tenido en cuenta la potencialidad, la complejidad y los riesgos de la recolección y el tratamiento de información a partir de fuentes abiertas en internet y en redes sociales. A este déficit regulatorio se suma una suerte de delegación de la regulación de la actividad a las propias agencias de inteligencia, sin que existan criterios comunes y claros. Veamos.

## Regulación de inteligencia y "medios" de inteligencia

La Ley Estatutaria 1621 de 2013, de Inteligencia y Contrainteligencia, fue impulsada en su momento para ordenar una actividad con un largo historial de abusos en el contexto colombiano; hasta entonces, estas actividades se habían adelantado sin un marco jurídico claro y con un alto nivel de discrecionalidad por parte de todos los gobiernos colombianos. Esta ley viene a corregir esta falencia y configura, a partir de su expedición, la base normativa de la actividad de inteligencia que llevan a cabo distintos organismos especializados.

En Colombia, la inteligencia es una actividad que ejecutan distintas agencias de forma compartimentada, bajo el amparo de un marco legal de base. En el listado de entidades o agencias de inteligencia se encuentran:

- → Las Fuerzas Militares (Ejército Nacional; Armada Nacional; Fuerza Aérea).
- → La Policía Nacional.
- → La Dirección Nacional de Inteligencia (DNI).
- → La Unidad de Información y Análisis Financiero (UIAF).

Este grupo de entidades conforman la "comunidad de inteligencia"; las autoridades que conforman dicha comunidad tienen facultades para adelantar operaciones o misiones de inteligencia en internet y en las redes sociales. En 2011, por ejemplo, se facultó a la DNI a recolectar información a través de "medios técnicos [y] medios abiertos" de información. Y en 2013, la Ley Estatutaria 1621 concedió la misma facultad al resto de la comunidad de inteligencia (Decreto 4179, 2011; Ley 1621, 2013). La legislación en la materia considera que la internet y las redes sociales son "medios de inteligencia".

Sin embargo, la disposición que habilita el uso de estos "medios" no viene acompañada de ninguna definición sobre su alcance y su extensión. Gracias a diversas solicitudes de acceso a la información que remitimos a las agencias de inteligencia a propósito de esta investigación, sabemos que en la categoría

de "medio abierto" y "medio técnico", tanto la Policía Nacional como la DNI incluyen a internet y las redes sociales.[1]

Ahora bien, la Ley de Inteligencia prevé como límites al uso de medios técnicos y abiertos la aplicación de los principios de idoneidad y de proporcionalidad, así como el cumplimiento del Plan Nacional de Inteligencia.

El principio de idoneidad prevé que los medios de inteligencia que sean empleados deben permitir la realización de los fines de inteligencia que consagra la Ley 1621 de 2013 (asegurar el cumplimiento de los fines del Estado, garantizar la seguridad nacional, la vigencia del orden constitucional y la protección de los derechos fundamentales); y el principio de proporcionalidad apunta a que los beneficios obtenidos de los medios de inteligencia sean mayores a las restricciones que pesan sobre otros "principios y valores constitucionales". Y, por supuesto, se acude a la expresión de garantizar el cumplimiento de la Constitución y la ley.

Un límite interno de tipo operativo a las actividades de inteligencia en "medios técnicos y abiertos" es el Plan Nacional de Inteligencia. Su contenido es reservado, pero en él se fijan cuáles son, según el Gobierno nacional, los riesgos, las amenazas y prioridades de inteligencia; los límites y fines que debe satisfacer dicha actividad; los responsables de su ejecución, entre otros (Ley 1621; Decreto 1070).

De tal manera, operaciones o misiones de inteligencia para, por ejemplo, desarticular bandas criminales, tuvieron que haber sido previstas, por regla general, como requerimientos de inteligencia en el Plan Nacional de Inteligencia para que se puedan llevar a cabo.

La orden de una operación o misión de inteligencia debe corresponderse con las prioridades y necesidades fijadas por el Gobierno nacional. Esto funciona como un límite a la improvisación de las operaciones de inteligencia que, aun cuando puedan llegar a parecer idóneas y proporcionales, solo pueden tener lugar si han sido planificadas.

Pese a su importancia, el Plan Nacional de Inteligencia no

1 Ver respuestas con radicado número DIPOL-ASJD-13, 10 de junio de 2022; y radicado 2-2022-139C, 14 de junio de 2022.

tiene el papel de prever los medios de inteligencia que serán empleados, cuya elección y despliegue compete, en esencia, a quienes elevan requerimientos de inteligencia puntuales, autorizan las operaciones de inteligencia y a quienes las ejecutan.

## El escalón siguiente: los manuales y protocolos de inteligencia

Sobre la definición de los límites concretos a las actividades de inteligencia en medios técnicos y abiertos las disposiciones de la Ley 1621 de 2013 son muy generales, son límites de principio. El detalle sobre su contenido, en todo caso, queda en manos de las agencias de inteligencia. Esta facultad está comprendida en la competencia para expedir sus propios manuales y protocolos, lo que a su vez incluye la posibilidad de precisar los límites aplicables a la explotación de medios como la internet y las redes sociales.

Este diseño institucional, de entrada, significa que la regulación sobre la recolección y el tratamiento de la información disponible en internet y en redes sociales puede ser tan numerosa y diversa como las agencias que integran la comunidad de inteligencia.

La Ley de Inteligencia y el Decreto 857 de 2014 previeron que los manuales y protocolos deben observar la Constitución y la ley, pero el carácter reservado de su contenido impide entender cómo se traduce dicha observancia en el plano jurídico, o en la adopción de límites de tipo metodológico o tecnológico.

Es más, ni siquiera los manuales de inteligencia disponibles en internet son lo suficientemente explícitos sobre cuáles son los límites de su actividad, en especial cuando se trata de "medios técnicos y abiertos" como la internet y las redes sociales. Un ejemplo de esto son los manuales de Inteligencia de la Policía Nacional y del Ejército Nacional.

El contenido de ambos manuales prevé la posibilidad de emplear la internet para adelantar actividades de inteligencia. Sin embargo, ninguno detalla los límites jurídicos de la actividad, a partir de una consideración de los aspectos técnicos y legales de internet y de las redes sociales. Nos preguntamos,

entonces, ¿qué protección o salvaguarda conceden, por ejemplo, a las interacciones en línea que suceden en grupos privados de una red social, o que están protegidas por ajustes de privacidad? ¿Qué información personal está excluida, o debe ser excluida, de ser consultada o accedida durante la ejecución de actividades de inteligencia? Los manuales no abordan este tipo de preguntas. En el punto se limitan a señalar que se respetará la Constitución y la ley.

El Manual Fundamental de Inteligencia del Ejército Nacional, que data de 2016, y que por diferentes vías a la de la página oficial de la entidad está disponible en internet, no tiene disposiciones específicas sobre las actividades de recolección y tratamiento de información con fines de inteligencia en línea y en las redes sociales. El manual y su actualización se limitan a prever el uso de las fuentes abiertas de inteligencia (OSINT) junto a otras fuentes que, en su conjunto, son necesarias "para ayudar a la comprensión de la situación, apoyar el desarrollo de planes y órdenes y responder a los requerimientos de información" (Resolución 01886 de 2016; Resolución 01869 de 2017).

En efecto, el manual del Ejército Nacional no menciona ningún límite asociado al despliegue de actividades de inteligencia en internet o en redes sociales, pese a estar dirigido a los funcionarios de inteligencia en formación. Un dato no menor tiene que ver con la ausencia de referencia a las redes sociales como medio-fuente de información de inteligencia, máxime si ya existe evidencia de que estas ya han sido empleadas por el Ejército Nacional, como fue revelado en el caso de "Las carpetas secretas". Esta situación nos lleva a preguntarnos si se acude a otras fuentes de información no previstas por el manual, si dicha institución establece o no alguna diferencia entre las redes sociales del resto de la internet, y si las diferencias entre una y otra deberían ser objeto de especial consideración de cara a las tareas de inteligencia.

A estas particularidades regulatorias hay que sumar que el legislador, al expedir la Ley General de Protección de Datos, decidió excluir de su ámbito de aplicación las actividades de inteligencia y contrainteligencia (Ley 1581, art. 2). Que se hubiese

excluido no significa, sin embargo, que no debiera existir para el caso una regulación especial. Por su parte, la Ley de Inteligencia, expedida un año después, en 2013, guardó silencio sobre el punto.

Aunque las bases de datos con información de inteligencia y contrainteligencia se encuentren excluidas de la aplicación de la Ley de Protección de Datos Personales, a estas les son aplicables los principios generales del tratamiento de datos (Ley 1581, art. 2).

Desde luego, se trata tan solo de algunos de esos principios, pues en tanto que la inteligencia no es una actividad consentida por el titular de los datos, la persona afectada no podría oponerse a la recolección de su información personal, por lo que el principio de libertad quedaría por fuera de la discusión. Sin embargo, a la fecha no se ha precisado por la legislación ni la jurisprudencia constitucional cómo serían operacionalizados los otros principios, como el de acceso y circulación restringida de la información, o el de transparencia, veracidad o calidad de esta, y con qué extensión podría la persona afectada ejercer los derechos de control sobre su información y los que habilita el derecho de *habeas data*.

***

Las actividades estatales de inteligencia que tienen el efecto neto de intervenir en la privacidad en línea demandan límites claros. Se trata de labores que por definición persiguen la extracción de información del medio original en el que fue publicada, que resulta siendo usada sin conocimiento, para fines no previstos por su titular, y que es agregada junto a otras fuentes públicas (como las bases de datos que produce y que pertenecen al Estado) y privadas de información. Se trata de información que permite perfilar a las personas y que habilita la construcción o la demostración de hipótesis con un alto potencial de afectarlas o perjudicarlas.

La pretensión de lograr la fijación de estos límites librada, en el caso colombiano, a la redacción de los manuales y protocolos por parte de cada agencia de inteligencia, es también insu-

ficiente. En especial, por dos razones: porque no existen reglas comunes, más precisas, a las que deban adecuarse los procedimientos así regulados, y porque la idea de favorecer una posible autorregulación riñe con los sesgos de la actividad y con la inercia institucional del Estado colombiano de adelantar estas actividades sin límites jurídicos ni controles externos.

Por último, la definición de estos límites tiene el reto de precisar cuál es, o cuál debería ser, el alcance de la expectativa de privacidad en las redes sociales y, en general, en internet. Máxime si la inteligencia es, por sí misma, una actividad que prescinde en su despliegue del consentimiento de las personas; se adelanta, por definición, sin conocimiento de la persona, y su naturaleza, métodos y procedimientos impiden a estas ejercer algún mecanismo administrativo para controlar la información que se recolecta sobre ellas.

VOLVER AL CONTENIDO

## 3. Prácticas de las agencias de inteligencia

El Estado colombiano recolecta información con fines de inteligencia en internet, de forma rutinaria y sistemática, desde hace más de un lustro. Las agencias de inteligencia y los expertos consultados reconocen que es una práctica usual. A pesar de que el marco regulatorio básico sobre las actividades de inteligencia coincide en el tiempo con el inicio formal y sostenido de estas prácticas, dicho marco no es específico ni exhaustivo en relación con las particularidades de adelantar actividades de inteligencia en internet y en redes sociales.

Esta ausencia de criterios normativos a nivel general se intentó suplir de facto mediante la facultad que la propia ley le reconoce a las autoridades de inteligencia para expedir sus manuales operacionales. Lo que permite una especie de autorregulación, en los planos técnico y operativo, respecto al uso de medios y prácticas para la concreción de sus funciones legales y constitucionales de proteger la seguridad y la defensa nacional.

La identificación de estas prácticas y su reconocimiento, como lo advertimos en las respuestas a las solicitudes de infor-

mación que elevamos, parece funcionar como sustituto de la regulación. Aun así, la conclusión no cambia, los límites siguen siendo vagos, lo que se presta para que el desarrollo de estas actividades esté caracterizado por altos niveles de arbitrariedad.

En esta sección exploramos el porqué y para qué de la inteligencia en internet y redes sociales, y los límites que dicen aplicar en su tarea algunas de las agencias de inteligencia. Asimismo, presentamos la información sobre cómo capacitan a su personal para su correcta aplicación, y cuál es la información de inteligencia que buscan obtener de internet y las redes sociales.

Veremos que los límites propios son vagos, y que los procesos de capacitación parecen reiterar fórmulas abstractas sobre el apego a la ley, que poco orientan la actividad y poco sirven para evitar la intromisión injustificada en la vida privada como, por ejemplo, si es posible o no extraer información de inteligencia de grupos o cuentas privadas de las redes sociales, o si la información personal contenida en las bases de datos públicas del Estado puede ser usada con fines de inteligencia, una finalidad claramente no prevista ni advertida a la ciudadanía al momento de su creación.

También veremos que, en comparación con la vaguedad de los límites, parece existir una mayor certeza sobre qué información en línea resulta de interés para la inteligencia estatal. Sin embargo, no hay evidencia sobre prácticas especiales de clasificación o de tratamiento diferenciado de la información personal pública, privada o sensible obtenida de internet y las redes sociales. Esto último es diciente sobre el estado de las discusiones acerca de la privacidad y el tratamiento de datos personales por parte de las agencias de inteligencia.

## Razones y propósitos de la inteligencia en internet y en redes sociales

Según nuestros entrevistados, la inteligencia en internet y redes sociales permite ilustrar el contexto para la realización de este tipo de operaciones. El contexto hace parte de la primera fase del ciclo de inteligencia: la planificación. Esto facilita la delimitación de esfuerzos de las fases siguientes destinadas a

la recolección, el almacenamiento, procesamiento y análisis de la información obtenida. Uno de los entrevistados sostiene que "sin contexto no se puede enriquecer dicha tarea".

La información de contexto obtenida en internet y las redes sociales está dirigida a responder preguntas básicas pero determinantes en relación con una persona: quién es esta persona, con quién se relaciona, cuál es la intensidad de sus vínculos, qué ha hecho y a qué se dedica, cuál es su trayectoria, en qué círculos ejerce influencia, qué sabe, etc. Esto, a su vez, permite avanzar en hipótesis más concretas: qué relación puede existir entre esta persona y eventos críticos en materia de seguridad ciudadana, seguridad nacional o defensa nacional. Antes de internet, dicha información era obtenida de las fuentes abiertas y públicas en sentido tradicional, es decir, la prensa escrita, la radio, la televisión, revistas académicas, libros impresos y la literatura gris (la transcripción y traducción de eventos, entre otros). O a través de fuentes secretas o encubiertas, mucho más costosas y riesgosas en comparación con la obtención de información disponible en línea.

Como sostiene uno de los expertos entrevistados, gracias a la masificación de la red y la digitalización de la mayoría de las fuentes públicas y abiertas tradicionales "se podría decir que un 80% de la inteligencia [en Colombia] hoy día se obtiene en línea". Distintos autores coinciden con ese diagnóstico respecto de otros países (Steele, 2007; Pallaris, 2008; Marzell, 2016). Pero no solo es una de las primeras fuentes de consulta en materia de inteligencia, incluso la ausencia de información en línea sobre una persona de interés, por ejemplo, podría llegar a constituir un motivo de sospecha pues "todos, queramos o no, tenemos una huella digital en internet", afirma el mismo entrevistado.

Aun cuando los entrevistados no tienen certeza sobre cómo se lleva a cabo dicha tarea por las agencias de inteligencia en Colombia, es decir, si se hace de manera manual o a través del uso de ciertas tecnologías (a través del uso de la API de las redes sociales, del rastrillado automatizado en la web o *scraping*, etc.), coinciden en que su empleo en la actualidad trasciende a los intereses y actores en materia de protección de la seguridad

y la defensa nacional. Es decir, la explotación de internet y las redes sociales se emplea también para la investigación criminal o "ciberpatrullaje", así como en el marco de estrategias de comunicación estatal.

De hecho, dos de los entrevistados afirman que funcionarios del gobierno buscan, a través de la obtención de información disponible, especialmente en las redes sociales, mapear cuáles son los temas y actores que participan en la discusión pública. Se trata de esfuerzos enmarcados en las estrategias de comunicación cuyo objetivo es, entre otros, medir el posible éxito de ciertas decisiones de política pública o incluso mejorar las estrategias de comunicación del gobierno, para elevar sus niveles de aprobación.[2] Es decir, una actividad que despliegan ciertos gobiernos, aun cuando no se trate de una actividad del Estado.

En este contexto, merece especial mención el contrato celebrado entre el Departamento Administrativo de la Presidencia y la firma Du Brands S.A.S. Dicho contrato estuvo dirigido a la "creación de estrategias de comunicaciones para la divulgación en medios, la producción de contenidos y la administración de los canales digitales de Duque y de la presidencia". Entre las estrategias desplegadas por la empresa contratista se llevó a cabo "la parametrización de usuarios de redes sociales [y] el monitoreo de medios de comunicación" (Fundación para la Libertad de Prensa, 2020, p. 38).

Las tareas desplegadas en redes sociales por Du Brands, así como las que llevan a cabo las agencias de inteligencia, comparten elementos comunes: el monitoreo de la actividad en línea para perfilar a un grupo de personas, lo cual incluye en ambos casos la identificación de su círculo de seguidores en una red social determinada. En ambas tareas, las redes de contactos responden a la pregunta *quién es quién* en razón de su opinión

2 En su investigación sobre el Reino Unido, Privacy International (2020) da cuenta del uso de la inteligencia en redes sociales por el Estado para apoyar la toma de decisiones en los servicios sociales de la infancia, el monitoreo de la protesta social, la recuperación de los impuestos impagos, la detección de publicidad de bienes ilegales, para confirmar la veracidad de la información provista por solicitantes de beneficios sociales, entre otros.

acerca del gobierno (caso Du Brands), o en razón del riesgo que representa para la seguridad (caso de la inteligencia).

En ambas tareas, los datos públicos, privados (y sensibles, como los que dan cuenta de la postura política) son obtenidos de internet y las redes sociales sin el consentimiento, conocimiento ni autorización de quien decidió, en un principio, publicarlos libremente en razón del ejercicio de su derecho a la libertad de expresión y opinión. La expectativa de privacidad de la persona que decide publicar información personal es, en ese caso, la de interactuar en un foro público, no la de ser objeto del monitoreo y perfilamiento por parte del gobierno de turno.

De hecho, uno de los tuiteros calificados como "negativo" por Du Brands, debido a su postura crítica frente al gobierno, interpuso una acción de tutela para proteger su derecho a la intimidad y al *habeas data*. El caso fue resuelto por la Corte Suprema de Justicia que reconoció que la información sensible publicada en Twitter por su titular, en ejercicio del derecho a la libre opinión en internet, no puede ser empleada en actividades de tratamiento de datos que este no ha consentido de manera libre y previa. La publicación y fácil acceso de los datos sensibles no constituyen un permiso para que terceros, como el gobierno, puedan usarla de forma indiscriminada para fines tales como mejorar la imagen pública del mandatario del Ejecutivo (Corte Suprema de Justicia, 2020).

En este caso, uno de los expertos consultados insiste en la importancia de distinguir las actividades de inteligencia de las actividades de investigación en internet y redes sociales, de cara a regular el tratamiento de la información personal. La información personal recogida y tratada en el marco de actividades de inteligencia es sometida al ciclo de inteligencia, y está destinada a ser consumida por los altos mandos del sector para orientar procesos de toma de decisiones en materia de seguridad. Estas actividades serían muy diferentes a las relacionadas con la investigación periodística o con empresas de *marketing* político o comercial, como las adelantadas por Du Brands en el contrato ya referido.

En materia de inteligencia en internet y redes sociales, los entrevistados destacan la importancia de activar la discusión so-

bre los límites aplicables a la inteligencia estatal. Se requiere de mayor precisión sobre el objetivo que persigue; los límites aplicables en la recogida de información pública, privada y sensible disponible en línea; así como las tareas subsiguientes de almacenamiento y tratamiento de esta. Estos son aspectos que, de hecho, emergen como prioridades en las siguientes secciones .

## Prácticas sin límites claros

La Dirección de Inteligencia de la Policía Nacional (Dipol) afirma, de forma explícita, no distinguir entre el entorno físico y el entorno digital cuando se trata de recoger información con fines de inteligencia. Para esta entidad, las actividades de inteligencia en internet y en redes sociales comparten el mismo propósito en el mundo análogo: identificar "fenómenos y amenazas, que puedan atentar contra los valores constitucionales del régimen constitucional y legal, régimen democrático y la seguridad y defensa nacional".[3] Estas actividades "son realizadas regularmente", su uso depende de "las condiciones que en cada caso se presenten",[4] lo que impide determinar si la consulta de fuentes abiertas supera a la consulta de otras fuentes de información. Una situación similar es predicable de la DNI, que afirma realizar actividades de inteligencia en internet y en redes sociales en aras de cumplir sus funciones legales y constitucionales.[5]

Tanto la DNI como la Dipol repiten el mantra del respeto a la Constitución y la ley. En las respuestas a nuestras solicitudes de acceso a la información, la Dipol dice cumplir con los principios de idoneidad, necesidad y proporcionalidad, así como las prioridades que se encuentran en el Plan Nacional de Inteligencia y los límites de la actividad que prevén las órdenes o las misiones de trabajo.[6] La DNI, por su parte, afirma no tener linea-

3 Ver radicado GS-2022/DIPOL-ASJUD-13, 10 de junio de 2022, p. 4.

4 Ver radicado GS-2022-028515/DIPOL-ASJUD-13, 05 de septiembre de 2022.

5 Ver radicado 2-2022-139C, 14 de junio de 2022, p. 2.

6 Ver radicado DIPOL-ASJUD-13, 10 de junio de 2022, p. 3.

mientos internos para el despliegue de la inteligencia en fuentes abiertas y redes sociales.[7]

Ambas agencias de inteligencia[8] señalan el rol de los Centros de Protección de Datos (CPD) presentes en todas las agencias de inteligencia, y que tienen a su cargo la curaduría de la información de inteligencia que es recolectada en el despliegue de dicha tarea. Los CPD se encargan de tres tareas: i) verificar que los procesos de recolección, almacenamiento y procesamiento de la información de inteligencia sean compatibles con la ley; ii) de garantizar la exclusión de la información que fue recogida pero que no es compatible con la ley; iii) garantizar que el almacenamiento de la información de inteligencia atienda criterios de neutralidad y no discriminación.

Su misión es esencial, sin duda, pero su alcance es limitado. Su régimen legal no permite a la persona afectada el acceso a la información que la individualiza y que fue recogida con fines de inteligencia; tampoco permite elevar solicitudes de rectificación de información personal, privada o sensible que fuese imprecisa, desactualizada o errónea; mucho menos solicitar la eliminación o depuración de los archivos de inteligencia en que consta información suya que fue recogida sin atender el principio de legalidad o que ya cumplió su ciclo y utilidad.

### Capacitación de los agentes de inteligencia

Otro punto clave para la exploración de las prácticas es el relacionado con el entrenamiento y la capacitación del personal de inteligencia. La capacitación es fundamental para el éxito de la actividad, pero también para su corrección. Aquella es obligatoria según la Ley 1621 de 2013, pues concreta dos roles críticos: i) instruir sobre el cómo se llevan a cabo las tareas de inteligencia, y ii) instruir sobre los límites que definen la corrección y la legalidad de la actividad.

La información sobre el desarrollo de capacidades permi-

7 Ver radicado 2-2022-139C, 14 de junio de 2022.

8 Ver radicados 2-2022-2113, p. 2; GS-2022-028515/DIPOL-ASJUD-13, 05 de septiembre de 2022, p. 2.

te saber, además, cómo procuran en verdad cumplir con lo prescrito por la Constitución y la ley, más aún cuando en su rol de investigadores ejecutan una actividad que no está sujeta al control, la revisión ni la auditoría externas –al menos no de naturaleza preventiva–.

A pesar de que la Escuela de Inteligencia y Contrainteligencia de la Dipol no cuenta con seminarios dedicados a la inteligencia en internet y redes sociales "ello no quiere decir que la recolección de información en fuentes abiertas o redes sociales no sea objeto de estudio, pues se halla implícito como una de las fuentes de información [que se estudia] en el componente de recolección".[9]

La Dipol adjuntó a sus respuestas un par de lecturas de sus talleres de capacitación. La primera sobre "la función de inteligencia y contrainteligencia en el Estado colombiano" y la segunda sobre "límites de la función de inteligencia y contrainteligencia, fines, principios y controles".[10]

La segunda lectura es exhaustiva en el recorrido de la jurisprudencia constitucional y la regulación vigente en materia de inteligencia. Menciona la importancia de aplicar los principios de idoneidad y proporcionalidad, mas no cómo debe hacerse en la práctica. Reitera el rol de la protección de la privacidad de las personas, pero no especifica qué pasos o precauciones deben ser desplegadas en su protección.[11]

Es decir, no se trata de verdadera pedagogía sobre los límites aplicables, sino de la reiteración de fórmulas valiosas pero vagas que, en todo caso, no se explican si se considera que, tratándose del desarrollo de habilidades en la ejecución de una tarea concreta, el contenido de los talleres de capacitación debe ser tan preciso y puntual como sea posible.

La DNI, por su parte, cuenta con un ciclo de formación denominado "Fuentes abiertas" que se dicta aproximadamente

9 Ver radicado GS-2022-001408/DIREC-GUSAP-29.25, p. 4.

10 Ver radicado 2-2022-2113, pp. 12 y ss.

11 Ver radicado 2-2022-2113, pp. 12 y ss.

cuatro veces al año, pero sus contenidos, estrategias didácticas y proceso de evaluación son reservados.[12]

## Certeza a medias sobre la información extraída de internet

Frente a la incertidumbre existente acerca de los límites de la actividad de recolección y tratamiento de información personal con fines de inteligencia, contamos con un poco más de certeza sobre las piezas de información que algunas de las agencias de inteligencia obtienen de internet y de las redes sociales. Se trata de una certeza a medias, en todo caso, pues al ser preguntadas sobre si emplean alguna distinción en el tratamiento de la información recogida en tanto datos públicos, privados o sensibles, las respuestas no son específicas.

La Dipol, por ejemplo, sostiene que recoge *datos abiertos*, expresión que emplea como sinónimo de contenido publicado en línea, y que constituye el primer "insumo para la generación de conocimiento" de inteligencia. Dice consultar, en general, todos los ambientes digitales que son de público acceso en internet "sin que esté limitado a un listado o sitio web preestablecido para la acción de recolección".[13]

La DNI, por su parte, afirma que consulta fuentes de información de acceso público y fuentes abiertas, lo que "incluye redes sociales, blogs, revistas, periódicos" con información sobre personas naturales y jurídicas que sea de interés. No restringe su consulta a sitios web o plataformas concretas. Dice en todo caso que se trata de una consulta "en lo que es estrictamente indispensable para el cumplimiento de la función" de inteligencia.[14] Es más, señala que la consulta de fuentes abiertas "es virtualmente ilimitada" por lo que puede "superar las consultas de otras fuentes de información".[15]

---

12 Ver radicado 2-2022-2113, p. 1.

13 Ver radicado DIPOL-ASJUD-13, 10 de junio de 2022, p. 2.

14 Ver radicado 2-2022-139C, 14 de junio de 2022.

15 Ver radicado 2-2022-2113, p. 1.

Ahora bien, la pregunta sobre la distinción entre los tipos de datos personales que esperan extraer de internet no es banal, pues impacta en la "delimitación e identificación tanto de las personas como de las autoridades que se encuentran legitimadas para acceder o divulgar dicha información" (Corte Constitucional, Sentencia T-729 de 2002).

Según la Corte Constitucional, "cualquier persona de manera directa y sin el deber de satisfacer requisito alguno" puede acceder a los datos personales públicos o de dominio del Estado. El titular de los datos públicos no puede oponerse a su acceso lícito por terceros, aun cuando es su derecho solicitar su actualización, rectificación y cancelación siempre que no tenga el deber de permanecer en dicha base de datos por obra de la ley o un contrato (Corte Constitucional, Sentencia T-729 de 2002).

Los datos personales privados y sensibles, por su parte, significan barreras jurídicas de acceso más o menos intensas para terceros. Aun cuando estos datos puedan estar publicados en internet, su naturaleza no cambia, es decir, su publicidad no los convierte en datos públicos (Superintendencia de Industria y Comercio, 2022). Y solo pueden ser ofrecidos a terceros por "orden de autoridad en el cumplimiento de sus funciones o el marco de los principios de la administración de datos personales" a cargo del responsable (Corte Constitucional, Sentencia T-729 de 2002).

Así mismo, la agregación de datos personales públicos, privados y sensibles, aun cuando está facilitada por el estado del arte tecnológico, está prohibida[16] pues contribuye a la elaboración de "perfiles virtuales", lo cual va en contra del principio de individualidad del dato. Así, el cruce de bases de datos exige de autorización expresa para ello (Superintendencia de Industria y Comercio, 2020; Corte Constitucional, Sentencia C-748 de 2011).

16 Si bien la SIC y la Corte comparten que la agregación de datos es una actividad prohibida, creemos que las dinámicas del tratamiento de datos en el mundo digital tornan a la agregación en una condición necesaria, pues es una práctica de la que dependen los procesos de predicción e inferencia de otros datos. Cambiar el sentido de este criterio demandaría, entre otros, abrir la discusión a la actualización del régimen de protección de datos que, al menos por ahora, no parece estar en el horizonte.

A la pregunta de si en sus tareas de inteligencia efectuaba alguna distinción entre la naturaleza de los datos recogidos en línea, la DNI dijo acoger el contenido de la Ley de Protección de Datos Financieros y la Ley General de Protección de Datos Personales. Sostuvo que "es importante resaltar que [la] excepción al tratamiento de datos personales de que tratan las leyes 1266 de 2008 y 1581 de 2012, no es óbice para que los organismos de inteligencia utilicen indiscriminadamente los datos personales recolectados".[17] Sobre la posibilidad de reconocer al titular del dato el ejercicio del derecho a controlar su información señaló que "el ejercicio del régimen de tratamiento de datos personales no les corresponde a los ciudadanos, cuando estos datos han sido recogidos por organismos de Seguridad del Estado bajo la finalidad de la seguridad y la defensa nacional interna y externa".[18]

Por su parte, la Dipol sostiene[19] que acoge en materia de datos personales "la naturaleza, carácter y condición que las normas existentes establecen para el territorio nacional", pero que "las disposiciones de dicha norma [la Ley General de Protección de Datos] no serán de aplicación". Entonces ¿quiere decir que no aplica la ley de protección de datos personales pero que, al tiempo, acoge la distinción entre datos privados y sensibles de dicho marco normativo? La posición de la Dipol es confusa. Adicionalmente, en materia de derechos del titular, se delimitó a reconocer el papel que ejercen en el tratamiento de los datos los Centros de Protección de Datos, cuyas limitaciones destacamos más arriba.

Las respuestas de las entidades apuntan a la necesidad de reabrir debates aparentemente superados, pero que merecen ser examinados de fondo. Por ejemplo, si los cruces de información en materia de inteligencia están destinados a la inferencia de datos que permitan corroborar ciertas hipótesis ¿cuál es la base jurídica en que se justifican los cruces de bases de datos que pue-

17 Ver radicado 2-2022-2113, p. 3.

18 Ver radicado 2-2022-2113, p. 4.

19 Ver radicado GS-2022-028515/DIPOL-ASJUD-13, 05 de septiembre de 2022, pp. 2 y 3.

den generar efectos jurídicos potencialmente negativos para su titular? Más aún, ¿por qué la naturaleza no consentida de las tareas de inteligencia se debe traducir necesariamente en la imposibilidad del titular de ejercer algún control sobre su información personal, incluso frente a la que es pública?

Por otro lado, ¿pueden las agencias de inteligencia acceder y usar a discreción los datos públicos administrados por el Estado siempre y por cualquier motivo?, ¿qué restricciones conviene aplicar, si es del caso, para que datos personales públicos sean objeto de recolección y tratamiento con fines de inteligencia, por el mero hecho de ser accesibles en línea?

## Práctica de ciberpatrullaje

El ciberpatrullaje es un conjunto de actividades dirigidas a identificar amenazas e incidentes de ciberseguridad, así como a detectar la vulneración de la disponibilidad, integridad y confidencialidad de la información que circula en internet (Resolución 5839, 2015).

Según información oficial, las actividades de ciberpatrullaje[20] comprenden la consulta, observación y recolección de información en línea sobre datos y contenidos abiertos y públicos en internet y redes sociales, "sin ninguna restricción o configuración de privacidad".[21] Los datos de interés son los que permiten estimar el impacto de una publicación en redes sociales, tales como "el conteo sobre el número de publicaciones, interacciones y visualizaciones que ofrecen las mismas redes sociales y páginas web".[22]

Como puede advertirse, la recolección de información

20 Agradecemos a la Fundación para la Libertad de Prensa (FLIP) haber facilitado la consulta pública de las solicitudes de acceso a la información que remitió en 2021 a propósito del despliegue de acciones de ciberpatrullaje en el marco de la protesta social que tuvo lugar durante el mes de mayo de ese mismo año.

21 Ver radicado GS-2021-108176-DIJIN-CECIP 1.10, 24 de agosto de 2021, FLIP, p. 1.

22 Ver radicado GS-2021-DIJIN-CECIP-1.10, 30 de junio de 2021, FLIP, p. 5.

personal en internet, en el contexto de actividades de ciberpatrullaje, parte de presuponer un concepto de lo público y abierto en internet y en redes sociales. Pese a que en estas actividades se aplican límites técnicos –como el de las configuraciones de privacidad que efectúan los usuarios sobre sus cuentas–, la regulación de la actividad y el alcance de estas actividades no son más precisas que las que regulan las actividades de las agencias de inteligencia que fueron consultadas.

Las actividades de ciberpatrullaje están a cargo del Centro Cibernético de la Policía Nacional, adscrito a la dependencia de investigación criminal de este cuerpo. Por la función y la finalidad que realiza esta agencia, la actividad de ciberpatrullaje no es considerada una actividad de inteligencia policial, sino de investigación criminal. El punto crítico es que esta actividad sucede también en línea, y supone el monitoreo de la internet y las redes sociales, así como el acceso y el tratamiento de información personal accesible por estos medios.

La referencia al ciberpatrullaje, sin embargo, permite entender cuál es la visión y la capacidad de algunas autoridades en relación con las actividades de consulta en internet y en las redes sociales como medios para la recolección de información de interés. Pero, sobre todo, apunta a un asunto clave para caracterizar la actividad: precisar los propios conceptos de inteligencia en internet y en redes sociales, y prefigurar los elementos característicos de su eventual regulación.

La distinción entre la actividad de inteligencia y la de investigación criminal ya ha sido explorada en el pasado por la Corte Constitucional colombiana que ha sentado dicha distinción a partir de dos criterios. El criterio funcional, según el cual la actividad de inteligencia busca la protección de intereses generales de mayor alcance, como la vigencia del orden constitucional o la seguridad nacional; orienta las tareas de prevención, control y neutralización de amenazas, y soporta hipótesis de las operaciones que informan la toma de decisiones de Estado. Y el criterio del valor probatorio, según el cual la información de inteligencia no tiene valor probatorio en materia judicial (sentencias C-913 de 2010 y C-540 de 2012).

La investigación criminal, en cambio, está enfocada en recabar elementos probatorios que puedan ser valorados en un juicio, ante un juez independiente, con el fin de determinar la eventual responsabilidad penal de una persona. Asimismo, por su especial vocación probatoria, debe ser producida según las reglas del debido proceso y está sometida a la contradicción pública. Aunque es cierto que la información de inteligencia puede llegar a ser usada en la etapa de indagación penal, solo tiene la capacidad de servir como "criterio orientador", no como prueba (Ley 1621 de 2013; Corte Constitucional, sentencias C-913 de 2010 y C-540 de 2012).

***

A partir de las respuestas de las entidades que integran la comunidad de inteligencia y de las demás autoridades públicas inquiridas, hemos llegado a dos conclusiones preliminares que dan cuenta de un escenario complejo, que trasciende a la confección de la ley de inteligencia.

Primero, el presupuesto o el punto de partida según el cual toda la información personal accesible o disponible en internet es sinónimo de dato personal público, accesible y usable sin límite o restricción. Este presupuesto sirve para desestimar toda distinción relevante en materia de datos personales, y su incidencia en el valor asociado a la protección de la vida privada. Esta concepción de la información personal impide siquiera proponer la posibilidad de ejercer algún tipo de control sobre la información personal por parte de su titular.

Segundo, la excepción de la que gozan las agencias de inteligencia para no aplicar la Ley de Protección de Datos genera lecturas que no solo son confusas de cara a la ciudadanía, sino que no son convergentes, incluso entre la misma comunidad de inteligencia. Dicha excepción cumplió una década de vigencia, sin embargo, no hay claridad sobre cómo las tareas de inteligencia deben aplicar los principios de la protección de datos exigibles a los regímenes exceptuados de dicha ley. Tampoco es claro quién tiene a su cargo vigilar la garantía en su aplicación.

Sobre esto último preguntamos a la Procuraduría General de la Nación, en su rol de autoridad de protección de datos de las entidades públicas, si lleva a cabo la vigilancia en la aplicación de los principios de protección de datos por parte de las agencias de inteligencia. En su respuesta nos indicó "carecer de competencia para conocer de este asunto".[23] Lo anterior, en tanto la resolución interna que regulaba el ejercicio de estas facultades fue derogada, por la propia Procuraduría General, en el mes de mayo de 2022. Una situación crítica. Claro indicio de la precariedad de los mecanismos de control y seguimiento externo, preventivo e independiente sobre la inteligencia nacional.

Tercero, pese a que las agencias de inteligencia opusieron reserva sobre distintos aspectos satisfaciendo la carga argumentativa que impone el test del daño, el alegato de la reserva según la materia sigue siendo discrecional. Por ejemplo, la DNI alegó reserva sobre la información de capacitación de su personal, información que proveyó con amplitud la Dipol.

En cuarto lugar, y no menos importante, queremos evidenciar las dificultades asociadas a la aprehensión de la gobernanza de la inteligencia en Colombia. No es fácil comprender cómo se organizan las agencias de inteligencia internamente, o cómo colaboran entre sí, incluso cómo se relaciona la comunidad de inteligencia (que lleva a cabo las tareas propias) con la Junta de Inteligencia Conjunta (que decide sobre la cooperación interinstitucional en la materia).[24]

Por ejemplo, preguntamos al Departamento Conjunto de

---

23 Ver radicado Oficio 1135, 1 de junio de 2022.

24 Integrada, entre otros, por el ministro de la Defensa Nacional, el Alto Asesor para la Seguridad Nacional o el funcionario de nivel asesor o superior que delegue para ello el presidente de la República; el viceministro de Defensa Nacional; el jefe de Inteligencia Conjunta, en representación del comandante general de las Fuerzas Militares; el jefe de Inteligencia del Ejército Nacional, en representación del comandante de esa Fuerza; el jefe de Inteligencia de la Armada Nacional, en representación del comandante de esa Fuerza; el jefe de Inteligencia de la Fuerza Aérea Colombiana, en representación del comandante de esa Fuerza; el director de Inteligencia Policial, en representación del director general de la Policía Nacional; el director de la UIAF, o su delegado, entre otros.

Inteligencia del Comando General de las Fuerzas Militares[25] si, fruto de la aplicación de la Ley 1621 de 2013, acudía a la inteligencia en internet y redes sociales, a lo que respondió que no, en tanto que no hace parte de sus funciones.[26] Para apreciar esta respuesta tenemos que acudir a la distinción entre *producción* de la información de inteligencia (a cargo únicamente de la comunidad de inteligencia, y en donde se toman decisiones sobre el medio de recolección de información), y el *consumo* y *compartición* del análisis de la información de inteligencia (en la que participa la Junta de Inteligencia Conjunta).

Sin embargo, ¿es responsabilidad de los más altos mandos militares conocer cuáles son las fuentes de información que fueron empleadas por la comunidad de inteligencia en sus tareas operativas?, ¿el principio de compartimentación de la información inhibe a la Junta de Inteligencia Conjunta para conocer cuáles fueron los medios de inteligencia empleados en el marco de una operación? La reserva sobre (casi) todo lo que tiene que ver con la actividad de inteligencia nos impide ahondar en esas preguntas.

Por último, los expertos consultados coinciden en afirmar que la inteligencia en internet y redes sociales precisa de límites jurídicos claros, más allá de las fórmulas abiertas que ordenan el cumplimiento de la Constitución y la ley. Además, estiman que los límites deberían intentar armonizar los intereses relacionados con la protección de la privacidad de las personas con el ejercicio de las funciones del Estado.

La moderación de las expectativas sobre lo que los límites a la explotación de internet y las redes sociales pueden lograr es otro punto en el que coinciden los entrevistados. Serán reducidas hasta que, por ejemplo, las prácticas y los criterios de identificación de los objetivos de inteligencia no cuenten con mecanismos de supervisión y control externa e independiente.

---

25 Y que hace parte de la Junta de Inteligencia Conjunta.

26 Ver radicado 0122006705402/MDN-COGFM-JEMCO-SEMOC-CGDJ2-OASPP-1.10, 9 de junio de 2022.

Declarar objetivos de interés a periodistas, defensores de derechos humanos o miembros de partidos políticos es altamente problemático y es, *prima facie*, ilegal, según los términos de la propia Ley de Inteligencia. Adicionalmente, su individualización, a partir de su categorización como supuestas amenazas a la seguridad nacional es claramente ilegal.

Desde luego, la discusión sobre los medios de inteligencia obliga a reconocer las fallas estructurales que padece la inteligencia colombiana en lo que tiene que ver con el funcionamiento de los mecanismos de control interno, judicial, disciplinario y de control político (a cargo del Congreso de la República y que, por cuestiones asociadas a la acreditación de seguridad de sus integrantes, no ha podido sesionar una sola vez); la desviación de recursos de inteligencia y la adquisición opaca de tecnologías de vigilancia masiva, entre otros.

VOLVER AL CONTENIDO

## 4. Una propuesta para avanzar en la discusión sobre los límites deseables

Frente a la relativa novedad de las actividades de inteligencia en fuentes abiertas, específicamente en internet y en redes sociales, la ausencia de regulación y lo que revelan las prácticas de inteligencia en relación con el entendimiento del objeto (información personal disponible en fuentes abiertas), así como la laxitud de los límites, esto es, ante la necesidad de avanzar en el proceso de institucionalización de las prácticas de inteligencia, nos preguntamos ¿cómo deberían enfocarse los esfuerzos para abordar el uso legítimo de la inteligencia estatal que se despliega en internet y en las redes sociales?

En primer lugar, debemos partir de la vocación regulatoria del derecho a la protección de la vida privada a toda actividad que se desarrolle en, y a partir de, los escenarios digitales. Debemos, igualmente, partir de entender la inteligencia en internet y en redes sociales como una actividad que merece un abordaje más allá del de mera fuente o medio de información. La internet y las redes sociales son espacios con arquitecturas específicas,

políticas y actores que merecen ser considerados a la hora de desplegar y regular la actividad de inteligencia.

En segundo lugar, debemos atender a la naturaleza de la inteligencia en fuentes abiertas y no desnaturalizarla en el camino. La información que no es pública ni abierta, y que se busca explotar a través de las actividades de inteligencia, obedece a otro tipo de inteligencia cuyos impactos merecen ser igualmente analizados y cuyas particularidades deben ser estimadas para efectos de una regulación integral de la actividad.

En tercer lugar, debemos avanzar en el reconocimiento del derecho a la protección de datos personales frente a las agencias que adelantan actividades de inteligencia en fuentes abiertas y frente a la información así obtenida y registrada en los archivos de inteligencia. Es indispensable diseñar reglas claras que definan la oportunidad y la extensión de mecanismos legales que permitan a las personas saber qué información se recoge de ellas en las tareas de inteligencia así desarrolladas, cómo ha sido recogida, para qué finalidad y bajo qué procedimientos.

En especial, se debería partir del deber de facilitar el acceso y la entrega efectiva de la información personal que haya sido recogida a partir de fuentes abiertas o en redes sociales, y que sea solicitada por su titular. La razón es sencilla: la información que fue recogida y tratada bajo el presupuesto de ser pública o información obtenida en medios o en fuentes abiertas, no debería privatizarse-reservarse tras su obtención, y menos aún frente a su titular.

Sobre el particular, las buenas prácticas sobre promoción de los derechos humanos por los servicios de inteligencia, del Relator de las Naciones Unidas sobre derechos humanos y lucha contra el terrorismo Martín Scheinin, reconocen que, si bien la reserva de la información puede estar destinada a proteger las investigaciones en curso, sus fuentes y métodos, aquella no es incompatible con el derecho de acceso a la información personal respecto de investigaciones que ya concluyeron o que ya cumplieron su ciclo y utilidad, incluso frente a la información que reposa en archivos de inteligencia.

Las buenas prácticas reafirman que el acceso a la información personal es una herramienta que "protege del abuso, la mala administración y la corrupción [que] contribuye a aumentar la confianza de los ciudadanos en la acción del gobierno" (Scheinin, 2010, pp. 25, 26). Estas buenas prácticas pueden ser acogidas vía legislativa, pues ya han tenido eco en la jurisprudencia constitucional, más concretamente, en el contenido de la Sentencia C-540 de 2012 que declaró a la Ley de Inteligencia ajustada a la Constitución Política.

### Privacidad en línea

Al contrario de la posición que parece ser sostenida por algunos expertos y agencias de inteligencia, la información personal que se publica en internet no es, por el hecho de haber sido publicada, información que pueda ser usada de cualquier manera y para cualquier finalidad por parte del Estado.

La posición de algunos expertos, acogida por las agencias de inteligencia, sugiere que la publicación en internet supone una renuncia total a la posibilidad de controlar la propia información y de reivindicar, en todo caso, la protección de la vida privada como un derecho fundamental. Se trata de una posición que sugiere que la información personal bien sea sensible, privada o pública, puede ser objeto de libre acceso y tratamiento por parte de las agencias de inteligencia del Estado, lo que termina por trasladar toda la carga de la protección de la propia información a sus titulares. Además de ser controvertible, esta posición busca ocultar una discusión de fondo más importante: aquella sobre los límites necesarios a la actividad de inteligencia.

Lo cierto es que la posibilidad de controlar la información propia, como una manifestación de los derechos fundamentales a la identidad, a la libertad personal y a la protección de la vida privada, se extiende tanto en línea como fuera de ella, así lo ha reconocido la Corte Constitucional en su propia jurisprudencia.[27] El hecho circunstancial de que información personal esté

27 De hecho, la Corte sostuvo hace más de dos décadas que "los mandatos expresados en la Carta Política cobran un significado sustancial que

disponible en línea, por diversos motivos y de diferentes formas, no implica que la persona pierda jurídicamente la facultad de controlarla, ni de intervenir cuando la misma está siendo empleada en actividades o en circunstancias que la afecten o puedan afectarla.

Por ejemplo, una persona que decide compartir en redes sociales su postura respecto del gobierno de turno, así como información sobre los lugares que visita, no cuenta con la posibilidad de controlar los posibles usos no previstos y no queridos a los que pueda ser sometida esta información por parte de terceros, y, especialmente, por parte del Estado. Los ajustes de privacidad que pueda efectuar sobre su cuenta en la red social son límites técnicos que, en todo caso, pueden ser superados fácilmente por los investigadores de inteligencia a través del envío de una solicitud de amistad o para seguir dicha cuenta a través de un perfil falso cuyas intenciones son indetectables para la persona propietaria de la cuenta.

Pero por estar disponible en internet, la información que puede ser considerada privada y sensible (que lo es en razón del riesgo de discriminación que su recolección significa para su titular) no pierde su naturaleza,[28] ni su titular pierde la posibilidad

---

demanda del juez constitucional la protección de los derechos reconocidos a todas las personas, pues se trata de garantías que también resultan aplicables en ese ámbito. En Internet puede haber una realidad virtual, pero ello no significa que los derechos, en dicho contexto, también lo sean. Por el contrario, no son virtuales: se trata de garantías expresas por cuyo goce efectivo en el llamado "ciberespacio" también debe velar el juez constitucional" (Corte Constitucional, Sentencia C-1147 de 2001). Esta distinción entre derechos en línea y fuera de ella ha sido eliminada también por la Carta para Derechos Humanos y Principios en Internet de Unesco (Internet Rights & Principles Coalition, 2015).

28 "Independientemente que la información del accionante en su cuenta de Twitter y sus trinos puedan ser consultados abiertamente por el público, la accionada [la Presidencia de la República] no estaba facultada para hacer uso de la misma como si se tratase de datos de naturaleza pública y con fundamento en ello elaborar el listado de influenciadores en el que incluyó el acto, pues es evidente que lo que determinó su inclusión y el calificativo de 'negativo' fue precisamente su ideología política, plasmada en la interacción en su red social" (Corte Suprema de Justicia, 2020).

de exigir la limitación de su uso, así como el derecho a impedir su tratamiento para fines ilegales o inconstitucionales.

Por tratamiento entendemos, según la legislación colombiana, tanto su recolección como su agregación con otra información tomada de fuentes públicas o privadas, incluidos, por ejemplo, los cruces de bases de datos y la recopilación del historial de interacciones o de la información compartida por una persona en el pasado. De más está decir que, en ese último evento, la persona no solo tiene el derecho a cambiar de ideas y modificar su identidad con el paso del tiempo; y que la información, en tanto que personal (que no deja de serlo por el hecho de su divulgación en línea[29]), puede ser protegida por su vinculación con diferentes derechos fundamentales, incluido el derecho a la protección de la vida privada y de datos personales en los entornos digitales que son, a su vez, instrumentales para el ejercicio de otros derechos de interés tanto individual como colectivo, como el de libertad de expresión.

Es cierto que la expectativa de privacidad en línea, o la posibilidad de controlar el uso de la propia información personal disponible en internet enfrenta serios retos en distintos escenarios. Y que las discusiones sobre el alcance de estos derechos van mucho más allá de los debates propios de la inteligencia estatal que se despliega en internet y redes sociales.

También es cierto que, frente a la complejidad de estos retos, los propios de la inteligencia estatal parecen tener un rol marginal. La consciencia de esta complejidad sirve para concentrar el debate y para contextualizar nuestra propuesta. Sobre todo, porque estamos frente a una actividad estatal que debe adelantarse bajo las formas constitucionales y respetar los límites del Estado de derecho, que obedece a unas dinámicas institucionales cuyas reglas han sido construidas durante décadas por los sistemas democráticos.

---

29 "No todos los datos que se encuentran en una base de datos pública, en medios de comunicación masiva o internet, son públicos por este solo hecho" (Superintendencia de Industria y Comercio, 2022); "los datos personales que se encuentren en sitios de acceso público como redes sociales o internet por ese solo hecho no convierte a dichos datos personales en naturaleza pública" (Superintendencia de Industria y Comercio, 2020).

## Nuestra propuesta: regular a partir de casos análogos

### La inteligencia en las redes sociales

Para pensar los límites legales a las actividades de inteligencia en línea podríamos tomar prestado el conjunto de limitaciones propias de dos figuras prominentes de las actividades de inteligencia del Estado colombiano: el monitoreo pasivo del espectro electromagnético y la interceptación de las comunicaciones. Nuestra propuesta es asimilar las actividades de inteligencia que suceden en las redes sociales, como una forma activa de monitoreo en línea que merece un estatus de protección similar al que se concede a la interceptación de las comunicaciones.

En Colombia, la legislación distingue entre el monitoreo pasivo del espectro y la interceptación de las telecomunicaciones. El monitoreo pasivo del espectro electromagnético es una actividad de rastreo indeterminado, abstracto y temporalmente limitado de la autopista invisible por la que transitan las comunicaciones, y que está dirigida a la identificación de amenazas al conjunto de bienes sociales que la inteligencia procura proteger (Corte Constitucional, sentencias C-540 de 2012 y C-570 de 2010).

Cuando el monitoreo pasivo del espectro busca trascender hacia la individualización de una persona para escuchar las comunicaciones que esta sostiene con otras, se está frente a la interceptación de las comunicaciones que, por su impacto en la privacidad en el intercambio de las comunicaciones, solo procede con orden previa de las autoridades competentes para adelantar la investigación de delitos. Sus resultados están sometidos al control de un juez de la República que debe garantizar la legalidad de los procedimientos y la protección de los derechos fundamentales, incluido el derecho a la intimidad de las personas afectadas (leyes 906 de 2004 y 1621 de 2013). Por suponer una limitación concreta a la órbita del derecho a la intimidad de una persona determinada, las agencias de inteligencia no tienen facultades para llevarla a cabo.

Por sus particularidades, el monitoreo activo en redes sociales supone tanto la lectura como la recopilación de infor-

mación asociada a las interacciones de una única persona en cualquier red social. Este tipo de monitoreo no es impersonal, mucho menos abstracto; está dirigido al perfilamiento, es decir, a la individualización plena de una persona. En tanto que busca responder a la pregunta *quién es quién*, apunta intencionadamente a la delimitación de su personalidad y comportamiento (en el pasado y en el presente), a revelar sus interacciones y red de contactos, así como a la caracterización de sus hábitos sociales e incluso, de sus posturas políticas, religiosas o ideológicas. Todo lo anterior, con el fin de agregar dicha información con otra proveniente de fuentes públicas y privadas, con el objetivo último de extraer conclusiones potencialmente riesgosas para la persona objeto del monitoreo.

Así, el monitoreo activo de las redes sociales tiene un potencial altamente invasivo, equivalente a la invasión a la privacidad fruto de la interceptación de las comunicaciones. Ahora bien, si las plataformas de redes sociales buscan, en general, servir como espacios de interacción social entre las personas que, para tal efecto, intercambian información de todo tipo sobre sí mismas (contenido que incluye, o puede incluir, datos personales privados y sensibles), ¿por qué no trasladar a dichos entornos garantías similares a las que cobijan el intercambio de las comunicaciones privadas?, es más, ¿por qué sería legítimo establecer una distinción en punto a las garantías para la protección de la vida privada, entre el medio en que circula la información y el medio del que termina por ser obtenida?

Es decir, si la individualización de las personas a través de sus interacciones en redes sociales genera el mismo resultado que las actividades de interceptación de las comunicaciones, esto es, su perfilamiento a través del monitoreo, no habría en principio razones para conceder a la inteligencia en redes sociales garantías más débiles que aquellas aplicables a la afectación de la privacidad en el marco de las tareas de interceptación de las comunicaciones. Ambas tareas tienen incidencia en la vida privada de las personas, casi con la misma intensidad.

Desde luego, aceptar esta postura significaría reformar las actividades de inteligencia para someter, por primera vez, dicha

tarea a la revisión de un organismo independiente, lo que significa una oportunidad valiosa para fortalecer la legislación sobre inteligencia a través de la adopción de las buenas prácticas de las Naciones Unidas en la materia. Al respecto, el Relator M. Scheinin sugirió que "las medidas invasivas de recopilación de información sean autorizadas por una institución independiente de los servicios de inteligencia, por ejemplo, un miembro del poder ejecutivo que asuma la responsabilidad política o un organismo (cuasi) judicial" (2010, p. 22), incluso por un organismo judicial en tanto que "están en mejores condiciones de efectuar una evaluación independiente e imparcial de una solicitud de aplicación de medidas invasivas de recopilación de información" (p. 22).

Conceder al monitoreo activo de las redes sociales las garantías de supervisión externa e independiente, similares a las aplicables a las interceptaciones de las comunicaciones, permitiría asegurar, entre otras, i) la revisión de la pertinencia, idoneidad, finalidad y necesidad de la información (privada y sensible) que busca ser extraída de las redes sociales con el fin de individualizar a una persona; ii) revisar la motivación que justifica el despliegue de la medida, la cual debe estar debidamente fundada; iii) ponderar la extensión razonable en el tiempo del monitoreo. Sobre cada uno de estos criterios, la jurisprudencia emitida en materia de interceptación de las comunicaciones puede llegar a aportar elementos que sirvan para la construcción de buenos estándares.

Con la adopción de medidas de este tipo, y, especialmente, a través de la intervención de un organismo independiente, las tareas de investigación y de decisión sobre la pertinencia de la recolección de información altamente invasiva de la privacidad recaerían en dos organismos distintos, a diferencia del estado de cosas actual, en que el superior jerárquico de quien dicta la orden de una misión de inteligencia es quien tiene a su cargo verificar la compatibilidad de la medida, con la limitación que representa para el ejercicio de los derechos de la persona afectada.

Asimismo, le permitiría a la persona afectada el ejercicio de su derecho al debido proceso a través, por ejemplo, de la solicitud de exclusión de su información personal y sensible, bien

porque no sea pertinente para la investigación de inteligencia que ya concluyó o que se encuentra archivada, porque haya sido obtenida de manera ilícita o ilegal, o porque esté orientada por criterios discriminatorios –como su pertenencia a un partido político, su ejercicio de defensa de los derechos humanos, o su trabajo periodístico crítico del gobierno de turno–.

Más aún, cuando la información de inteligencia llegue a ser empleada como criterio orientador en el marco de un procedimiento judicial, la persona afectada debería poder ser notificada sobre la obtención de información personal suya en el marco de las actividades de inteligencia, lo que la facultaría para el ejercicio del derecho de acceso y contradicción pública de la información personal que fuese recogida sobre ella.

### La inteligencia en el resto de la internet

Ahora bien, la inteligencia que se adelanta en el resto de la internet –es decir, fuera de las redes sociales– merece un comentario aparte. Aquí tendríamos que considerar el impacto de la inteligencia que se despliega en la capa más superficial para los usuarios o la capa de contenidos,[30] es decir, en el resto de plataformas, servicios y aplicaciones en línea en los que circulan contenidos e información generados por los usuarios y que merecen análisis diferenciados, lo que desde ya representa un reto en la regulación de la inteligencia en línea en un ecosistema de intermediarios que muta constantemente.

Esta diferenciación, sin embargo, es relevante. Las reflexiones sobre monitoreo de las redes sociales no se pueden extender al monitoreo de los servicios de mensajería instantánea, por ejemplo. No solo porque son plataformas con una arquitectura de la información diferenciada, sino porque la difusión de información entre los usuarios sirve para propósitos comuni-

30 Hay tipos de inteligencia que, de hecho, se despliegan sobre la capa física o de infraestructura de internet. Por sus particularidades y potencial altamente invasivo de las comunicaciones de las personas merece un abordaje separado del que proponemos para la inteligencia que tiene lugar sobre la capa de contenidos, servicios y aplicaciones de la red.

cativos disímiles, en los que la expectativa de privacidad puede variar.

Por ejemplo, es mucho más intensa la expectativa de privacidad frente al Estado tratándose del intercambio de las comunicaciones que tienen lugar en los servicios de mensajería privada, en comparación con el grado de expectativa de privacidad que opera frente a los mensajes que se publican en redes sociales para una audiencia más o menos abierta según la red social en cuestión.

Desde luego, garantías tecnológicas como la del cifrado impiden el monitoreo pasivo por el Estado sobre los mensajes enviados a través de ciertos servicios de mensajería instantánea que ofrecen dicha garantía de privacidad a sus usuarios. En ese caso, el acceso de las autoridades al intercambio de esos mensajes (y los metadatos asociados a estos) debe estar amparado por reglas específicas que, como mínimo, deberían prever mecanismos de revisión o autorización judicial.

## Esfuerzos adicionales a los de regulación

Aun así, quizá no sea conveniente inhibir del todo el despliegue de las tareas de inteligencia en internet para hacer frente a las amenazas a la seguridad nacional que tienen lugar en línea. Para ello, conviene hacer un llamado adicional a la reflexión ante la posible duplicación de capacidades en tanto que la inteligencia que se despliega en internet está también en manos de entidades especializadas en materia de ciberseguridad. Ambas conservan una finalidad preventiva, pero ¿cuáles son los límites o las fronteras de cada una?

De hecho, el documento del Consejo Nacional de Política Económica y Social (Conpes) "Política nacional de confianza y seguridad digital" advierte que entre las entidades de ciberseguridad y las entidades tradicionales de inteligencia que se despliegan en línea (entre ellas las Fuerzas Militares y la Policía Nacional) no existe interacción, coordinación, articulación ni cohesión suficiente que permita entender a qué objetivo se dedica cada una a la hora de contener amenazas en el entorno digital (Conpes 3995, 2020).

La falta de interacción y cohesión no es un asunto menor entre entidades que ejercen facultades de inteligencia con una misma finalidad preventiva. De hecho, preguntamos al Grupo de Respuesta a Emergencias Cibernéticas (ColCERT), que integra el grupo de organizaciones encargadas de la protección de la Seguridad Digital Nacional, si desplegaba tareas de monitoreo o perfilamiento a partir de la actividad en línea de usuarios en internet y redes sociales, a lo que respondió que no lo hacía.[31]

Sin embargo, como hemos visto hasta ahora, las entidades "tradicionales" de inteligencia que han trasladado sus tareas a internet más recientemente, lo hacen en el contexto de sus labores de protección de la seguridad nacional, sin importar el entorno en el que surge, se multiplica o circula una amenaza; entonces ¿cómo se articulan entre sí en el entorno digital? Más aún, ¿cómo entender el margen de acción de las actividades de inteligencia en internet y las de ciberseguridad con las de ciberpatrullaje? El volcamiento de las fuerzas de seguridad del Estado a internet y las redes sociales merece un acercamiento comprensivo que llame la atención por un posible escenario de hipervigilancia de la actividad de los usuarios de internet, que no ha sido plenamente delimitado hasta ahora.

Ante este escenario de creciente hipervigilancia, de origen múltiple, conviene responder con el fortalecimiento de los mecanismos de transparencia activa que deberían tener a su cargo los servicios de inteligencia. Sobre este punto, las buenas prácticas del Relator Especial de las Naciones Unidas Martín Scheinin llaman la atención para que se informe "al público en general de la clase de datos personales que tienen en archivo, el tipo de datos personales que pueden retener en el archivo, el alcance de los datos y los motivos que justifican la retención de información personal en el servicio" (2010, p. 24). Junto a estos esfuerzos, se debe insistir en la desclasificación y depuración de los archivos de inteligencia de manera independiente y supervisada por organizaciones de la sociedad civil.

Finalmente, la discusión sobre los límites a la inteligencia

31 Ver radicado 221042369 de 2022, 17 de junio.

en internet y en redes sociales trasciende el análisis sobre cómo se explota un medio en el que circula información personal que es declarada de interés y que incide, entre otros, en el derecho a la vida privada. Esta es una discusión que implica abordar un panorama mucho más extenso que involucra a diversos actores, capacidades y tecnologías. Una visión comprensiva del problema no debe perder de vista que en el centro de la discusión están las personas, así como la garantía y la protección de sus derechos, en el entorno que sea.

VOLVER AL CONTENIDO

## Recomendaciones

Mejorar la regulación de inteligencia es una agenda con múltiples prioridades. A los llamados de atención tradicionales para el fortalecimiento de los mecanismos de seguimiento y control judicial, disciplinario, político e interno de dichas actividades; de definición de competencias y facultades interinstitucionales; de adquisición transparente de tecnologías de vigilancia masiva; de depuración de los archivos de inteligencia, entre otras, se suma también la necesidad de una mejor consideración sobre la internet y las redes sociales.

La internet y las redes sociales son mucho más que un medio de información estratégica para obtener contexto. Para las personas que las emplean constituyen un espacio de encuentro, socialización e intercambio con otros. Su explotación en materia de inteligencia debe ser sensible a los usos y fines que satisface la red hoy, que tiende cada vez más a la digitalización continua de la vida y que se espera aumente los flujos de información sobre las personas que serán cada vez mayores y diversos en su tipo. Para avanzar en la solución de algunos de los problemas advertidos en esta investigación, proponemos las siguientes recomendaciones:

### *Para el Congreso*

1. Regular el derecho a la protección de datos de cara a las actividades de inteligencia en internet y las redes sociales. Frente a la excepción introducida en la Ley General

de Protección de Datos Personales de 2012, y el silencio de la Ley de Inteligencia de 2013 en la materia, el Congreso no puede continuar evadiendo la pertinencia y la urgencia de activar formas de control jurídico sobre la información personal recolectada y sometida a tratamiento con fines de inteligencia.

2. Delimitar la amplitud con que las agencias de inteligencia pueden recoger información personal pública, que reposa en las bases de datos administradas por el Estado. Asimismo, precisar las reglas sobre recolección de información personal y sensible mediante el monitoreo y el perfilamiento sostenido en internet y en redes sociales.
3. Avanzar en la activación del control político a cargo de la Comisión de Inteligencia y Contrainteligencia del Congreso, su labor es esencial para transparentar dicha tarea y exigir de manera pública la entrega de información cuyo acceso se deniega a la ciudadanía. Su funcionamiento debe cuestionar, entre otras, cómo se explotan internet y las redes sociales, qué tecnologías digitales se tienen y despliegan a propósito de esa tarea, y cómo se activan las garantías de protección de datos a cargo de los Centros de Protección de Datos, entre otros.

*Para las agencias de inteligencia*

1. Regular internamente sus prácticas sobre la explotación de internet y las redes sociales en el marco de sus tareas. Al avanzar en su desarrollo, es importante que provean instrucciones precisas a los investigadores de inteligencia sobre qué tipo de información personal debe o no ser extraída de internet y las redes sociales, con base en qué criterios se orienta la obtención de contexto sobre las personas y sus redes de contactos, y cómo se llevará a cabo el tratamiento de la información a partir de la naturaleza del dato personal (público, privado o sensible), entre otros.

2. Fortalecer los procesos de capacitación sobre inteligencia en internet y en redes sociales. En especial, a fin de que los investigadores de inteligencia tomen conciencia sobre el valor que tiene internet como entorno de socialización e intercambio de ideas y opiniones. Un espacio en el que se deben aplicar las mismas garantías vigentes fuera de línea en materia de privacidad, y en el que la presencia o actividad de las personas no debe ser entendida como una cesión automática sobre el ejercicio de sus derechos a la protección de su información personal.
3. Avanzar en la apropiación institucional de la Ley de Acceso a la Información, y en la aplicación consistente de su contenido. La oposición de la reserva debe ser excepcional y estar fundada en algo más que los temores de que la publicación de la información sobre, por ejemplo, el tipo de datos que recogen de internet y las redes sociales pueda ser "usada por el enemigo" para contrarrestar los esfuerzos de protección de la seguridad nacional del Estado.

*Para el resto del Gobierno nacional*

1. Delimitar las funciones, el alcance y la extensión de las actividades de inteligencia en internet frente a las actividades de ciberseguridad, a fin de que la convergencia de las múltiples entidades públicas involucradas en la protección de la seguridad nacional en línea no se traduzca en una redundancia de funciones que derive en la vigilancia de múltiples capas de los usuarios de internet.
2. Avanzar en la depuración de los archivos de inteligencia. Se trata de un mecanismo que, si bien no concede a las personas un control directo sobre la información personal que reposa en las bases de datos de inteligencia, permite a otros garantizar una curaduría de la información de inteligencia para que, la que ya cumplió su ciclo o valor, o que fue recolectada de manera ilegal, sea finalmente excluida y eliminada. La depuración debe, además, ser garantizada con la participación de organizaciones de la sociedad civil

y de organismos independientes que puedan vigilar dicho proceso de manera externa, tal y como ha sido solicitado por Dejusticia en el pasado.

*Para la academia y la sociedad civil*

1. Avanzar en el análisis sobre los impactos que tiene la inteligencia en internet y redes sociales frente al derecho a la protección de la vida privada y su carácter instrumental para el ejercicio de otros derechos, como la libertad de expresión. Análisis que deben volver sobre debates en apariencia cerrados, como la imposibilidad de ejercer acciones de control sobre los datos personales en manos de las agencias de inteligencia.
2. Interrogar acerca de los estándares de protección de los derechos fundamentales en el contexto de, o a partir de internet, los cuales no deberían reducir su nivel de protección ni su alcance en razón del medio de circulación de la información, sino por el impacto que tiene su uso para fines no previstos por su titular.

   En concreto, se debe pensar en las garantías deseables en razón del impacto que tiene para el derecho a la protección de la vida privada la recolección de información (pública, privada o sensible) que fue publicada en internet como parte del ejercicio de su libertad de expresión, su agregación con otras fuentes de información pública y privada, y el perfilamiento a través del monitoreo de la actividad en línea para apuntalar o para probar hipótesis que tengan impactos potencialmente negativos sobre los titulares de dicha información.

VOLVER AL CONTENIDO

## Referencias

Akhgar, B. (2016). OSINT as an Integral Part of the National Security Apparatus. En B. Akhgar, P. S. Bayerl y F. Sampson (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation* (pp. 3-10). Springer International Publishing.

Bruneau, T. C. y Boraz, S. C. (2007). Intelligence reform: Balancing democracy and effectiveness. En T. C. Bruneau y S. C. Boraz (Eds.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (pp. 1-24). University of Texas Press.

Consejo Nacional de Política Económica y Social (2020). Política Nacional de Confianza y Seguridad Digital (3995). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Congreso de la República (2004). Ley 906 por la cual se expide el Código de Procedimiento Penal. http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Congreso de la República (2012). Ley 1581 por la cual se dictan disposiciones generales para la protección de datos personales. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la República (2013). Ley 1621 por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Corte Constitucional, Sentencia C-1147 de 2001, M. P. Manuel José Cepeda Espinosa. https://www.corteconstitucional.gov.co/Relatoria/2001/C-1147-01.htm

_____, Sentencia T-729, 2002, M.P. Eduardo Montealegre Lynett. https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

_____, Sentencia C-570 de 2010, M.P. Gabriel Eduardo Mendoza Martelo. https://www.corteconstitucional.gov.co/RELATORIA/2010/C-570-10.htm

_____, Sentencia T-708 de 2008, M. P. Clara Inés Vargas Hernández. https://www.corteconstitucional.gov.co/relatoria/2008/T-708-08.htm

_____, Sentencia C-913 de 2010, M. P. Nilson Pinilla Pinilla. https://www.corteconstitucional.gov.co/RELATORIA/2010/C-913-10.htm

_____, Sentencia C-540 de 2012, M. P. Jorge Iván Palacio Palacio. https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

Corte Suprema de Justicia, Sala de Casación Penal, Sala de decisión de tutelas n. 1, Sentencia STP9319-2020, M. P. Eugenio Fernández Carlier. https://vlex.com.co/vid/sentencia-corte-suprema-justicia-851632638

Departamento Administrativo de Presidencia (2011). Decreto 4179 por el cual se crea un Departamento Administrativo y se establece su objetivo, funciones y estructura. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44666

_____ (2014). Decreto 857 por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones". https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57315#0

Dirección de Inteligencia Policial (2022, junio 10). Respuesta a solicitud de acceso a la información, radicado DIPOL-ASJUD-13.

_____ (2022, septiembre 05). Respuesta a solicitud de acceso a la información, radicado GS-2022-028515/DIPOL-ASJUD-13.

DNI (2022, junio 14). Respuesta a solicitud de acceso a la información radicado 2-2022-139C.

_____ (2022, agosto 29). Respuesta a solicitud de acceso a la información, radicado 2-2022-2113.

Dirección General, Policía Nacional (2014). Resolución 01446 por la cual se establece el Manual de Inteligencia y Contrainteligencia para la Policía Nacional.

Ejército Nacional (2016). Resolución 01886 por la cual se aprueba el Manual Fundamental del Ejército MFE 2-0 Inteligencia.

_____ (2017). Resolución 01869 por la cual se aprueba la actualización del Manual Fundamental del Ejército MFE 2-0.

El País (2020, mayo 6). Chuzadas en Colombia, un fenómeno ilegal que parece no tener fin. *El País*. https://www.elpais.com.co/colombia/chuzadas-en-un-fenomeno-ilegal-que-parece-no-tener-fin.html

Fundación para la Libertad de Prensa (2020). Páginas para la libertad de expresión. *Revista de la Fundación para la Libertad de Prensa (FLIP)*, 4, agosto.

Gibson, H. (2016). Acquisition and preparation of Data for OSINT investigations. En B. Akhgar, P. S. Bayerl y F. Sampson (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation* (pp. 69-94). Springer International Publishing.

Hassan, N. A. (2019). Gathering Evidence from OSINT Sources. *Digital Forensics Basics* (pp. 311-322). Apress.

Internet Rights & Principles Coalition (2015). Carta de Derechos Humanos y Principios para Internet. https://www.palermo.edu/cele/pdf/Carta-de-Derechos-Humanos-y-Principios-para-Internet-en-Espanol.pdf

Marzell, L. (2016). OSINT as Part of the strategic National Security Landscape. En B. Akhgar, P. S. Bayerl y F. Sampson (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation* (pp. 3-10). Springer International Publishing.

Ministerio de Defensa (2015). Decreto 1070 por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76837

Ministerio de las Tecnologías de la Información y las Comunicaciones (2022). Respuesta a solicitud de acceso a la información, radicado 221042369 del 17 de junio.

Miller, B. (2018). Open Source Intelligence (OSINT): An Oxymoron? *International Journal of Intelligence and Counter Intelligence*, 31 (4), 702-719.

Omand, D., Bartlett, J. y Miller, C. (2012). Introducing Social Media Intelligence. *Intelligence and National Security*, 27 (6), 801-823.

Omand, D. (2017). Social Media Intelligence. En R. Dover, H. Dylan y M. Goodman (Eds.), *The Palgrave Handbook of Security, Risk and Intelligence* (pp. 355-372). Springer.

Pallaris, C. (2008). Open source intelligence: A strategic enabler of national security. *CSS Analyses Secur Policy*, 3 (32), 1-3.

Privacy International (2020). *Is your local authority looking at your Facebook likes?* https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020_0.pdf

Policía Nacional, Escuela de Inteligencia y Contrainteligencia "Teniente Coronel Javier Antonio Uribe Uribe" (2022). Respuesta a solicitud de acceso a la información, radicado GS-2022-001408/DIREC-GUSAP-29.25.

Policía Nacional, Dirección de Investigación Criminal e Interpol (2021, agosto 24). Respuesta a solicitud de acceso a la información, radicado GS-2021-108176-DIJIN-CECIP 1.10.

_____ (2021, junio 30). Respuesta a solicitud de acceso a la información radicado GS-2021-DIJIN-CECIP-1.10.

Revista Semana (2020a, mayo 1). Las carpetas secretas. *Semana.com*. https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/

Revista Semana (2020b, enero 12). Chuzadas sin cuartel. *Semana.com*. https://www.semana.com/nacion/articulo/chuzadas-por-que-se-retiro-el-general-nicacio-martinez-del-ejercito/647810/

Scheinin, M. (2010, mayo 17). Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión, A/HRC/14/46, Consejo de Derechos Humanos, Naciones Unidas.

Steele, D. R. (2007). Open Source Intelligence. En L. K. Johnson (Ed.), *Handbook of Intelligence Studies* (pp. 129-147). Routledge.

Superintendencia de Industria y Comercio (2020). Radicación 20-423123, del 15 de diciembre.

_____ (2022). Radicación 22-212677, del 13 de julio.

La inteligencia estatal hace mucho que se trasladó a la internet y las redes sociales. Esto, por supuesto, representa riesgos adicionales al ejercicio del derecho a la privacidad en línea que ya enfrenta serios obstáculos por cuenta de prácticas nocivas que desempeñan otros actores.

En esta investigación ofrecemos una primera aproximación sobre dicha materia a través del caso de las "Carpetas Secretas" publicado en 2020 por la Revista Semana, que da cuenta de cómo la inteligencia colombiana explota las publicaciones en redes sociales, así como la información pública disponible en internet con la intención de monitorear y perfilar a las personas.

La aproximación que ofrece este texto advierte que los límites de la legislación son más bien exiguos, y que la autorregulación de las agencias de inteligencia es casi inexistente pese a demostrar, al tiempo, una mayor claridad sobre los datos en internet y redes sociales que les resultan de interés.

Nuestra propuesta parte por afirmar la importancia del derecho a la privacidad en el mundo digital incluso de cara al Estado. Creemos que, en la discusión sobre los límites deseables, las reflexiones que han surgido respecto al monitoreo pasivo del espectro electromagnético y la interceptación de las comunicaciones ofrecen lecciones valiosas con las cuales se podría abordar mejor el impacto de la inteligencia en línea.

Esperamos con esta publicación abrir la discusión sobre un tema cuyos retos éticos y legales merecen la atención de la comunidad de usuarios de la Red, así como de la comunidad jurídica.