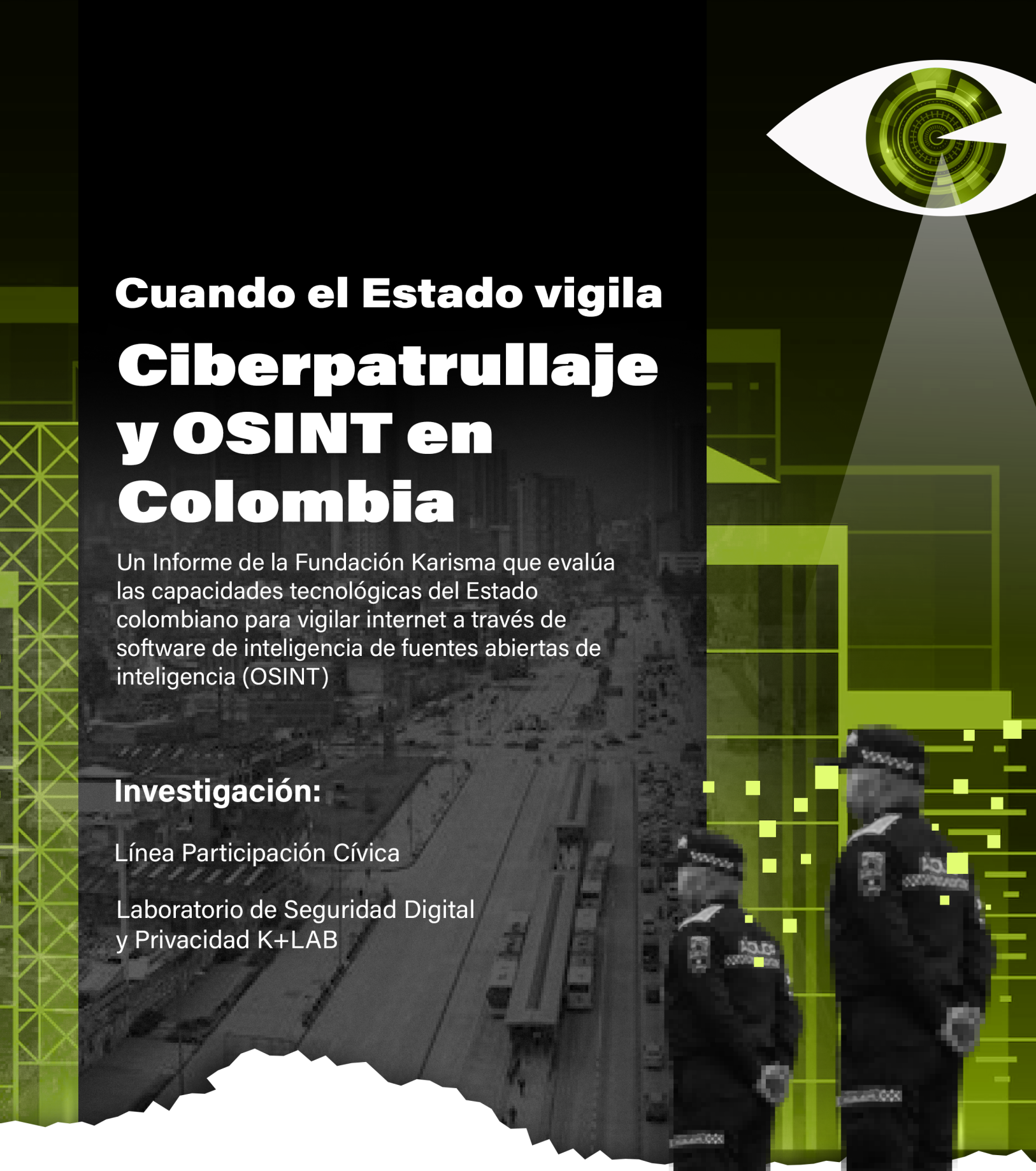
Cuando el Estado vigila

Ciberpatrullaje y OSINT en Colombia

Un Informe de la Fundación Karisma que evalúa las capacidades tecnológicas del Estado colombiano para vigilar internet a través de software de inteligencia de fuentes abiertas de inteligencia (OSINT)

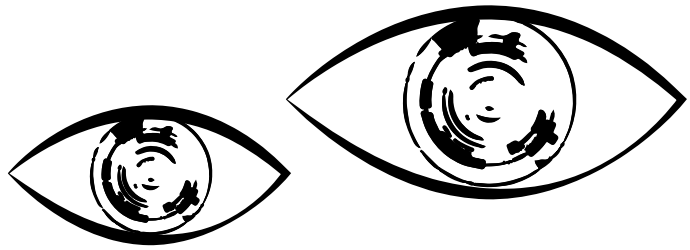


Investigación:

Línea Participación Cívica

Laboratorio de Seguridad Digital y Privacidad K+LAB

20 años Fundación Karisma



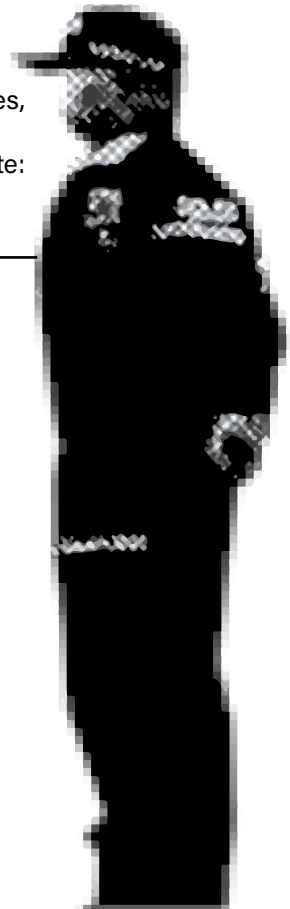
Bogotá, Colombia
Febrero de 2023

20 años Fundación Karisma

Investigación:
Línea de Partición Cívica
Laboratorio de Seguridad Digital y Privacidad (K+LAB)

Con el apoyo especial de Privacy International

PRIVACY INTERNATIONAL



En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema: http://www.documentoaccesible.com/#que-es.

fundacionkarismaa @Karisma karismacol

karisma.org.co

Tabla de contenido

Introducción y metodología

En 2021, durante el Paro Nacional, el Estado colombiano puso en marcha el Puesto de Mando Unificado de Ciberseguridad (PMU-Ciber). Este consistía en una mesa de cooperación entre varios organismos de seguridad que vigiló contenidos publicados por la ciudadanía en el marco de las manifestaciones[1]. El PMU-Ciber operó sin que estuviera clara su justificación legal y reglas de funcionamiento[2] y, más importante aún, no estaba claro qué hacía y cómo. La única certeza, según las declaraciones de sus integrantes, era que estaban realizando "ciberpatrullaje" en internet.

¿Pero qué es el ciberpatrullaje? o ¿qué hacían los organismos de seguridad del Estado cuando ciberpatrullaban? En 2021, cuando la inquietud surgió entre las organizaciones de la sociedad civil, no teníamos una respuesta clara[3], pero el Estado tampoco. Así quedó evidenciado en múltiples solicitudes de información pública realizadas desde Karisma y como resultado de una revisión de las leyes y normas nacionales aplicables al monitoreo de internet. Por ejemplo, el Ministerio de Defensa y el Centro Cibernético Policial, a pesar de que destinaron esfuerzos y espacios en sus sitios web para desmentir supuestas noticias falsas, hicieron gestión de amenazas cibernéticas y análisis de miles de videos para la identificación de responsables de "actos de vandalismo"[4], solo señalaron como sustento legal los principios constitucionales de colaboración y cooperación entre entidades públicas[5]. Normas que aplicaban a su participación del PMU-Ciber, pero no sobre su actuar en el mismo.

En últimas, a pesar de la ausencia de claridad conceptual o jurídica sobre qué era el ciberpatrullaje, en 2021 había indicios de que, para las autoridades colombianas, patrullar en la web significaba monitorear internet y lo que las personas hacían y decían allí.

Esta situación generó una importante pregunta: ¿Cuál era y es la capacidad real del Estado para monitorear internet? ¿Podría el Estado, por ejemplo, monitorear tendencias en Twitter o perfilar a una persona a partir de la información que encuentra en internet? ¿Puede hacerlo desde el anonimato? ¿Cómo puede eso afectar los derechos de las personas? Es decir, con qué herramientas técnicas cuenta para ello y qué pueden hacer los software en su poder, pues

1. Los jueces de la verdad, el mar de mentiras detrás del ciberpatrullaje del Estado. Fundación Para la Libertad de Prensa. Disponible en: https://www.youtube.com/watch?v=ljsr99Zy010
2. Poniéndoles el ojo a los PMU CIBER: qué son y para qué sirven. Carolina Botero y Juan Pablo Parra. Disponible en: https://www.lasillavacia.com/historias/historias-silla-llena/poniendoles-el-ojo-a-los-pmu-ciber-que-son-y-para-que-sirven/
3. Pistolas contra celulares. Fundación Karisma. Disponible en: https://web.karisma.org.co/pistolas-contra-celulares/
4. BALANCE GENERAL - PARO NACIONAL 2021. 28 de abril al 27 de junio de 2021 – Corte a las 23.59 HR. pg4. MinDefensa. Disponible en: https://web.karisma.org.co/pistolas-contra-celulares/ y INFORME DEL SECTOR DEFENSA GARANTÍAS A LA MANIFESTACIÓN PACÍFICA Y CONTROL DE ACCIONES VIOLENTAS. PERIODO 28 DE ABRIL A 4 DE JUNIO DE 2021 09 DE JUNIO, 2021 pg 87. Mindefensa. Disponible en: https://www.policia.gov.co/noticia/informe-sector-defensa
5. Más de 80 noticias falsas se han detectado durante el paro. Policía Nacional. Disponible en: https://www.policia.gov.co/noticia/mas-80-noticias-falsas-se-han-detectado-paro

dependiendo de la capacidad técnica, del tipo de software o de equipos, la incidencia sobre los derechos y libertades fundamentales puede variar de forma sustancial[6].

Para responder a la pregunta, Karisma planteó y desarrolló una investigación centrada en la tecnología que habían comprado los miembros del PMU-Ciber entre 2019 y 2022. En la primera fase, hicimos un rastreo de procesos de contratación mediante los cuales las autoridades del PMU adquirieron tecnologías que pudieran ser utilizadas para monitorear internet. En esta etapa se realizaron búsquedas de información en la página Colombia Licita[7] y dicha información fue verificada en las páginas oficiales de contratación SECOP I y 2. En total rastreamos 60 procesos de contratación relacionados con tecnologías. Posteriormente revisamos la descripción técnica presente en los contratos y sus anexos para analizar la naturaleza de los dispositivos y programas de cómputo relacionados en los procesos.

Paralelamente con el propósito de realizar un doble chequeo fueron enviados 10 derechos de petición a las siguientes entidades: Fiscalía General de la Nación, Ministerio de las TIC, Presidencia de la República, Policía Nacional, DIJIN, Ejército Nacional, Fuerza Aérea Colombiana, Comando General de las Fuerzas Militares, Dirección Nacional de Inteligencia y Ministerio de Defensa Nacional. Estas peticiones solicitaban información acerca de los procesos de contratación mediante los cuales cada entidad hubiera cotizado o adquirido, desde el 2019 hasta la agosto de 2022, tecnología (plataformas, hardware o software) que le permitiera llevar a cabo monitoreo de internet. Además preguntamos específicamente sobre el tratamiento de la eventual información monitoreada, del rol de las tecnologías en su participación en el PMU-Ciber y los criterios usados para el monitoreo en internet.

Aunque las solicitudes replicaban el lenguaje usado en los objetos de los contratos previamente encontrados, sólo tres entidades, la Fiscalía, la Fuerza Aérea y el Ministerio TIC remitieron una parte de su contratación (un contrato cada una). Mientras que, las demás (Presidencia, DIJIN, DNI, Ministerio de Defensa y Ejército) se negaron a hacerlo señalando que tras revisar los archivos físicos y digitales no encontraron en sus registros procesos relacionados con los objetos de la petición[8]. Esto a pesar de que, en casi todos los casos, Karisma ya había encontrado contratos para herramientas de este tipo en el tiempo determinado para la investigación.

En la segunda fase se realizó la construcción de un marco conceptual que se utilizaría para analizar los contratos previamente rastreados. Fue necesario buscar definiciones y establecer cómo funciona la tecnología para monitorear internet y proceder a clasificar las tecnologías según si en nuestro criterio corresponden a actividades de ciberpatrullaje.

---

6. En un informe de 2019, el relator para libertad de expresión de las Naciones Unidas, David Kaye, concluyó que aunque ese informe se detiene en tecnologías sofisticadas como las de reconocimiento facial o los spyware, sus conclusiones son generales y recuerdan que la responsabilidad compete tanto a los Estados como a las empresas que producen la tecnología. El informe invita a los Estados a tomar medidas a nivel nacional para controlar la adquisición, exportación y uso de estas tecnologías. Disponible en: https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance
7. Colombia lícita es un página privada que permite a interesados en participar en licitaciones con el Estado colombiano encontrar de forma fácil los procesos de selección. La página tiene una versión gratuita, que permite la búsqueda, pero no descarga información. Esta fue la opción usada por Karisma ante la falta de usabilidad de la página de SECOP donde no es fácil realizar búsquedas. Disponible en: https://colombialicita.com/
8. Respuesta Número GS-2022-103091-DIJIN-CECIP del 19 de agosto de 2022.

Además, para tener un entendimiento más completo del problema realizamos un barrido jurídico sobre normas aplicables a las actividades de monitoreo de internet y un rastreo sobre las declaraciones públicas (medios, prensa de entidades públicas y comunicados) respecto a ciberpatrullaje o monitoreo de internet, esto para entender con qué justificación, soporte jurídico o motivos se está usando la tecnología.

Finalmente, en la tercera fase, los contratos fueron analizados a nivel jurídico, determinando si la tecnología podría ser peligrosa para la ciudadanía si se usaba de forma abusiva y, lo más interesante, el laboratorio de seguridad digital y privacidad de Karisma, K+Lab, revisó las características técnicas de los equipos y software adquiridos, así como las empresas proveedores de la tecnología. Esto para saber si estas tecnologías podrían realizar más funciones que las pedidas en los contratos o si las metodologías y protocolos usados podrían lesionar derechos a niveles que la simple revisión del texto no permitía avisar.

Para mayor claridad, el informe se dividirá de la siguiente forma: primero, (i) explicaremos en qué consiste el ciberpatrullaje y el OSINT; en segundo lugar, (ii) explicaremos de forma general las capacidades del Estado colombiano para monitorear internet, a partir de la parte de la contratación que conocemos; en seguida, (iii) explicaremos las implicaciones de la capacidades no regulados del estado respecto al OSINT, para, finalmente, (iv) presentar recomendaciones sobre el tema al Estado.

Sección 1:
Técnicas de monitoreo en internet en Colombia. Ciberpatrullaje y OSINT

1.1 La construcción del concepto de ciberpatrullaje

El término ciberpatrullaje apareció por primera vez en el ordenamiento jurídico colombiano en la Resolución 05839/15 de la Policía Nacional[9]. Allí se estableció que una de las funciones del Centro Cibernético Policial o CAI virtual consiste en identificar, a través de acciones constantes en la web, amenazas en contra de la ciberseguridad ciudadana, y detectar factores comunes en los incidentes de ciberseguridad y en eventos en los que se vulnere la disponibilidad, integridad y confidencialidad de la información que circula en el ciberespacio[10]. Es decir, investigar posibles delitos informáticos.

Al respecto, empezamos por precisar que a pesar de que el ciberpatrullaje es una actividad que restringe derechos fundamentales, como toda investigación judicial o de inteligencia llevada a cabo por el Estado, en este caso no se cumple con los estándares internacionales que establecen que se debe regular las materias referentes a derechos humanos mediante una ley.

Ahora bien, según información oficial brindada por autoridades policiales en respuestas a derechos de petición radicados por la FLIP y Karisma, "las actividades de ciberpatrullaje comprenden la consulta, observación y recolección de información en línea sobre datos y contenidos abiertos y públicos en internet y redes sociales[11]". Además, en una declaración pública en 2021, el ex director de la policía, Jorge Luis Vargas, se refirió al asunto señalando que el ciberpatrullaje es como el patrullaje ordinario, pero llevado a cabo en internet[12].

Esta falta de una consagración legal de forma clara y precisa ha generado en la práctica dos escenarios preocupantes: el primero es que la Policía realiza actuaciones que llama ciberpatrullaje, aunque no se relacionan con la identificación de amenazas de ciberseguridad, como faculta la resolución; tal como sucedió durante el paro nacional en el que la Policía realizó otro tipo de actividades, como calificar publicaciones en internet como verdaderas o falsas cuando afirman realizar ciberpatrullaje y; el segundo, en el que autoridades distintas a la Policía, como el ejército, afirman realizar ciberpatrullaje, esto a pesar de que legalmente la resolución sólo hablaba del CAI virtual.

Algunos ejemplos de las actuaciones que fueron justificadas con las actividades de ciberpatrullaje son: 1) la caza de supuestas noticias falsas sobre el Covid-19 (a pesar de que de forma reiterada el Estado señaló que las noticias falsas no son ni un riesgo digital ni un

9. Resolución 05839/15 de la Policía Nacional. Disponible en: https://www.policia.gov.co/file/32305/download?token=0A0OIAOJ
10. Ley 1273 de 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
11. Inteligencia Estatal en Internet y Redes Sociales: el caso Colombiano de Dejusticia, pág. 31
12. ¿Qué es el ciberpatrullaje?. Revista semana. Disponible en: https://ne-np.facebook.com/RevistaSemana/videos/qu%C3%A9-es-el-ciberpatrullaje/438397297775230/?__so__=permalink&__rv__=related_videos

ciberdelito)[13], realizada mediante ciberpatrullaje en fuentes abiertas[14]; 2) El uso de herramientas tecnológicas para recolectar información en redes sociales y perfilar a personas en escándalos como el de las Carpetas Secretas del ejército[15] o 3) tachar de falsas denuncias ciudadanas sobre violaciones a derechos humanos durante el Paro Nacional de 2021, por supuesto, identificadas a través actividades de ciberpatrullaje en redes sociales[16] en un monitoreo de 21.000 horas[17].

En ausencia de controles adecuados las actividades que impliquen monitoreo de internet, como el ciberpatrullaje para investigar ciberdelitos, las búsquedas de la Fiscalía en virtud de la figura penal del agente encubierto virtual o las actividades no reguladas de recolección de información para inteligencia en internet, puede convertirse en un caso de vigilancia masiva desde el Estado a la ciudadanía. Según Amnistía Internacional, la vigilancia masiva en internet consiste en "el control de las comunicaciones de un gran número de personas -a veces de países enteros- sin que existan indicios suficientes de conducta delictiva. Este tipo de vigilancia no es legal[18]" , y parece ser lo que sucedió en los ejemplos citados.

No debe olvidarse, que la vigilancia de contenidos en internet por parte del Estado además genera el efecto chilling[19] o inhibitorio. Es decir, que la respuesta agresiva del Estado persuada a las personas de manifestarse libremente para evitar represalias, lo que sin duda representa un riesgo inminente de vulneración a la libertad de expresión en línea.

En últimas, el ciberpatrullaje es un concepto no delimitado, que remite de forma vaga a normas jurídicas poco detalladas y se sirve para justificar el monitoreo indiscriminado de internet por parte del Estado; falsamente escudado en fines legítimos como la lucha contra la ciberdelincuencia o las actividades de inteligencia para defender la democracia y los derechos humanos.

Muy por el contrario, ciberpatrullaje debería consistir únicamente en las actividades de investigación que permitan a la fuerza pública detectar posibles amenazas de ciberseguridad y cibercrímenes y delitos comunes, previamente delimitados en la ley, usando herramientas de búsqueda, análisis, tratamiento y presentación de la información procedente de fuentes abiertas (OSINT).

Dichas facultades de investigación deben aparecer en una ley formal, contar con un análisis de impacto en derechos humanos, tener controles claros dentro del gobierno y mecanismos de

13. Respuesta Número GS-2021-099094-DIJIN del 03/08/2021
14. Reporte de noticias falsas detectadas por CAI Virtual. Policía Nacional. Disponible en: https://www.policia.gov.co/reporte-fakenews
15. Las Carpetas Secretas. Semana. Disponible en: https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/
16. BALANCE GENERAL - PARO NACIONAL 2021 28 de abril al 27 de junio de 2021 – Corte a las 23.59 HR. Min Defensa. Disponible en: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios_sectoriales/info_estadistica/InformeCorrido_Balance_Paro_2021.pdf
17. 21.647 horas vigilando internet: el ciberpatrullaje en 36 días del paro. Carolina Botero. Disponible en: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/21647-horas-vigilando-internet-el-ciberpatrullaje-en-36-dias-del-paro/
18. Vigilancia Masiva en Internet. Amnistía Internacional. Disponible en: https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/
19. El chill de la censura en Colombia. Revista 070. Disponible en: https://cerosetenta.uniandes.edu.co/el-chill-de-la-censura-en-colombia/

seguimiento por la ciudadanía. Además, estas tecnologías -como cualquiera que hace vigilancia de la ciudadanía- requieren de mecanismos de control del gasto, una política de transparencia respecto de la finalidad y los métodos usados y debe contar con acciones de reparación para las víctimas cuando hay abuso en su uso. Esperamos que próximamente sea así.

1.2 Qué es OSINT y su relación con el ciberpatrullaje.

El OSINT, Open Source INTelligence o Inteligencia de Fuentes Abiertas, consiste en una serie de técnicas para recolectar y analizar datos que se encuentren alojados en fuentes de información de libre acceso con fines ofensivos o defensivos[20]. El OSINT puede realizarse de forma manual o automatizada, tanto en fuentes físicas como digitales, pero en la actualidad, suele realizarse mediante software aplicados a la web, los cuales extraen y descargan información de fuentes públicas, como las páginas de medios, blogs, foros, redes sociales, bases de datos, entre otras.

Es usual que las herramientas de software OSINT tengan la capacidad de obtener y recolectar información utilizando técnicas de scrapping, lo que implica que la cantidad de información que pueden procesar es muy grande. El scrapping consiste en la extracción de datos de un sitio web, de forma automatizada e indiscriminada, mediante software que descarga toda la información de una página web, usando los vínculos que las mismas proveen.

El OSINT es una variante del Open source research o investigación basada en una búsqueda de información disponible en fuentes públicas, bases de datos o medios de comunicación, que se realiza con fines académicos, periodísticos o en investigaciones judiciales. Pero en el caso de la inteligencia de fuentes abiertas, el análisis de la información recolectada sirve en la planeación, coordinación o ejecución de planes que permitan conseguir ventajas, adelantándose a los competidores de determinado sector (ofensiva) o para resistir o rechazar una agresión (defensiva) respecto de quien se considera un competidor, opositor o enemigo.

Ahora bien, las herramientas OSINT aplicadas a internet son la base técnica de lo que en Colombia se ha llamado ciberpatrullaje. Ya que son estas herramientas las que hacen posible un monitoreo en tiempo real de la web y porque, como lo mostramos más adelante, cuando el estado pretende monitorear internet adquiere herramientas OSINT. Un ejemplo claro de ello es el contrato firmado el 30 de diciembre de 2019, entre la DIJIN y la empresa Deinteko SAS, con objetivo de permitir el "acceso a plataformas de fuentes abiertas para ciberpatrullaje"[21].

Es por la relación integral entre ciberpatrullaje y las técnicas OSINT, siendo, el primero, el nombre usado en la normativa[22] y en las declaraciones públicas del Estado[23] y, el segundo, la técnica que la facilita o las herramientas que el Estado compra para hacer el ciberpatrullaje. En consecuencia, el análisis de Karismas sobre las capacidades del Estado para monitorear internet o hacer ciberpatrullaje esta vez se centró en las herramientas OSINT compradas por las

20. Información y Blog sobre OSINT. Disponible en: https://odint.net/osint/
21. Búsquese en SECOP II, ingresando a la pestaña de búsqueda de procesos de contratación. Elimine los datos de fecha del formato e ingrese en la casilla de número del proceso: PN DIJIN SA MC 029 DE 2019.
22. Resolución 5839 de 2015
23. ¿Qué es el ciberpatrullaje?. Revista semana. Disponible en: https://ne-np.facebook.com/RevistaSemana/videos/qu%C3%A9-es-el-ciberpatrullaje/438397297775230/?so=permalink&rv__=related_videos

entidades del PMU-Ciber durante el paro de 2021.

Sección 2.
El OSINT explicado desde las herramientas tecnológicas

Karisma rastreó y analizó los procesos de contratación relacionados con OSINT, entre 2019 y 2022, de las entidades que hicieron parte del PMU-Ciber que operó durante el Paro Nacional de 2021. Es decir, los contratos que celebraron: Presidencia de la República, Ministerio de Defensa (MinDefensa), Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), Policía Nacional, Fiscalía General de la Nación, Fuerzas Militares (CCOCI) y la Dirección Nacional de Inteligencia (DNI).

De estas entidades, hay tres de las cuales no encontramos ningún contrato relacionado con OSINT: el DNI, la presidencia y el Mintic. Esto no significa que las entidades no cuenten con este tipo de herramientas, sino que con las herramientas que contaba Karisma: Secop, Colombia Licita y solicitudes de información, no tuvimos acceso a la contratación de esta entidad.

Respecto de la DNI resulta extraño que siendo esta entidad la encargada de los asuntos de inteligencia y cont rainteligencia no cuente con herramientas OSINT. Seguramente resulta más creíble qué dada la alta opacidad del Estado colombiano en relación con las actividades de inteligencia, los contratos de adquisición de OSINT de la DNI no se hayan subido al SECOP argumentando reserva por seguridad nacional[24]. Otro indicio de que la DNI sí tiene herramientas OSINT apareció recientemente en el Leak del Ejército realizado por Guacamayas y en el que, según El Espectador, se referencia que la empresa Mollitiam ha contratado este tipo de sistemas con la DNI[25].

24. Respecto de la DNI encontramos un único contrato un contrato del 2013, previo al periodo de análisis y razón por la cual no lo incluímos en el cuerpo del texto. Sin embargo, señalamos que el mismo tenía por objeto el monitoreo de medios nacionales y regionales y se celebró con la empresa, Mediciones y Medios SAS, una empresa de ingeniería de datos, "especializada en mercados, medios y opinión pública" y que señala en su página oficial tener monitoreados: 518 emisoras regionales, 53 impresos nacionales, 27 canales "capturados" y haber visitado 4.500 sitios web.
La metodología del servicio que ofrece Mymcol consiste en recoger y almacenar la información disponible en medios de comunicación y de redes sociales, blogs o sitios web. Una vez hecho esto, clasifican y analizan la información recogida, según los parámetros establecidos en conjunto con sus clientes, para obtener los datos relevantes y medir el impacto en la opinión pública de cada uno de los hechos noticiosos o relevantes de la actualidad.
Si bien, la metodología de Mymcol remite al funcionamiento de tecnologías OSINT, pues usa datos de fuentes de información abiertas para conseguir una ventaja en la generación de discusión pública, persé esto no implica una violación de derechos, pues no se cataloga, perfila o vigila a la ciudadanía, sino se recolecta información con fines comunicacionales para el Estado.
25. Mollitiam: así es la contratista del Ejército y sus herramientas de ciberespionaje. Disponible en: https://www.elespectador.com/judicial/mollitiam-asi-es-la-contratista-del-ejercito-y-sus-herramientas-de-ciberespionaje/

Respecto de la presidencia, si bien se encontró un contrato con la empresa Alotrópico[26], la cual diseñó usando OSINT la campaña #ColombiaEsMiVerdad, los documentos del mismo no evidencian que se usara esta tecnología contra la ciudadanía[27]. En el caso de MinTic solo se encontraron contratos para adquirir servicios de ciberseguridad interna o para dar capacidades al CSIRT nacional.

Ahora bien, respecto al resto de las entidades que formaron el PMU-Ciber sí encontramos contratos de adquisición de sistemas OSINT de forma directa. A continuación y a partir de un análisis de cinco contratos, les presentamos de forma general las capacidades de monitoreo de internet del Estado colombiano a través de sistemas OSINT. La explicación se realizará a partir de las capacidades técnicas del Estado y las mismas se ejemplifican, dentro de los recuadros que aparecerán a continuación, con la referencia al contrato correspondiente. Si está interesado en conocer el detalle de cada compra, lo invitamos a revisar el Anexo Contratos de herramientas OSINT en Colombia.

Entidad	Número del proceso	Fecha	Contratista	Objeto	Costo
Comando Conjunto Cibernético	124COGFM 2020	31/03/2020	Desarrollo e Integración de Tecnología y Comunicaciones S.A.S. (Deinteko SAS)	Desarrollo e Integración de Tecnología y Comunicaciones S.A.S. (Deinteko SAS)	$398.199.000, 00
DIJIN	PN DIJIN SA MC 029 DE 2019	30/12/2019	Desarrollo e Integración de Tecnología y Comunicaciones S.A.S. (Deinteko SAS)	Acceso a plataforma de fuentes abiertas para el ciberpatrullaje	$ 3.990.903.550,00
Ejército Nacional	325-DIADQ-CAD-CO-CENACINTE-LIGENCIA-2016	12/09/2016	Gamma Ingenieros SAS	Adquisición de equipo de inteligencia con ampliación de licencia y arquitectura de hardware para el sistema de fuentes abiertas	$ 370.000.00,00

26. Búsquese en SECOP II, ingresando a la pestaña de búsqueda de procesos de contratación. Elimine los datos de fecha del formato e ingrese en la casilla de número del proceso: 234-2022-MDN-UGG-DA

27. Con el contrato con Alotrópico, Mindefensa adquirió un servicio para posicionar su ”marca” que usa herramientas de OSINT para actividades con marketing como los son análisis de percepción, detectar crisis de imagen en las redes sociales, identificar actores importantes o aliados en esta estrategia de comunicación, sobre todo si consideramos que esta empresa fue la que desarrolló para este ministerio la estrategía de “Colombia es mi verdad” durante el Paro Nacional.
Ese antecedente de 2021 entre MinDefensa y Alotrópico, fue referenciado por la Corte Interamericana de Derechos Humanos como problemático. Para esta entidad categorizar publicaciones de la ciudadanía y tomarse atribuciones de juez de la verdad, son peligrosos para la democracia, si bien del texto del contrato no se deriva que se realizarán este tipo de actuaciones, este antecedente contribuye a un ambiente de falta de confianza en el uso que las herramienta de OSINT en manos de las autoridades.

Policía Nacional	PN DIPOL SA MC 027-2021	22/07/2021	Unión Temporal Phoenix027-2021	Sistema de ciberinteligencia basado en inteligencia artificial	$4.291.887.417, 98
Fiscalía General de la Nación	FGN-NC-CD-0016-2022	26/01/2022	Desarrollo e Integración de Tecnología y Comunicaciones S.A.S. (Deinteko SAS)	Actualización licencia de plataforma Tangles	$ 1.087.858.666, 00

Cuadro 1. Resumen contratación de software OSINT por entidades parte del PMU-Ciber durante el Paro Nacional

2.1 Monitoreo masivo y perfilamiento a partir de fuentes abiertas

Cuando el OSINT que contrata el Estado está diseñado para hacer barridos en páginas web, redes sociales, foros e incluso grupos de chat con el fin de extraer información sobre temas, personas, organizaciones o movimientos que, de alguna manera, sean del interés de las entidades contratantes, nos encontramos ante el uso de OSINT para monitorear masivamente las actividades en la red o para perfilar a las personas.

Es importante empezar dejando claro que, aunque las autoridades intenten justificar estas compras con propósitos legítimos (como la búsqueda de amenazas, la lucha contra la criminalidad o las investigaciones judiciales), las capacidades de estas herramientas normalmente afectan varios derechos fundamentales de la mayoría de las personas usuarias de internet (especialmente la privacidad, la libertad de expresión, la libertad de asociación o la participación política), aún si se usan con controles y de forma proporcional.

Hablamos de software capaces de barrer una porción suficiente de la web para recolectar y procesar información de miles de personas, aún sin que exista un motivo legítimo para ello (monitoreo masivo) o que pueden recolectar datos de forma precisa para crear perfiles de sujetos concretos (perfilamiento).

La búsqueda de amenazas del Comando Conjunto Cibernético (ver Anexo. Punto 1)

Con la justificación de buscar amenazas digitales en la Darknet, el Comando Conjunto Cibernético (CCOCI) contrató acceso a una de las plataformas ofertadas por la empresa isrelí, Sixgill, a través de su representante en Colombia: Deinteko. Esta plataforma que se anuncia como una herramienta de rastreo e infiltración de grupos criminales en la Dark Web, no solo opera como un detector de amenazas, sino que tiene capacidades de monitoreo masivo en los lugares más comunes de la web y de aplicaciones de mensajería instantánea. Esto hace que el alcance de los productos de Sixgill sirvan -como otros sistemas de OSINT- para hacer perfilamientos y monitoreo de temas, grupos o personas que no necesariamente encajan en el conjunto de sitios conocidos como la Darknet.

De hecho, el término Darknet, explotado ampliamente en el marketing de Sixgill es solo una de las funcionalidades de los sistemas que venden y se parece a lo que hacen otros sistemas similares. Sin embargo, explotar este término -de difícil definición- hace que a primera vista el sistema no parezca un sistema de vigilancia masiva y sea más fácil de justificar por los clientes de esta compañía, especialmente por sus clientes estatales.

El CCOCI es principalmente una entidad generadora de política pública cuyas funciones están relacionadas con asesorar al presidente, preparar documentos sobre seguridad nacional y desarrollar políticas, adicionalmente ejerce el mando estratégico en las operaciones militares de las tres ramas de la fuerza pública. En la justificación del contrato firmado con Deinteko SAS se habla que su propósito es combatir ataques cibernéticos que afecten los "valores e intereses nacionales", sin precisar el sustento normativo.

El uso de términos abiertos como valores o intereses nacionales, sumado a que el CCOCI, no tiene funciones investigativas, genera dudas respecto de quién usa este software que le permite el perfilamiento en redes sociales sin control alguno, los fines de su uso o qué implica esto para la ciudadanía. La incertidumbre deja abierta la pregunta si la información íntima en redes sociales está siendo usada en operaciones militares.

¿Cómo funcionan en la práctica estas herramientas? acá les explicamos las generalidades que permiten entender los contratos que presentamos más adelante:

2.1.1 Crawlers. Búsquedas, indexación y etiquetamiento automatizado de contenido en la web

En la base de los sistemas de OSINT están los populares crawlers que son, básicamente, programas que navegan internet automáticamente siguiendo los enlaces que tiene cada

página para luego ser indexados, guardados y/o etiquetados. Esto no es nada diferente a lo que usa Google o Bing para crear sus buscadores. Sin embargo, en el caso de los sistemas de OSINT, el resultado no es un catálogo de información que las personas pueden consultar, sino que la indexación resultante de la lectura que hacen los crawlers -el análisis semántico de lo que recoge-, su clasificación y priorización genera alertas sobre temas que han definido sus operadores.

Es difícil definir el alcance de un crawler ya que normalmente, la idea es que vaya lo más profundo posible en los enlaces que encuentra. Es decir, cuando un crawler lee una página no solo extrae todo su contenido, sino que toma cada enlace en esa página y lo lee, repitiendo el proceso enlace, tras enlace, tras enlace.

A diferencia de los crawlers de los buscadores normales de internet, los crawlers de los sistemas OSINT normalmente utilizan cuentas falsas para acceder a información dentro de comunidades cerradas como grupos de Facebook o, por ejemplo, los datos de una cuenta de Twitter que sólo serían visibles a otro usuario de la plataforma. De esta manera, la información recolectada por estas herramientas de OSINT no se limita a lo meramente público sino que, incluso, infringiendo términos y condiciones de algunas plataformas, recolectan información masiva que se convierte en la materia prima de este proceso de vigilancia.

Acceso a plataforma OSINT de la DIJIN (ver Anexo. Punto 2)

El OSINT es una disciplina que comprende innumerables técnicas que pueden ser muy útiles en el desarrollo de investigaciones judiciales; sin necesidad de ejercer vigilancia masiva. Sin embargo, las características del software contratado por la DIJIN afecta la privacidad de personas que no están dentro de esas investigaciones.

La capacitación de funcionarios públicos en técnicas no invasivas de la privacidad de los y las ciudadanas no vinculadas con las investigaciones es la clave para un uso proporcional de las técnicas y herramientas de OSINT.

La DIJIN menciona la Resolución 05839/15 como soporte para la adquisición de OSINT y su capacidad para la recolección masiva de información de personas de forma anónima por parte del Estado, su vigilancia y geolocalización mucho más allá de la investigación de ciberdelitos que es lo que corresponde a la mencionada resolución. De la lectura del contrato habría que deducir que la DIJIN adquirió una herramienta que permite la vigilancia para la investigación criminal pero, no es posible saber si la forma como se usa viola el debido proceso (en ningún momento se habla de control por parte de un juez).

No podemos dejar de mencionar que El sistema de OSINT contratado por la DIJIN vulnera los términos y condiciones de las políticas comunitarias de las plataformas ya que entre las características se solicita la creación de cuentas falsas (en masa) que deben "parecer humanas" para evadir los monitoreos que hace el sistema. Las plataformas monitorean activamente sus redes para evitar los bots que no tienen

comportamiento humano, la creación masiva de cuentas falsas puede suponer la creación de estrategias coordinadas con comportamientos artificiales que pueden engañar al algoritmo y que tienen consecuencias en temas como la desinformación. Que el contrato tenga esta disposición significa que intencionalmente quiere evadir este tipo de controles.

En el contrato con la DIJIN[28] -Dirección de Investigación Criminal e INTERPOL- se establece que la plataforma contratada debe permitir hacer búsquedas anónimas y se especifica que cuando se use esta funcionalidad no deben generarse registros de la misma. Para poder cumplir con las especificaciones contractuales sobre anonimato lo más probable es que la DIJIN esté usando perfiles falsos que permitirían el ingreso a enlaces privados (como grupos en Facebook o perfiles con información oculta) con el fin de poder recoger información también en ellos y que éstos sean eliminados una vez se termine la búsqueda y la información sea descargada.

En el caso del monitoreo de canales de chat en sistemas de mensajería instantánea, la palabra adecuada no sería crawler, sino bot: un programa que se conecta automáticamente a canales de chat que monitorea y graba todas las conversaciones que allí suceden para igualmente indexarlas y etiquetarlas para su posterior análisis.

En el caso de las aplicaciones de OSINT que aquí nos conciernen, este proceso normalmente baja toda la información a la que se accede guardando textos, imágenes, videos o metadatos en un proceso denominado scrapping.

2.1.2 Alertas. Monitoreo constante

La idea central del OSINT es que toda la información recolectada por los crawlers o bots en el scrapping pueda ser clasificada, ya sea por un motor de análisis semántico que pueda medir el sentimiento de una publicación (como rabia o ironía), o por las etiquetas que la acompañan de tal forma que se puedan extraer temas de interés para los operarios de la herramienta, quiénes escogen los temas a priorizar.

En la mayoría de los casos, los criterios para disparar estas alertas son definidos por los operarios del sistema y su exactitud depende de la cantidad de información recolectada. El incentivo está en recolectar la mayor cantidad de información posible para tener un mapeo de lo que habla la ciudadanía en internet. De forma tal que, una herramienta OSINT con sistemas de alerta contínua, implica una vigilancia masiva a la personas que utilizan internet tanto por el Estado como por empresas privadas.

El seguimiento de un hashtag o de una mención a una cuenta específica afecta a todas las personas que interactúen con estos pedazos de información y su vigilancia está garantizada también por la industria del OSINT.

28. Véase en el anexo punto 2, página 3. Para más información del contrato búsquese en SECOP II, ingresando a la pestaña de búsqueda de procesos de contratación. Elimine los datos de fecha del formato e ingrese en la casilla de número del proceso: PN DIJIN SA MC 029 DE 2019.

¿El Ejército Nacional fortalece sus capacidades para la ciberguerra? (Anexo. Punto 3)

En un contrato del 2016, a través la compañía Gamma Ingenieros, el Ejercito Nacional[29] adquirió software de OSINT producido por la compañía española 4IQ (hoy conocida como Constella Intelligence). Por sus capacidades podemos deducir que está en la misma línea de los que ya hemos mencionado previamente. Pero en este caso, llama la atención las justificaciones del Ejército para comprar y el marketing de Constella Intelligence para vender su producto.

En la Resolución No 243 de 2016 de la Central Administrativa y Contable Especializada de Inteligencia se menciona como justificación para la solicitud de reserva que la herramienta de OSINT tiene como fin "fortalecer las capacidades de guerra electrónica del ejército nacional"[30], esto a pesar de que se añade que la herramienta será aplicada a la ciudadanía y se solicita expresamente que se haga reservada la motivación[31]. Más adelante, en los Estudios Previos publicados en SECIP, la motivación varió y se refiere a "averiguar lo que las personas están diciendo", proporcionando a la fuerza información adicional en caso de un suceso que las relacione, para "saber quienes están hablando de la institución y los hechos que las rodean"[32]. Así como reaccionar rápidamente a crisis sociales y hechos dañinos, monitorear fuentes consideradas "competencia o el enemigo", saber qué información del medio se publica y cómo están siendo percibidos. Además de que se menciona como un antecedente, en la sección de aspectos generales del mercado de los Estudios Previos, la filtración de datos de inteligencia estadounidense realizada por Edward Snowden, acusándola de revelar datos de la lucha contra el terrorismo e ignorando su valor como denuncia y elemento periodístico.

Constella Intelligence, por su parte, ofrece los productos Dome y Hunter como herramientas para realizar Monitoreo de Inteligencia Geopolítica. La descripción de los productos en su sitio web se acompaña con imágenes de protesta social y párrafos en donde el ejercicio de este derecho se referencia como un problema que puede dañar la reputación de una marca. Esto hace que la ya problemática justificación de un sistema de este tipo como una herramienta de manejo de imagen sea aún más problemática pues se asocia, por parte del Estado, con capacidades de guerra electrónica.

La adquisición del ejército tiene como claro objetivo vigilar a las personas que ejercen su derecho a la protesta o expresan su opinión a través de medios digitales, a quienes ven como "enemigos". Además, como dentro de los requerimientos técnicos se

29. Proceso Número: 325-DIADQ-CADCO-CENACINTELIGENCIA-2016.
30. Resolución No 243 de 2016 de la Central Administrativa y Contable Especializada de Inteligencia.
31. Proyecto OSINT: cómo la inteligencia militar se acerca a la vigilancia masiva. El Espectador. Disponible en: https://www.elespectador.com/judicial/proyecto-osint-como-la-inteligencia-militar-se-acerca-a-la-vigilancia-masiva/
32. ESTUDIO PREVIO PARA EL PROCESO DE SELECCIÓN CONTRATACIÓN DIRECTA No. 325-DIADQ CADCO-CENACINTELIGENCIA-2016, EL CUAL TIENE POR OBJETO LA "ADQUISICIÓN DE EQUIPO DE INTELIGENCIA CON AMPLIACION DE LICENCIAMIENTO Y ARQUITECTURA DE HARDWARE PARA EL SISTEMA DE FUENTES ABIERTAS DEL EJÉRCITO NACIONAL". Del la CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA "CENAC" INTELIGENCIA - 6 de diciembre de 2016.

menciona, por ejemplo, que "el proveedor se compromete a garantizar la visualización geográfica en mapas para el análisis de tendencias de objetos en redes sociales"

las dudas aumentan porque, aunque es improbable que el software sea capaz de identificar con precisión la ubicación de cada persona que genera estas tendencias, pero de acuerdo con la descripción de las herramientas ofrecidas por Constella, se podrían generar mapas del uso de ciertos términos sobre zonas geográficas amplias, como mapas de calor ¿Exactamente cuáles son los usos que le da el ejército "en tiempo real" a estas capacidades?, no lo sabemos.

Tanto el cliente como el proveedor están contratando armas tácticas justificando que estas sean apuntadas hacia la población civil. A pesar de que todas las herramientas OSINT contratadas por el Estado colombiano tienen características similares, es muy preocupante que el Ejército compre precisamente una herramienta que se anuncia para monitorear la opinión de la ciudadanía y responder a eventos sociales (protesta) como si estuviera en guerra contra ellos.

Este contrato está claramente destinado a vigilar a la sociedad civil. Así se infiere de la justificación que busca monitorear la opinión pública sobre el ejército, responder a crisis sociales (como el caso de una protesta social), así como encontrar trinos que consideren falsos, publicados por el "enemigo", refiriéndose con este apelativo a personas usuarias de internet.

2.1.3 Identificación de Actores y perfilamientos

Ahora bien, una vez el sistema ha sido configurado para buscar información específica, el siguiente paso es identificar los actores principales que disparan las alertas del sistema o que preocupan a los operadores (Estado).

Usando las mismas técnicas descritas anteriormente, es posible apuntar a un perfil específico y nuevamente, bajar, clasificar y etiquetar toda la información relacionada con el mismo. El cruce de toda esta información puede revelar mucha información personal, calcular por varios medios su ubicación e incluso des-anonimizar perfiles anónimos en las redes sociales o grupos de chat. Además es posible hacer mapas o grafos sociales de las persona perfiladas, no solo afectando la privacidad de quien es investigado, sino de todas las personas a su alrededor: familia, amigos, socios, etc.

Al final todo se trata de esto, identificar actores. ¿Quiénes son? ¿Dónde viven? ¿Con quién se relacionan? ¿Cuáles son sus opiniones? ¿Qué dicen? ¿A qué horas? ¿Cuál es su reputación o credibilidad?

La Policía y la Unión Temporal Phoenix (ver Anexo. Punto 5)

La unión temporal conformada por Newsat S.A.S y la conocida compañía española de productos para la vigilancia en internet, Mollitiam Industries, fue la encargada de instalar y desarrollar para la policía un sistema que describen los contratistas en su anexo técnico de esta manera:

> *"PHOENIX es un sistema de **monitoreo masivo en Internet** para generar inteligencia a partir de la descarga anónima de datos provenientes de Redes Sociales, Darknets y otras fuentes abiertas o cerradas que se integren."*

Con un poco más de crudeza que sus contrapartes en otras instituciones estatales, Phoenix explica en detalle cómo su sistema mina datos de internet constantemente, alerta, perfila o busca nuevos actores. También a diferencia de sus contrapartes, este sistema es controlado completamente por la policía en sus propios servidores y no se limita sólo a información pública, pues pueden usar bases de datos en su poder.

De acuerdo con la información del contrato de la Policía Nacional[33] el software sería capaz, por ejemplo, de revisar el hashtag "#ParoNacional", en varias redes sociales, e identificar actores importantes, interacciones y catalogar los mismos. Catalogados podría definir grupos y perfilarlos: quiénes son, qué hacen, dónde viven, en qué eventos quieren participar. Y este proceso se puede repetir con cada persona que se manifieste de forma digital. El nivel de precisión con que esto se logre puede ser cuestionable, pero la posibilidad de que se haga masivamente y con base en estos procesos se tomen decisiones de vigilancia de las personas que son "sospechosas" de protestar, es muy preocupante y alimenta la desconfianza respecto del Estado.

2.1.4 Búsquedas anónimas. La práctica del Agente Secreto Virtual

Normalmente las herramientas OSINT no se limitan a la mera observación pasiva de lo que sucede en internet, sino que, pensadas para los cuerpos de seguridad e investigación (estatales o no) brindan herramientas que permiten a un operador crear identidades falsas por lotes o esconder las interacciones que tengan los operadores con los portales de internet a través de sistemas de anonimización como proxies o VPNs.

33. Véase en el anexo, punto 5, página 17. Para encontrar el proceso de contratación búsquese en SECOP II, ingresando a la pestaña de búsqueda de procesos de contratación. Elimine los datos de fecha del formato e ingrese en la casilla de número del proceso: PN DIPOL SA MC 027-2021.

Además, la funcionalidad para operar anónimos en internet con varias cuentas que simulan ser humanas les facilita penetrar círculos más cerrados que el sistema por sí solo no puede alcanzar.

Hacer amigos o seguidores que permitan un monitoreo más preciso de un perfil objetivo es otra capacidad invaluable en el perfilamiento de personas, grupos u organizaciones que sean objeto de la vigilancia.

> En contratos como el de la Policía con la Unión Temporal Phoenix, la creación y administración de cuentas falsas puede ser tan masiva que aparenta tener además, la intención de hacer operaciones de influencia.

De cualquier forma, el trabajo manual que se puede hacer con la información que brindan estos sistemas requiere formación en otras técnicas, también de OSINT, para que los perfilamientos y la infiltración sea más precisa. En consecuencia, la industria ofrece o incluye capacitaciones para que los funcionarios utilicen de forma más eficiente el OSINT.

OSINT PRO, Agente encubierto en medios de comunicación virtual (ver Anexo. Punto 4)

La Fiscalía General de la Nación en un contrato de 2022 actualiza las licencias de su software de OSINT Tangle al que le adiciona un módulo de Dark Web -que para soluciones más modernas viene casi por defecto-. El contratista es la empresa Cobwebs, intermediada por la omnipresente Deinteko S.A.S.

La Fiscalía tiene, además, un segundo contrato en el que se adquiere un curso con el particular nombre de: "OSINT PRO, Agente encubierto en medios de comunicación virtual" para enseñar a los agentes de esa entidad técnicas de búsqueda o anonimización en internet que puedan complementar los resultados obtenidos con Tangle. El curso se justifica con el artículo 242B del Código Procesal Penal, sobre agentes encubiertos en medios virtuales, pero no se señala en el contrato las limitantes que la ley consagra al respecto de la facultad de los fiscales.

Por básicas que parezcan las técnicas enseñadas en los cursos OSINT, estas hacen parte del concepto de inteligencia en fuentes abiertas, el cual combina procesos automatizados con otros más manuales de forma tal que permitan armar las investigaciones.

Además, en la respuesta de la Fiscalía a la solicitud de información sobre contratos OSINT en su poder enviada desde Karisma, no se responde a las preguntas sobre el cumplimiento de las garantías legales que nos permitan entender cómo se usa la herramienta en el marco de sus competencias. Karisma no tiene conocimiento si el Tangle de la Fiscalía solo se usa con las autorizaciones previas señaladas en la ley y solo para casos de hechos cometidos por organizaciones criminales. La Fiscalía debe contar con facultades investigativas suficientes para combatir el delito y la impunidad, pero siempre se debe respetar los derechos fundamentales y garantías de los investigados.

2.1.5 ¿Contratar el servicio o desarrollar capacidad interna?

Las capacidades que brinda el procesamiento de grandes cantidades de datos con el fin de vigilar y perfilar, a la vuelta de un clic, requiere un gran poder de computación y capacidades técnicas especiales.

En los contratos estudiados para este informe es notable que la mayoría de entidades prefieren contratar soluciones As A Service, es decir, plataformas en internet que hacen toda la carga pesada y a la cual los operadores acceden a través de una página web en internet. Esto implica que toda la información, consultas, alertas o perfilamientos hechos por dichas entidades se encuentran en servidores extranjeros de entidades privadas con todo lo que esto implica tanto para la seguridad de las personas monitoreadas, como para la seguridad de la misma entidad que contrata el servicio.

Por otro lado, como queda claro sobre todo en el contrato de la Policía, la otra modalidad de contratación implica que toda toda la infraestructura del sistema quede en los mismos servidores de la entidad contratante. Esto permite desarrollos mucho más personalizados y que no tienen que limitarse a las fuentes abiertas, sino que toda la información recolectada, puede cruzarse con información interna apalancando aún más el poder de vigilancia y perfilamiento del sistema.

Es decir, cada modalidad de contratación tiene riesgos diferentes que deberían estar siendo analizados también a la luz de su impacto en derechos.

2.2. Monitoreo y manejo de marca con fuentes abiertas.

Aunque con motivaciones distintas a las del software de OSINT vendido en el contexto de la inteligencia, la seguridad, la vigilancia y la investigación criminal, estas mismas técnicas y herramientas con frecuencia son parte también del manejo de la imagen de marcas, compañías, organizaciones, personas o estados.

Quienes contratan estos servicios buscan entender qué se dice de ellos en internet y de acuerdo con la información recolectada enfocan sus esfuerzos reputacionales, publicitarios o propagandísticos. Es común que estos servicios incluyan cierta inteligencia que le permite al contratante o a la misma empresa de manejo de imagen reaccionar ante situaciones adversas o potenciales escándalos que se estén gestando en Internet. La preocupación es que si sirve para una cosa, también sirve para otras: tanto vigilar, como promover políticas.

El contrato del Ejército (Anexo. Punto 3) también en esto es atípico pues expresamente se refiere a que el mismo software justifica tanto el manejo de la marca como el propósito de aumentar capacidades de guerra electrónica. Pero con mayor frecuencia, los contratos se refieren a lo primero, siendo entonces un contrato aparentemente inofensivo que, sin embargo, encierra una capacidad de vigilancia preocupante.

Dentro de los contratos de publicidad que incluyen la utilización de técnicas OSINT, aparentemente inofensivos pero con capacidades de vigilancia, Karisma encontró un contrato del año 2022 celebrado por el MinDefensa con Alotrópico SAS[34]. Con el objetivo de ayudar a fortalecer una campaña para que la ciudadanía entienda de mejor forma "los temas relacionados con la defensa y seguridad nacional" y con la idea de tener una comunicación asertiva y escucha activa con los ciudadanos. Mindefensa buscaba posicionar su "marca" y utilizando estrategias como análisis de percepción, detectar crisis de imagen en las redes sociales, identificar actores importantes o aliados en esta estrategia de comunicación.

La empresa contratista, Alotrópico es la misma que en 2021 diseñó la estrategia de "Colombia es mi verdad"[35] (que incluyó un falso ciberataque y catalogación de contenido ciudadano)[36]. Es importante agregar que, las actividades que llevaron a cabo MinDefensa y Alotrópico durante el Paro Nacional, fueron referenciadas como problemáticas por la Comisión Interamericana de Derechos Humanos (CIDH), tras su visita a Colombia durante el paro.[37]

En el caso del contrato de MinDefensa analizado para este informe, es posible caracterizarlo como de este tipo porque aunque se habla de un contrato comunicacional con la terminología propia de tales contratos: análisis de percepción, detectar crisis de imagen en las redes sociales, identificar actores importantes; los antecedentes tanto del contratante como del contratista en el uso que hicieron de estas herramientas en el pasado permiten anticipar que se usa OSINT realmente para planear estrategías concretas en términos ofensivos, como lo sería identificar o vigilar actores en redes.

34. Búsquese en SECOP II, ingresando a la pestaña de búsqueda de procesos de contratación. Elimine los datos de fecha del formato e ingrese en la casilla de número del proceso: 234-2022-MDN-UGG-DA
35. El millonario contrato del Ministerio de Defensa para mejorar la "percepción ciudadana" de su gestión. El Espectador. Disponible en: https://www.elespectador.com/judicial/el-millonario-contrato-del-ministerio-de-defensa-para-mejorar-la-percepcion-ciudadana-de-su-gestion-article/

36. Mindefensa instrumentaliza la ciberseguridad en su campaña pedagógica. Carolina Botero. Disponible en: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/mindefensa-instrumentaliza-la-ciberseguridad-en-su-campana-pedagogica/

37. CIDH culmina visita de trabajo a Colombia y presenta sus observaciones y recomendaciones. CIDH. Disponible en: https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/167.asp

Sección 3:
Las facultades OSINT que se adquieren para el ciberpatrullaje son ilegales, conceptualmente inciertas y preocupantes

La Resolución 05839/15 de la Policía Nacional[38] es la norma colombiana que se refiere expresamente al ciberpatrullaje. Por otra parte, Fiscalía y DIJIN mencionan el artículo 242B del Código Procesal Penal como origen también de facultades para monitorear las actividades de las personas en internet, sin que se mencione como ciberpatrullaje[39]. Ambas normas dan forma al monitoreo de internet como una actividad propia de la investigación de ciberdelitos y de los delitos relacionados con organizaciones criminales en el marco de procesos penales, respectivamente. Aparte de estas normas no hay en el sistema jurídico ninguna mención al ciberpatrullaje o al uso de herramientas OSINT en actividades de inteligencia, mucho menos de la forma como éste se desarrolla.

Ahora bien, además de los problemas de las narrativas que se vienen desarrollando en torno al ciberpatrullaje, la Resolución de la Policía tiene dos problemas estructurales: en primer lugar, al tratarse de una norma que regula una actividad que pone en riesgo derechos humanos, esta debería ser una ley formal, no una simple resolución ya que los estándares de derechos humanos nos obligan a que toda actividad que regule, directa o indirectamente, la vigilancia estatal debe ser discutida democráticamente en una ley. En segundo lugar, la resolución no es lo suficientemente precisa como para establecer los límites del ciberpatrullaje, técnicas permitidas o su procedimiento.

En suma, que el ciberpatrullaje se desarrolle en una norma infralegal, que no aclara qué es, cómo se hace y quiénes están autorizados para realizar ciberpatrullaje significa que no se cumplen los estándares internacionales de derechos humanos de legalidad, necesidad y proporcionalidad que son los que deben desarrollar toda norma que imponga restricciones a derechos humanos[40].

En cuanto a la norma del Código Penal hay que decir que esta se conoce como agente encubierto virtual y está circunscrita a una investigación penal de delitos de crimen organizado,

---

38. Resolución 05839/15 de la Policía Nacional
39. El Estado monitorea internet: implicaciones en los derechos humanos del ciberpatrullaje. Fundación Karisma. Disponible en: https://web.karisma.org.co/el-estado-monitorea-internet-implicaciones-en-los-derechos-humanos-del-ciberpatrullaje/
40. Necessary & Proportionate. On the Application of Human Rights to Communications Surveillance. Electronic Frontier Foundation. Disponible en Para más información véase: https://necessaryandproportionate.org/principles/ y UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. ONU. Disponible en: https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance.
Aunque el informe del relator especial para libertad de expresión de la ONU en 2019, David Kaye, sobre vigilancia y derechos humanos no incluyó expresamente tecnologías OSINT si describió algunos de los temas que perimiten estas tecnologías y al exponer el impacto de la vigilancia es fácil hacer la conexión, por tanto este documento es referente también en este tema y sirve de inspiración para recordar como todos los actores del ecosistema, incluídas las empresas tienen responsabilidades y compromisos con el respeto a los derechos humanos y el cumplimiento de los estándares internacionales en la materia.

donde deben haber pruebas de la comisión del delito, y con control de un juez. Pero no justifica el monitoreo masivo o general de contenido en la web.

A la sombra de un marco legal débil, el ciberpatrullaje sucede en la práctica sin ninguna claridad conceptual y con unas capacidades preocupantes.

El Estado, más allá de la DIJIN y la Fiscalía, está adquiriendo capacidades tecnológicas en cabeza de diferentes autoridades para propósitos que van más allá de la investigación de ciberdelitos ya que también se aplican a otros delitos y sobre todo al interés por perfilar personas, incluyendo aquellas que legítimamente protestan.

Por otro lado, no hay pruebas de que Colombia esté avanzando en la construcción de garantías para un uso democrático de estas herramientas de OSINT; con respeto a los derechos humanos[41], contrapesos y transparencia de cara a la ciudadanía. Colombia, en línea con lo que sucede en la región Latinoamericana, está en mora de regular las tecnologías que facilitan la vigilancia masiva.

Las herramientas OSINT usadas para la vigilancia de las personas son como una draga de pesca que arrasa con el fondo del mar para capturar unos cuantos peces. Los software de inteligencia en fuentes abiertas arrasan con la información de cientos o miles o millones de personas en búsqueda de un solo objetivo, de un solo perfil. El Estado fue dotado de capacidades de vigilancia masiva que se han convertido en un arma cuyo objetivo son las personas[42]. Lo sucedido durante el Paro Nacional es el mejor ejemplo de ello.

Del análisis de los contratos identificados como de OSINT por Karisma hemos establecido una serie de preocupaciones que consideramos deberán ser objeto de investigaciones más profundas y cambios sustanciales en el abordaje del ciberpatrullaje y el uso de OSINT por parte del Estado:

1. En Colombia las autoridades encargadas de responder a la inconformidad social han estado contratando capacidades de vigilancia masiva sin que paralelamente el Estado haya desarrollado un marco jurídico garantista que ajuste dichas capacidades a los estándares internacionales de derechos humanos: legalidad, necesidad y proporcionalidad. Tampoco se están implementando mecanismos de control, seguimiento y remedio para los posibles abusos. Al contrario, las narrativas de la ciudadanía como amenaza y enemigo a vencer han permeado el modelo de contratación de herramientas OSINT en el país.
2. La contratación de tecnologías que permiten la vigilancia en Colombia no es transparente y, por tanto, hacer seguimiento e investigar estas facultades se dificulta. Establecimos que la investigación en este tema se enfrenta al menos a tres problemas de transparencia: (i) el objeto de estos contratos puede estar siendo tramitado como un tema de seguridad nacional, lo que los hace completamente opacos; (ii) cuando los contratos son publicados, ocultan las especificaciones técnicas bajo la etiqueta de reservadas y (iii) las solicitudes de acceso a información pública son inefectivas. Este tema deberá ser trabajado a mayor profundidad para establecer cómo se puede usar en forma más efectiva esta herramienta

41. Un marco jurídico de derechos humanos para la vigilancia de las comunicaciones en América Latina. Al Sur. Disponible en: https://www.alsur.lat/sites/default/files/2021-07/Vigilancia%20de%20las%20Comunicaciones%20ES_version%20completa.pdf
42. When your “friends” spy on you: The firm pitching Orwellian social media surveillance to militaries. Forbidden Stories. Disponible en: https://forbiddenstories.org/story-killers/osint-s2t-unlocking-cyberspace-journalists-activists/

de control ciudadano.

3. A excepción de dos de los contratos analizados, cuyos procesos se realizaron por selección abreviada de mínima cuantía, todos los demás son contrataciones directas. Los pliegos de condiciones de los procesos de contratación suelen ser muy específicos, la contratación se hace de forma directa con empresas que suelen ser las únicas representantes de un producto concreto -casi siempre de origen israeli y donde Deinteko SAS es el mayor contratista- y a un costo alto. Trabajar en conocer mejor la industria que provee estas herramientas sigue siendo un tema pendiente.
4. Los OSINT se presentan como funcionalidades que se basan en información disponible públicamente y, que, por tanto, no tiene ninguna restricción. Sin embargo, ver OSINT solo desde esta característica minimiza su contexto e impacto. La cantidad de información que esta tecnología puede agregar supone una escala para la analítica de datos que por sí misma puede producir resultados importantes para la vigilancia de las personas. Pero, esto no queda allí, en el análisis de los contratos establecimos, además, que las mismas herramientas que se presentan como OSINT, en la práctica, ofrecen capacidades que van más allá de la información pública y permiten también cruzar información de fuentes cerradas, lo que aumenta la capacidad del sistema para perfilar.
5. Las capacidades tan intrusivas que permiten estas herramientas incluyen, por ejemplo, perfilamientos, des-anonimización y localización de usuarios de internet e incluso capacidades para ocultar las huellas de la investigación. Lo anterior obliga a pedir más que transparencia contractual, exige una discusión democrática que permita discutir y crear controles sobre quién y cómo se usan las herramientas. De la información contractual se identifica que se contratan capacidades que las autoridades no tienen facultades para usar, que no es posible saber exáctamente qué productos compran, y que quedan muchas dudas sobre cómo los usan.
6. Cuando al analizar estos contratos confirmamos que el Estado está adquiriendo herramientas OSINT justificándolas con propósitos ilegales, confirmamos también que la desconfianza de las personas en el uso de estas herramientas es fundada y marca la urgencia por desarrollar un entorno legal que incluya el seguimiento al cómo se usan estas herramientas y prohibirlas cuando corresponda. Coincidimos en que no es un absurdo que las autoridades tengan capacidades de monitoreo de redes para prevenir y perseguir amenazas, sin embargo si el argumento es prevenir y perseguir la protesta, la libertad de expresión y el acceso a la información confirma lo sencillo que es abusar de la ductilidad de este tipo de técnicas y, como dijimos, muestra la necesidad de mayores controles.
7. La reserva de requerimientos técnicos en los contratos investigados es también un elemento que contribuye al deterioro de la confianza ciudadana. De la presente investigación se deriva que esta facultad antes que proteger las legítimas funciones de las autoridades para garantizar la seguridad de la ciudadanía ha sido usada para ocultar propósitos ilegales sin que existan mecanismos de control o seguimiento que permita identificar, castigar e incluso indemnizar estos abusos.
8. No existe certeza de que las garantías respecto de las actividades de monitoreo de internet asociadas a investigaciones judiciales o de inteligencia se estén aplicando de forma tal que no constituyan una amenaza para los derechos a la opinión y la protesta.
9. Discutir la forma como se usa la información y, sobre todo, lo que de ella se puede deducir cuando ha sido obtenida mediante herramientas tecnológicas es una necesidad urgente. La geolocalización que se basa en búsqueda en redes sociales, estaría limitada a nivel técnico a los metadatos suministrados por la red social -no todas las publicaciones cuentan con

información de geolocalización-, o se referiría a la información aportada por la persona en datos o imágenes en la plataforma de la que se pueden determinar dónde se encuentra. En caso tal de que el sistema sí pueda identificar una dirección IP, la geolocalización sería imprecisa pero permite la identificación de la ciudad de origen de un elemento digital. Para una ubicación precisa sería necesario realizar una solicitud a la empresa proveedora de internet (PSI). ¿Cómo se usan estas facultades?, es una pregunta que requiere mayor análisis para evitar que por sí misma afecte derechos de las personas como intimidad, libertad de expresión, participación, libertad de conciencia, debido proceso y asociación.

10. El Estado está usando sistemas de OSINT para monitorear su "marca" o "buen nombre", a pesar de que este derecho sea inexistente en su caso. Si bien esta no es una actividad ilegal, si revela que el Estado colombiano parece estar enfrentando al inconformismo ciudadano, no responsabilizándose y reparando sus propios errores, sino monitoreando a quienes lo critican.
11. En algunos de los contratos se solicita que el software haga búsquedas anónimas o evite que la actividad se califique por la plataforma como "artificial" (cuando lo es), lo que viola las normas comunitarias de la plataforma y plantea preguntas sobre la legalidad de este tipo de requerimientos contractuales. Estos requerimientos contractuales son también problemáticos porque implican que el Estado está usando métodos que en otros contextos se critican porque contribuyen a alimentar fenómenos como la desinformación. Si las autoridades públicas patrocinan mecanismos para evitar los controles que las empresas han estado adoptando para evitar comportamientos artificiales -que permiten identificar problemas de desinformación o violencia digital- está siendo incoherente con la iniciativa que como sociedad hemos venido librando contra fenómenos desestabilizadores de la democracia y de la seguridad de las personas.

Finalmente, es imposible no ver estos contratos sin hacernos preguntas como: ¿Cómo se están usando realmente estas capacidades? ¿Cuándo se discutirán salvaguardias y garantías al respecto? ¿Cómo puede una democracia construir confianza en lo que las autoridades hacen con esta herramienta? ¿Se han implementado garantías en los procesos penales para individualizar a estas personas? Tendremos que trabajar para obtener más información y así lo haremos.

Sección 4.
Recomendaciones

Ante la falta de garantías respecto a la adquisición y uso de las herramientas OSINT en Colombia, y a partir de los aprendizajes derivados de la investigación queremos presentar las siguientes recomendaciones al Estado colombiano.

4.1 Recomendaciones para la Cancillería

- A la luz del presente informe, y de las investigaciones que han publicado sobre estos temas El Espectador y la FLIP también, solicitamos a la Cancillería que adelante las actividades necesarias para que la recomendación número 40 de la visita de trabajo a Colombia de la CIDH con ocasión del Paro Nacional de 2021 sea incluída dentro la hoja de ruta de seguimiento a las recomendaciones propuestas por esa entidad al Estado colombiano en los términos de la visita de la CIDH a Colombia en enero de 2023.

4.2 Recomendaciones para las entidades PMU - Ciber

- Deben abstenerse de realizar actividades en internet para las que no estén facultados legalmente. En concreto les hacemos un llamado para que atiendan inmediatamente la Recomendación No. 40 que fue resultado de la visita de trabajo a Colombia de la CIDH con ocasión del Paro Nacional de 2021, bajo el entendido además de que los hallazgos de esta investigación sobre lo que las entidades están haciendo a la sombra del "ciberpatrullaje" va mucho más allá incluso de lo que se vislumbró durante la visita de la CIDH al país en mayo de 2021.
- En todo los casos en que sus actividades operen sobre internet o afecten a la ciudadanía deben cumplir con las obligaciones internacionales de Colombia y cumplir con los principios de legalidad, necesidad y proporcionalidad.
- Cuando de forma previa una ley los habilita a monitorear de contenidos en internet deben definir internamente el alcance de las actividades de ciberpatrullaje; incluyendo una descripción de las facultades que lo constituyen, los contrapesos, las medidas de transparencia y los funcionarios que la deben realizar.
- Deben abstenerse de justificar la ciberguerra contra la ciudadanía y de calificar como enemigos internos a quienes protestan o critican puesto que son actividades ilegales y bajo ninguna circunstancia deben llevarse a cabo.
- En cumplimiento de sus deberes legales, deben publicar toda la información contractual necesaria para que las obligaciones de transparencia contractual sirvan como contrapeso y control de la tecnología que se usa para actividades de vigilancia.
- Se deben desarrollar controles que permitan hacer seguimiento al gasto en tecnologías de vigilancia.

4.3 Recomendaciones para los organismos de control

- Exigir que la actividad de ciberpatrullaje, investigación criminal en internet o de inteligencia en la web, como cualquiera que supone la restricción de Derechos Humanos, cumpla con los estándares internacionales de legalidad, necesidad y proporcionalidad.
- Exigir y verificar que las entidades con funciones vinculadas con el monitoreo de internet cuenten con mecanismos de transparencia para poder hacer controles sobre la adquisición y uso de las tecnologías que utilicen.
- Exigir y verificar que las entidades con funciones vinculadas con el monitoreo de internet realicen evaluaciones de impacto en los derechos humanos de las contrataciones de tecnología por parte del Estado.
- Investigar la forma en que se está adelantando la contratación de herramientos OSINT. En especial deben evaluar las capacidades que se adquieren y hacer seguimiento a los montos y de las modalidades de contratación.
- Crear mesas técnicas que permitan hacer seguimiento y evaluar el uso de OSINT por parte del Estado con la participación de múltiples partes interesadas y víctimas.
- Desarrollar su propia capacidad para entender el ciberpatrullaje y la inteligencia en internet.

4.4 Recomendaciones para los legisladores

- Tramitar la ley que consagre formalmente las actividades de ciberpatrullaje de modo que cumplan con estándares internacionales de legalidad, necesidad y proporcionalidad. Se determinan responsables, contrapesos y medidas de transparencia. Y, que en consecuencia, prohíba por cualquier motivo, incluidos los judiciales y de inteligencia, la vigilancia masiva e indiscriminada a la ciudadanía.
- Asegurarse de que cuando el monitoreo de internet se torna en un mecanismo de vigilancia selectiva y específica de personas u organizaciones se cumplan con las garantías necesarias de modo que se justifique y se garantice el debido proceso, especialmente el derivado del control judicial.
- Hacer un estudio de impacto de derechos por el uso de OSINT desde el Estado Colombiano y que les permita a los Legisladores establecer límites claros.
- Crear obligaciones legales de informar cómo se usan las herramientas OSINT, de desclasificar e informar a quienes fueran afectados por una investigación o actividad de este tipo.
- Crear obligaciones legales para que las organizaciones responsables hagan pública información estadística sobre el uso de tecnologías para la vigilancia y las actividades de inteligencia. Tipo de tecnología, número de afectados, motivos, responsables son algunos de los datos que deben publicarse.
- Ofrecer dentro de la ley acciones de remedio y de reparación cuando haya responsabilidad por el uso abusivo de tecnología para la vigilancia a la ciudadanía.
- Crear desde la ley programas integrales para que todos los funcionarios públicos, pero sobre todo los pertenecientes a organismos de seguridad, integren y utilicen el marco de protección a los derechos humanos de forma adecuada.
- La Comisión de Seguimiento a las Actividades de Inteligencia y Contrainteligencia debe

hacer un llamado a la fuerza pública para que explique el uso que hace de las herramientas OSINT. Así como hacer evaluaciones periódicas al respecto y, en caso de evidenciar vulneración de derechos, tomar las medidas correspondientes.

4.5 Recomendaciones para las empresas proveedoras de estas tecnologías

- Deben abstenerse de ofrecer productos y servicios que tengan objetos contractuales que abiertamente vulneren los derechos humanos.
- Deben afirmar públicamente su responsabilidad de respetar los derechos humanos e integrar procesos de diligencia debida en materia de derechos humanos desde las primeras fases del desarrollo ,diseño de productos y a lo largo de todas sus operaciones. Además, se deben realizar consultas periódicas con la sociedad civil (especialmente con los grupos en riesgo de ser vigilados) e informes de transparencia sólidos sobre las actividades empresariales que tengan un impacto en los derechos humanos.
- Deben establecer salvaguardias sólidas para garantizar que el uso de sus productos o servicios se ajuste a las normas de derechos humanos. Estas salvaguardas deben incluir cláusulas contractuales que prohíban usos que violen la legislación internacional de derechos humanos, características técnicas de diseño para señalar, prevenir o mitigar el uso indebido, y auditorías de derechos humanos y procesos de verificación;
- Cuando detecten usos indebidos de sus productos y servicios para cometer abusos contra los derechos humanos, deben informar sin demora a los organismos de supervisión nacionales, regionales o internacionales pertinentes. También deben establecer mecanismos eficaces de reclamación y reparación que permitan a las víctimas de abusos de los derechos humanos relacionados con la vigilancia presentar quejas y obtener reparación.
- Deben disponer de mecanismos de transparencia activa en los que sea posible hacer seguimiento a las adquisiciones que hace el Estado de estas tecnologías.
- A nivel internacional se ha ido creando una serie de estándares en la industria de la vigilancia que incluyen requisitos de exportación de tecnologías, es necesario trabajar con la sociedad civil de los países destinatarios de estas tecnologías para explicar el cumplimiento de estos estándares.

ANEXO

CONTRATOS DE HERRAMIENTAS OSINT EN COLOMBIA

Un análisis de los contratos realizados por el Estado colombiano para vigilar internet a través de software de inteligencia de fuentes abiertas de inteligencia (OSINT)

20 años Fundación Karisma

PRIVACY INTERNATIONAL

<K+LAB>

Tabla de contenido

1. Comando Conjunto Cibernético (CCOCI). Ejemplo perfecto de falta de transparencia

Respecto del CCOCI encontramos un contrato para la adquisición de tecnologías que permiten la vigilancia de internet. Este se firmó el 31 de marzo de 2020 con la empresa Desarrollo e Integración de Tecnología y Comunicaciones S.A.S. (Deinteko[1]), recurrente contratista del Estado para soluciones tecnológicas. El objetivo del contrato es la "Adquisición de servicio a la plataforma de inteligencia DEEP-DARWEB/FUENTES ABIERTAS- de acuerdo con la especificaciones técnicas reservadas".

El contrato se asignó en la modalidad de contratación directa dado que Deinteko es la única empresa autorizada en Colombia por Sixgill[2] para promover sus servicios. Sixgill es una empresa israelí especializada en brindar servicios y productos de ciberinteligencia para monitorear la web y con experiencia trabajando para gobiernos, organismos de seguridad y empresas privadas[3].

Ahora bien, las especificaciones del producto comprado son reservadas sin justificación detallada, por lo tanto, en el SECOP no se encuentra mucha información.

No obstante, dentro de la página de Sixgill, en la sección de productos para gobiernos y fuerzas de seguridad, se encuentran algunas especificaciones sobre el tipo de software que pudo haber contratado el CCOCI. En concreto, dados los requisitos del contrato, es probable que el producto comprado sea similar al Intuitive & Secure Investigative Portal[4].

A pesar de que la solución de Sixgill es ofrecida como un producto para luchar contra el cibercrimen en la dark web, el mismo se trata de un sistema de OSINT muy completo que puede analizar sin problemas fuentes abiertas de internet o redes sociales. Como lo señaló en una entrevista en 2018, Gabriel Glusman, analista senior de ciberinteligencia de Sixgill[5] y como aparece referenciado en las características y funcionalidades del producto hacen monitoreo en tiempo real de páginas escogidas en la surface web o internet común.

El producto de Sixgill consiste en un plataforma que monitorea internet en tiempo real y que lanza alertas según las prioridades preestablecidas. Para las alertas usan un Natural Language Processing (NLP) algorithm que procesa las publicaciones en la web buscando menciones a los riesgos de seguridad predefinidos. Además, el sistema tiene incorporado un procesador de imágenes para identificar texto. El análisis del sistema finalmente tiene como objetivo el diseño de operaciones de respuesta a partir del estudio de las estrategias de actores específicos y de una evaluación del contexto.

En la citada entrevista de Gabriel Glusman se explicó el funcionamiento de Dark-I, una versión anterior (2017) o similar al producto ofertado hoy. Si bien no es posible afirmar que el producto sea igual, sí da luces de qué capacidades tiene. Glusman señaló que el programa de Sixgill

1. Página oficial de Deinteko SAS. Disponible en:http://www.deinteko.com/
2. Página oficial de Cybersix Gill. Disponible en: https://www.cybersixgill.com/
3. About Cybersixgill News. Disponible en: https://news.cybersixgill.com/about/
4. Documento de funciones y características del Intuitive & Secure Investigative Portal. Disponible en: https://sixgill.wpengine.com/wp-content/uploads/2020/09/Datasheet_Portal_2020.pdf
5. Pentester Academy TV. Sixgill's Dark-i with Gabriel Glusman. Disponible en: https://www.youtube.com/watch?v=5B8irycHR-s&t=462s

descarga a sus bases de datos y sistemas de almacenamiento toda la información que encuentra, de forma que los datos no se pierdan si son eliminados o desindexados. Una vez creada la base de datos, la información es procesada por una inteligencia artificial que la etiqueta y categoriza.

Respecto a DARK-I, el analista de Sigill señala que tiene una función que permite perfilamientos. La metodología que utiliza es la siguiente: una vez una pieza de información ingresa a la base de datos, esta es taggeada o categorizada y se identifican actores relacionados con la publicación. Una vez estos son identificados se buscan todas sus publicaciones en páginas y redes sociales como Pastebin, Twitter o Reddit, entre otras. Las publicaciones son guardadas y se realiza un segundo nivel de análisis revisando las interacciones del usuario. De forma tal que deja registrado con quién comparte la información o está en contacto. La categorización para perfilar se desarrolla por los usuarios según "objetivos importantes en el contexto de una operación militar"[6].

Finalmente, se precisa que cuando se etiqueta información de un perfil como un actor de riesgo el proceso es más invasivo. El sistema realiza un estudio de sus publicaciones, quién comparte o quién replica, determina cuáles son los momentos y días en que es más activo en la red o página. De igual forma, se crean nuevas alertas únicas y prioritarias sobre el contenido del perfilado. El objetivo del DARK- I es procesar todo el contenido producido para saber qué habla el perfilado, lo que incluye un procesador de texto y la descarga de las imágenes publicadas; las cuales son procesadas utilizando sobre ellas un sistema de reconocimiento óptico de carácteres (OCR), funciones que suenan similares a las del intuitive & Secure Investigative Portal actual. Todo esto con la finalidad de que ni una palabra de lo que el perfilado publique se pase por alto y se pueda saber con precisión de qué está hablando y en qué momento.

Además, Dark-I tenía la capacidad de realizar un estudio de credibilidad de los actores dentro de las comunidades donde se mueven para determinar el nivel de reputación e importancia del actor investigado. Esto se hace infiltrando grupos en chats o foros donde el actor interactúa.

En el contrato se justifica la adquisición de este programa en el deber del CCOCI de combatir ataques cibernéticos que afecten los "valores e intereses nacionales", sin precisar el sustento normativo. El uso de términos abiertos como valores o intereses nacionales, sumado a que el CCOCI no tiene funciones investigativas, genera dudas respecto de quién ha utilizado este software y en qué partes de internet.

El CCOCI es, principalmente, una entidad generadora de política pública. Sus funciones están relacionadas con asesorar al presidente, preparar documentos sobre seguridad nacional y desarrollar políticas. No obstante, ejerce el mando estratégico en las operaciones militares de las tres ramas de la fuerza pública. Siendo así, resulta preocupante que esta entidad cuente con herramientas que usen metodologías de perfilamiento en redes sociales sin control alguno, pues

no es claro con qué fines o qué implica esto para la ciudadanía. Además, deja abierta la pregunta sobre si información íntima en redes sociales está siendo usada en operaciones militares.

6. Ibidem.

2. Perfilamiento en redes sociales, geolocalización y búsquedas anónimas. Las capacidades de la Dirección de Investigación Criminal e Interpol (DIJIN)

El 30 de diciembre de 2019, la DIJIN contrató los servicios de la empresa Deinteko (segundo contrato) que le permitiera a la Policía "acceso a plataformas de fuentes abiertas para ciberpatrullaje"[7]. Según la justificación del contrato, se trata de una actualización de un contrato previo del año 2014 mediante el cual la DIJIN[8] ya había contratado una herramienta similar de búsqueda en redes sociales.

En cuanto a la justificación, la DIJIN señala que debe adquirir herramientas OSINT para fortalecer el ciberpatrullaje de conductas que atenten contra la integridad de las personas, las relacionadas con comercialización de productos ilegales, distribución de material de abuso infantil, entre otras, con fines de aportar material probatorio, ya que es complejo realizarlo de forma manual. La DIJIN cita como fuente jurídica la Resolución 05839 de 2015[9] y la Operativa Directiva Transitoria 030 de 2018, a pesar de que dicha norma solo aplica a ciberdelitos.

La plataforma contratada no tiene nombre. De nuevo, no sabemos exáctamente qué se compró. Por otro lado, en la página de Deinteko no hay información específica sobre este tipo de herramientas. Aunque las especificaciones técnicas del contrato son reservadas, los parámetros del contrato son muy precisos respecto a las especificaciones y capacidades de la herramienta contratada.

Respecto del funcionamiento interno del producto y el cómo opera, no es posible determinarlo pues las especificaciones son reservadas y los proveedores no lo han publicado. Sin embargo, es muy probable que el sistema funcione a partir de crawlers. En consecuencia, la principal

7. Búsquese en SECOP II, ingresando a la pestaña de búsqueda de procesos de contratación. Elimine los datos de fecha del formato e ingrese en la casilla de número del proceso: PN DIJIN SA MC 029 DE 2019
8. Disponible en: https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-1-120908)
9. https://www.policia.gov.co/file/32305/download?token=OA0OIAOJ

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL

RESOLUCIÓN NÚMERO 388 **DEL** 27 NOV 2019

"POR LA CUAL SE DEFINE EL PROCESO DE SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS PARA LA DEFENSA Y SEGURIDAD NACIONAL – PROCEDIMIENTO MENOR CUANTÍA PN DIJIN SA MC 029 DE 2019"

El Director de Investigación Criminal e INTERPOL, en uso de las facultades conferidas por la Ley 80 de 1993, Ley 1150 de 2007, Decreto 1082 de 2015, Resolución 03049 del 30 de julio de 2014 y en especial la Resolución 00008 del 01 de enero de 2017 de la Dirección General de la Policía "*Por la cual se delega en algunos funcionarios, la competencia para contratar, comprometer y ordenar el gasto, en desarrollo de las apropiaciones incorporadas al presupuesto de la Policía Nacional y suscribir convenios y/o contratos interadministrativos*" y,

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

Que la Ley 1150 de 2007, mediante la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos, dispuso que la escogencia del contratista se efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos, contratación directa y mínima cuantía.

Que con fecha 07 de octubre de 2019, se aprobó el estudio previo para el "ACCESO A PLATAFORMA DE FUENTES ABIERTAS PARA EL CIBERPATRULLAJE DE LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL" mediante numero SISCO 324098 suscrito por los señores, Teniente Coronel ALEX URIEL DURÁN SANTOS Jefe Centro Cibernético Policial, Mayor VICTOR HUGO BASTIDAS PORTILLO Jefe Grupo Telemática DIJIN, Capitán JUAN CARLOS HERRERA SÁNCHEZ, Subintendente EDILBERTO ALONSO TANGARIFE LONDOÑO, Subintendente JOSÉ DAVID LIZARAZO RIVERA y Patrullero HECTOR DANIEL SANTOS ROCHA Estructuradores del Estudio Previo y especificaciones técnicas, el Comité de Adquisiciones de la Dirección de Investigación Criminal e INTERPOL, revisó el estudio previo, verificó la etapa preparatoria del proceso, la existencia de recursos, la conveniencia y oportunidad de adelantar el proceso y recomendó al señor Director de Investigación Criminal e INTERPOL dar inicio al mismo.

Que existieron los recursos libres y disponibles de afectación para el desarrollo del presente proceso de contratación, por la suma de TRES MIL NOVECIENTOS NOVENTA Y DOS MILLONES NOVECIENTOS MIL PESOS MONEDA LEGAL COLOMBIANA ($3.992.900.000,00), amparado mediante el Certificado de Disponibilidad Presupuestal No. 12019 del 08/10/2019 expedido por la Jefe de Presupuesto de la Dirección de Investigación Criminal e INTERPOL (E), recurso 11.

Que el 07/10/2019 se expide aviso de convocatoria y proyecto de pliego de condiciones por medio de los cuales se da inicio el proceso, siendo publicados en el SECOP II el 08/10/2019.

Que mediante comunicación oficial No S-2019-153000-ARAFI-GRUCO-17.5 de fecha 08 de octubre de 2019, se da aviso de control preventivo estatal a la Procuraduría Delegada para la Vigilancia Preventiva de la Función Pública.

Que mediante comunicación oficial No S-2019-153026-ARAFI-GRUCO-17.5 de fecha 08 de octubre de 2019, se envía invitación a ejercer control social a la Red de Veedores y Veedurías Ciudadanas.

Que el 15/10/2019 se expide la Resolución número 335 *"Por la cual se designa el comité evaluador para el proceso de contratación de selección abreviada para la adquisición de bienes y servicios para la Defensa y Seguridad Nacional – Procedimiento menor cuantía PN DIJIN SA MC 029 DE 2019 cuyo objeto es el ACCESO A PLATAFORMA DE FUENTES ABIERTAS PARA EL CIBERPATRULLAJE DE LA DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL"*, la cual fue notificada mediante comunicación oficial No. S-2019-156981-ARAFI-GRUCO 17.5 de fecha 15/10/2019.

El contratista debe garantizar dentro de la plataforma la recolección de la siguiente información de manera continua e ininterrumpida: De Facebook: perfiles, páginas, grupo, evento, búsqueda De Twitter (perfil, búsqueda) De YouTube (video, usuario/canal, búsqueda) De Instagram (perfil, búsqueda, búsqueda geográfica) De LinkedIn (perfil) De Flickr (perfil, búsqueda, búsqueda geográfica) De Búsqueda en Google cache(se puede hacer la búsqueda por URL siempre y cuando recolecte el total de la información pública solicitada en la búsqueda, de no ser así, el contratista deberá realizar las actividades necesarias para lograr tal fin) De Deep Web y Darknet De sitios web, otros blogs, RSS, foros, noticias y demás) Estas actividades las deberá realizar utilizando los distintos métodos automatizados existentes (rastreo, robots, crawlers, extracción, APIs) o desarrollándolos sin generar costos adicionales para la Policía Nacional. En todo caso, el contratista debe garantizar que estas funciones SIEMPRE estén disponibles y funcionales para los usuarios que utilicen el servicio de la plataforma.
La plataforma debe permitir la recolección de información de distintos idiomas, clasificando de manera automática entidades tales como: eventos, tendencias, objetos, sitios, personas, perfiles, organizaciones, así como relaciones dispersas(información que ha sido compartida, reacciones(likes, me encanta, me divierte, me asombra, me entristece, me enoja) de forma pública por uno o varios usuarios diferentes al objetivo del analista y el cual se encuentra relacionado o asociado al objeto de interés, donde de acuerdo a esta información se genera un vínculo entre estos). Lo anterior tanto de información estructurada y no estructurada
La plataforma debe permitir la ubicación georreferenciada de las publicaciones, perfiles. En todo caso, el motor de georreferenciación proporcionado por el contratista debe estar integrado a la herramienta.
La plataforma debe permitir identificar las publicaciones realizadas en una zona geográfica delimitada en forma de polígonos, con capacidad de establecer filtros de sitios geográficos
La funcionalidad de georreferenciación de la plataforma debe funcionar de forma continua
La plataforma tendrá la capacidad de realizar georreferenciación en tiempo real sobre la información recolectada.
La plataforma deberá realizar búsqueda, recolección y análisis de información pública sobre peticiones realizadas por parámetros de búsqueda como números celulares, correos electrónicos, entre otros(cualquier otro tipo de información que se ha recolectado y que pueda ser vinculada con el objetivo de interés, incluyendo aquellas variables asociadas a los perfiles que sean implementadas por las redes sociales solicitadas durante el tiempo de servicio y que contengan información pública), logrando obtener información asociada a perfiles, publicaciones, personas, entre otras.
La plataforma debe permitir buscar por dirección IP sobre un componente de georreferenciación mostrando país, ciudad, latitud, longitud y proveedor de servicio de Internet.

función del sistema parece ser permitir búsquedas automatizadas en redes sociales como Twitter que no cuentan con una herramienta que permita recopilar la información a partir de la navegación del sitio web, facilitando a la policía encontrar publicaciones o contenido.

La herramienta debe extraer datos de redes sociales, portales web, medios de difusión masiva, foros, blogs, Internet, Dark Web, Darknet, entre otras espacios de "información pública disponible a través de fuentes abiertas"[10]. El software debe realizar búsquedas y presentación de resultados de forma automatizada y continua. El contrato es enfático en que la herramienta debe permitir capturar información pública dispersa, refiriéndose a las interacciones, compartidos, reacciones "me encanta, me divierte, me asombra, me entristece, me enoja", de forma tal que se puede establecer vínculos entre usuarios de internet.

Respecto de los usuarios de internet a los que se apunta con el software de ciberpatrullaje, se debe poder recolectar fotografías, publicaciones, comentarios, amigos en común, sitios frecuentados/visitados, lugares de trabajo, reacciones, lugares de estudio, relaciones familiares, hobbies, páginas seguidas, número telefónico, correos electrónicos (los dos últimos en caso de que sean públicos).

Esta información se debe recolectar de forma ininterrumpida y en varios idiomas en Facebook, Twitter, YouTube, Instagram, LinkedIn, Flickr, además de realizar búsquedas de Google para capturar caché y URL relacionadas, Deep Web, foros, noticias y blogs y a futuras redes sociales. De ser posible, debe poder brindar información de grupos abiertos de WhatsApp y WeChat y Xbox, y en sitios .onion. De igual forma, se deben poder hacer búsquedas usando como parámetros el número de celular, correos electrónicos, perfiles web y usando productos multimedia (videos, audios y fotografías).

La información recolectada se procesa con el fin de que la plataforma cree perfiles que incluyan: nombre, residencia, lugar de trabajo, foros, amigos, páginas de interés, información de interacciones de forma tal que se pueden "establecer conductas, comportamientos, tendencias, hábitos o modalidades delictivas". Además de almacenar la información y contenido multimedia de los perfiles offline.

Además, se exige que el software permita localizar geográficamente, y en tiempo real, publicaciones y perfiles, precisando que el motor de geolocalización debe estar incorporado en la herramienta, de forma tal que se pueda alimentar directamente por la DIJIN. Si bien no se precisa el método para la geolocalización (podría hacerse con metadatos, por ejemplo), si pide una función para localizar la IP y proporcionar información de país, ciudad, latitud, longitud y proveedor de internet.

Finalmente, pero igual de preocupante, es que la plataforma permite hacer búsquedas anónimas, de hecho en el contrato se especifica que en esta modalidad no deben generarse registros.

Sobre estas últimas funciones llamamos la atención que las mismas incumplen los términos de las redes sociales como Facebook, Instagram o Twitter en las que opera[11].

10. Resolución 388 de 2019.
11. Para más información revisar la Política de Integridad y Autenticidad de Twitter en: https://help.twitter.com/es/rules-and-policies#platform-integrity-and-authenticity y las Normas Comunitarias de Meta, sección Autenticidad e Integridad, en: https://transparency.fb.com/es-es/policies/community-standards

3. Vigilancia geopolítica. Ejército Nacional y Gamma INGENIEROS SAS

En 2016 el Ejército Nacional contrató con Gamma Ingenieros SAS la adquisición de un equipo de inteligencia con la finalidad de incorporarlo al sistema de fuentes abiertas del Ejército nacional[12]. El mismo se justificó en el marco de la "lucha contra la ciberdelincuencia" en redes sociales y para aumentar las capacidades de ciberguerra. En consecuencia, adquirieron un software que les permite realizar búsquedas mediante crawling en: Google, Bing, Yahoo, Twitter, Facebook, LinkedIn, YouTube, Instagram, páginas de medios de comunicación, emails por suscripción por pago y documentos almacenados en redes locales.

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
EJÉRCITO NACIONAL
CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA "CENAC"
INTELIGENCIA

TODOS POR UN NUEVO PAÍS

Bogotá D.C. 6 de diciembre de 2016

ESTUDIO PREVIO PARA EL PROCESO DE SELECCIÓN CONTRATACIÓN DIRECTA No. 325-DIADQ-CADCO-CENACINTELIGENCIA-2016, EL CUAL TIENE POR OBJETO LA "ADQUISICIÓN DE EQUIPO DE INTELIGENCIA CON AMPLIACION DE LICENCIAMIENTO Y ARQUITECTURA DE HARDWARE PARA EL SISTEMA DE FUENTES ABIERTAS DEL EJÉRCITO NACIONAL".

1. ANTECEDENTES

1.1. ADQUISICIONES PREVIAS DE LA ENTIDAD

NUMERO CONTRATO ACEPTACIÓN DE OFERTA:	185-CENACINTELIGENCIA-CACIM-2016
CLASE DE CONTRATO:	COMPRAVENTA
OBJETO DEL CONTRATO:	"ADQUISICION EQUIPO DE SISTEMAS INCLUYE HERRAMIENTA CON LICENCIAMIENTO PARA VERIFICACIÓN DE FUENTES ABIERTAS PRIMERA FASE"
DATOS CONTRATISTA	GAMMA INGENIEROS S.A.S
DURACIÓN:	EL PLAZO PARA LA EJECUCION SERA DENTRO DE LOS 90 DIAS CALENDARIO, CONTADOS A PARTIR DEL CUMPLIMIENTO DE LOS REQUISITOS DE PERFECCIONAMIENTO Y EJECUCIÓN DEL CONTRATO.
VALOR DEL CONTRATO:	TRESCIENTOS CUATRO MILLONES SEISCIENTOS CUARENTA MIL SEISCIENTOS SESENTA Y CINCO PESOS CON OCHO CENTAVOS ($ 304.640.665,08) IVA INCLUIDO.

2. DEFINICIÓN DE LA NECESIDAD Y ANÁLISIS DEL SECTOR

2.1. DEFINICIÓN Y JUSTIFICACIÓN DE LA NECESIDAD

En consecuencia el proceso de contratación estatal en mención, al tratarse de la adquisición de bienes y servicios de naturaleza misional que cumple los organismos de inteligencia y contrainteligencia en sus documentos, información y elementos goza de reserva legal de acuerdo a los términos descritos la reserva de información que se señala en la Ley 1621 de 2013 en su artículo 33 que procede así:

(...) "ARTÍCULO 33. RESERVA. Por la naturaleza de las funciones que cumplen los organismos de inteligencia y contrainteligencia sus documentos, información y elementos técnicos estarán amparados por la reserva legal por un término máximo de treinta (30) años contados a partir de la recolección de la información y tendrán carácter de información reservada.

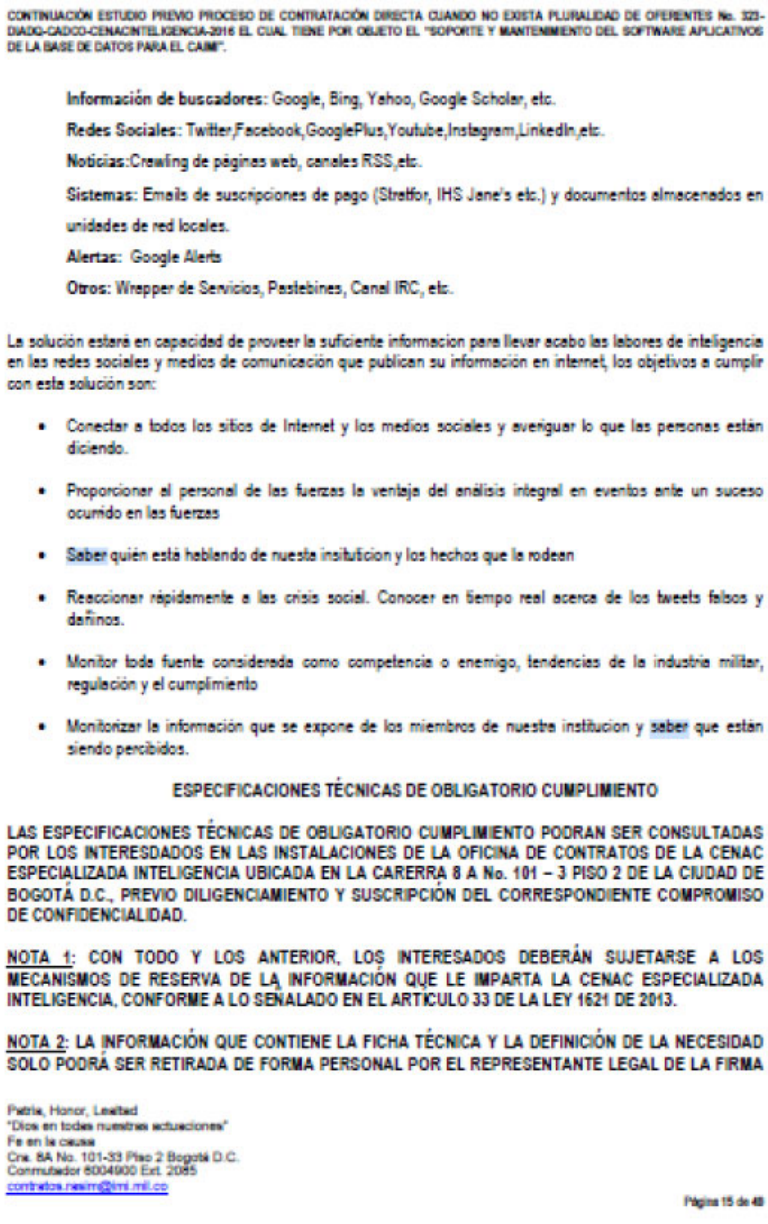
Excepcionalmente y en casos específicos, por recomendación de cualquier organismo que lleve a cabo actividades de inteligencia y contrainteligencia, el Presidente de la República podrá acoger la recomendación de extender la reserva por quince (15) años más, cuando su difusión suponga una amenaza grave interna o externa contra la seguridad o la defensa nacional, se trate de información que ponga en riesgo las relaciones internacionales, esté relacionada con grupos armados al margen de la ley, o atente contra la integridad personal de los agentes o las fuentes.

Parágrafo 2. El organismo de inteligencia que decida ampararse en la reserva para no suministrar una información que tenga este carácter, debe hacerlo por escrito, y por intermedio de su director, quien motivará por escrito la razonabilidad y proporcionalidad de su decisión y la fundará en esta disposición

Según la propia justificación del contrato, su finalidad será "averiguar lo que las personas están diciendo", proporcionando a la fuerza información adicional en caso de un suceso que

12. Proceso Número: 325-DIADQ-CADCO-CENACINTELIGENCIA-2016

las relacione para “saber quienes están hablando de la institución y los hechos que las rodean”. Así como reaccionar rápidamente a crisis sociales y hechos dañinos, monitorear fuentes consideradas “competencia o el enemigo”, saber qué información del medio se publica y cómo están siendo percibidos.



CONTINUACIÓN ESTUDIO PREVIO PROCESO DE CONTRATACIÓN DIRECTA CUANDO NO EXISTA PLURALIDAD DE OFERENTES No. 323-DIADG-CADCO-CENACINTELIGENCIA-2016 EL CUAL TIENE POR OBJETO EL "SOPORTE Y MANTENIMIENTO DEL SOFTWARE APLICATIVOS DE LA BASE DE DATOS PARA EL CAIM".

Información de buscadores: Google, Bing, Yahoo, Google Scholar, etc.

Redes Sociales: Twitter,Facebook,GooglePlus,Youtube,Instagram,LinkedIn,etc.

Noticias: Crawling de páginas web, canales RSS,etc.

Sistemas: Emails de suscripciones de pago (Stratfor, IHS Jane's etc.) y documentos almacenados en unidades de red locales.

Alertas: Google Alerts

Otros: Wrapper de Servicios, Pastebines, Canal IRC, etc.

La solución estará en capacidad de proveer la suficiente informacion para llevar acabo las labores de inteligencia en las redes sociales y medios de comunicación que publican su información en internet, los objetivos a cumplir con esta solución son:

- Conectar a todos los sitios de Internet y los medios sociales y averiguar lo que las personas están diciendo.
- Proporcionar al personal de las fuerzas la ventaja del análisis integral en eventos ante un suceso ocurrido en las fuerzas
- Saber quién está hablando de nuesta insituticion y los hechos que la rodean
- Reaccionar rápidamente a las crisis social. Conocer en tiempo real acerca de los tweets falsos y dañinos.
- Monitor toda fuente considerada como competencia o enemigo, tendencias de la industria militar, regulación y el cumplimiento
- Monitorizar la información que se expone de los miembros de nuestra institucion y saber que están siendo percibidos.

ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

LAS ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO PODRAN SER CONSULTADAS POR LOS INTERESDADOS EN LAS INSTALACIONES DE LA OFICINA DE CONTRATOS DE LA CENAC ESPECIALIZADA INTELIGENCIA UBICADA EN LA CARERRA 8 A No. 101 – 3 PISO 2 DE LA CIUDAD DE BOGOTÁ D.C., PREVIO DILIGENCIAMIENTO Y SUSCRIPCIÓN DEL CORRESPONDIENTE COMPROMISO DE CONFIDENCIALIDAD.

NOTA 1: CON TODO Y LOS ANTERIOR, LOS INTERESADOS DEBERÁN SUJETARSE A LOS MECANISMOS DE RESERVA DE LA INFORMACIÓN QUE LE IMPARTA LA CENAC ESPECIALIZADA INTELIGENCIA, CONFORME A LO SEÑALADO EN EL ARTICULO 33 DE LA LEY 1621 DE 2013.

NOTA 2: LA INFORMACIÓN QUE CONTIENE LA FICHA TÉCNICA Y LA DEFINICIÓN DE LA NECESIDAD SOLO PODRÁ SER RETIRADA DE FORMA PERSONAL POR EL REPRESENTANTE LEGAL DE LA FIRMA

Patria, Honor, Lealtad
"Dios en todas nuestras actuaciones"
Fe en la causa
Cra. 8A No. 101-33 Piso 2 Bogotá D.C.
Conmutador 6004900 Ext. 2085
contratos.neaime@ins.mil.co

Página 15 de 48

No obstante, existe otra justificación para la adquisición en la Resolución 243 de 2016 del CENAC Ejército Nacional en que se señala que la adquisición se realiza para “fortalecer la capacidad de guerra electrónica” del ejército y se solicita que la información al respecto sea reservada.

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
EJÉRCITO NACIONAL
CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA (CENAC) INTELIGENCIA

TODOS POR UN NUEVO PAÍS

RESOLUCIÓN No 243
(13 de Diciembre de 2016)

POR LA CUAL SE ADJUDICA EL PROCESO DE CONTRATACIÓN DIRECTA CUANDO NO EXISTA PLURALIDAD DE OFERENTES No. 325-DIADQ-CADCO-CENACINTELIGENCIA-2016, EL CUAL TIENE POR OBJETO LA "ADQUISICIÓN DE EQUIPO DE INTELIGENCIA CON AMPLIACION DE LICENCIAMIENTO Y ARQUITECTURA DE HARDWARE PARA EL SISTEMA DE FUENTES ABIERTAS DEL EJÉRCITO NACIONAL

EL DIRECTOR DE LA CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA CENAC DE INTELIGENCIA, quien actúa en nombre y representación de **LA NACIÓN - MINISTERIO DE DEFENSA NACIONAL - EJERCITO NACIONAL**, en su calidad de **ORDENADOR DEL GASTO**, previamente facultado cumpliendo con el plan de revelo comando de unidades operativas mayores, menores, táctica; jefaturas y direcciones, igualmente de conformidad a lo preceptuado por la Ley 80 de 1.993, Ley 1150 de 2.007, Decreto Reglamentario 1082 de 2015, **Resolución número 4519 del 27 de mayo del 2016 Artículo 9 numeral 9.2** (Por la cual se delegan una funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa Nacional, a las Fuerzas Militares y la Policía Nacional y se dictan otras disposiciones) Expedida por el Ministerio de Defensa Nacional, Resolución Número 6345 de 2012 (Manual de Contratación del Ministerio de Defensa Nacional y sus Unidades Ejecutoras), Directiva Permanente No.09 del 20 de Marzo de 2014 (políticas de Contratación Sector Defensa de Recursos Ordinarios y Extraordinarios) expedidas por el Ministerio de Defensa Nacional; quien en consecuencia representa, por la delegación conferida y demás normas concordantes y complementarias; quien en consecuencia representa, por la delegación conferida, y

CONSIDERANDO

Que mediante Resolución de Delegación No. Resolución número 4519 del 27 de mayo del 2016 Articulo 9 numeral 9.2, el Señor Ministro de Defensa Nacional, debidamente facultado por los artículos 211, 216 y 217 de la Constitución Política; el artículo 12 de la Ley 80 de 1993; los artículos 9, 10 y 12 de la Ley 489 de 1998; el artículo 37 del Decreto 2150 de 1995; artículo 110 del Decreto 111 de 1996; y la Ley 1150 de 2007, delegó parcialmente a esta Dependencia, la celebración, modificación, adición, prórroga, liquidación y terminación de contratos, así como los demás actos inherentes a la actividad contractual, cuando la cuantía sea desde 0 hasta 10.000 S.M.L.M.V.

NECESIDAD ADQUISICIÓN DE EQUIPO DE INTELIGENCIA CON AMPLIACION DE LICENCIAMIENTO Y ARQUITECTURA DE HARDWARE PARA EL SISTEMA DE FUENTES ABIERTAS DEL EJÉRCITO NACIONAL
DEFINICIÓN DE LA NECESIDAD

El presente proceso contiene información de carácter **RESERVADO**, por lo que se requiere dar el manejo a la misma, de acuerdo con lo estipulado en la ley estatutaria No. 1621 de 2013 o ley de inteligencia, así como lo reglamentado en el decreto 857 de 2014, si se tiene en cuenta que se trata de capacidades tecnológicas que tienen que ver de manera directa con la Defensa y Seguridad Nacional.

Finalmente me permito solicitar, no publicar cualquier información adicional dentro de los diversos apartes y documentos del proceso de contratación directa, considerando que se trata de una actividad que tiene por objeto fortalecer la capacidad de GUERRA ELECTRÓNICA DEL EJÉRCITO NACIONAL, siento esta una de las capacidades estratégicas del Estado Colombiano para la Defensa y Seguridad Nacional, dando estricto cumplimiento a lo ordenado en el marco de la ley estatutaria de Inteligencia No. 1621 de 2013.

Que conforme a la solicitud de oferta analizado el objeto del presente proceso y teniendo en cuenta lo definido por el Gerente de Proyecto en la necesidad establecida en del estudio previo, el cual trata de la "**ADQUISICIÓN DE EQUIPO DE INTELIGENCIA CON AMPLIACION DE LICENCIAMIENTO Y ARQIITECTURA DE HARDWARE PARA EL SISTEMA DE FUENTES ABIERTAS DEL EJÉRCITO NACIONAL**" y considerando que la firma **GAMMA INGENIEROS S.A.S.**, es la única firma que puede suministrar el objeto del presente contrato, toda vez que es la única empresa autorizada por el fabricante en Colombia para la distribución de los bienes y servicios objeto del presente proceso de selección.

Conforme documentos de contrato de distribuidor de soluciones 4IQ, el segundo en representación legal de la compañía GAMMA INGENIEROS S.A.S., (...) derecho, en lo sucesivo denominada el distribuidor.

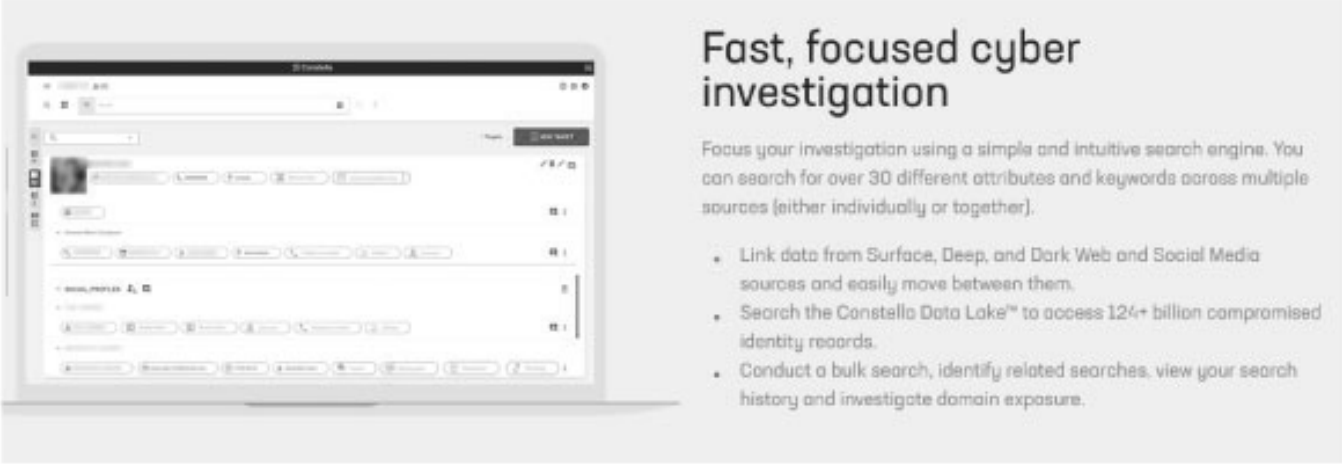
Que el presupuesto oficial para el presente proceso otorgado por el M.D.N. - EJÉRCITO NACIONAL - CENAC INTELIGENCIA es por **TRESCIENTOS SETENTA MILLONES PESOS MONEDA CORRIENTE ($370.000.000,00)M/CTE INCLUIDO IVA**, los cuales se encuentran amparados así:

Con el Certificado de Disponibilidad Presupuestal No. 38116 de fecha **DIECISIETE** (17) de noviembre de **DOS MIL DIECISÉIS** (2016), posición en el catálogo de gasto **A-2-0-4-3-3 EQUIPO DE INTELIGENCIA**, Fuente Nación, Recurso 10, Situación CFS; expedido por el Jefe de Presupuesto de la **CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA**

Respecto al producto comprado, GAMMA Ingenieros, era distribuidor de 4IQ, una empresa española, ahora llamada Constella Intelligence que provee herramientas de inteligencia basadas en búsqueda en fuentes abiertas. Constella cuenta con dos herramientas[13], **Dome y Hunter**, que tienen las características y capacidades que requiere el contrato.

Ambas herramientas realizan búsqueda en diversas fuentes de internet y prometen lograr identificación individual de perfiles anonimizados a través de la búsqueda de posibles conexiones y el cruce de información en internet, Dark Web y medios de comunicación.

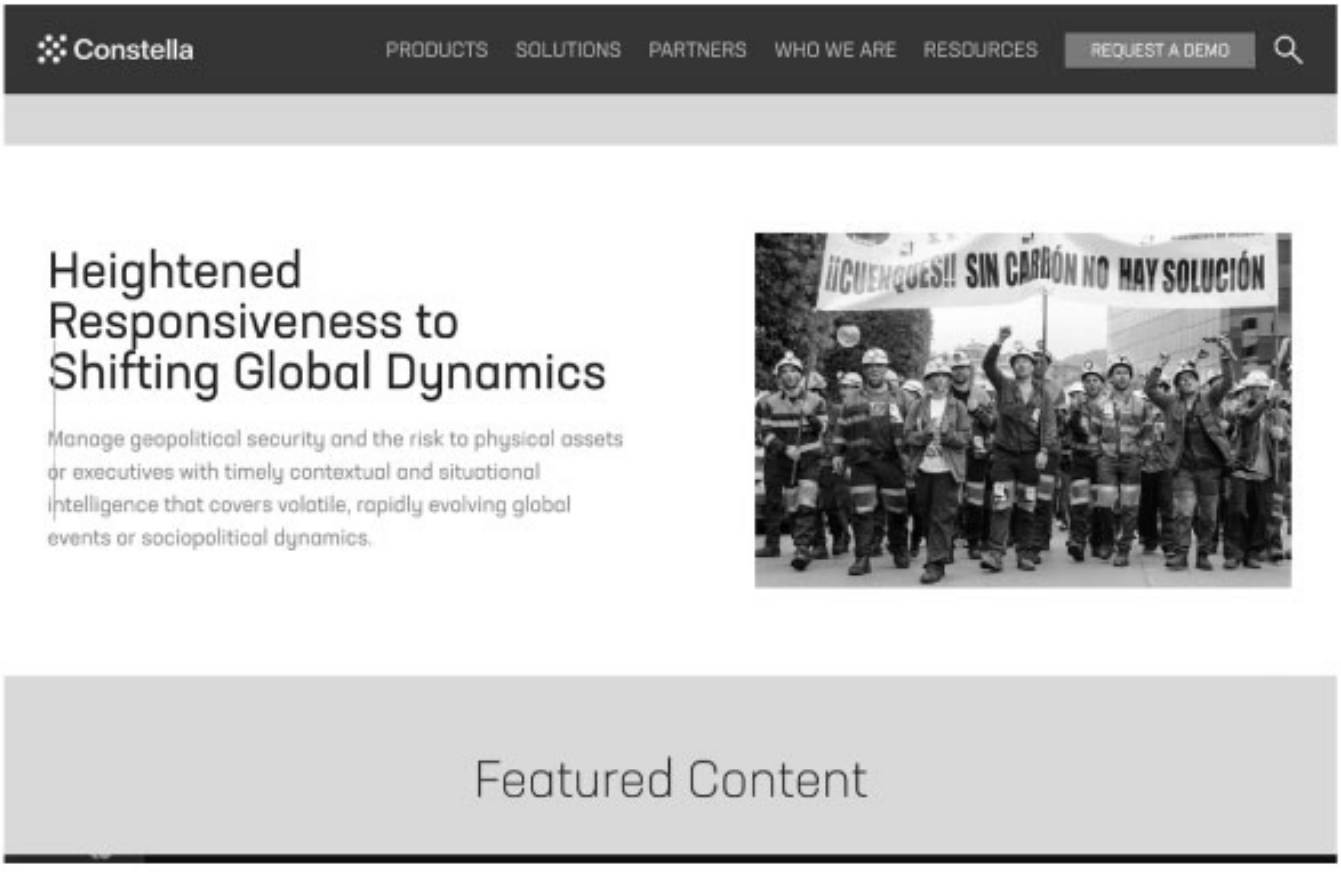
13. Hunter. Cyber Investigations | Investigate & Attribute Anonymous Threat Actors. Disponible en: https://constellaintelligence.com/our-offer/cyber-investigation-software-hunter/



Captura de pantalla del programa Hunter exhibida por la empresa para la promoción. Tomada de la página oficial de Constella Intellige[14].

Además, la empresa ofrece productos para la Geopolitical Intelligence Monitoring[15]. Señalando que los mismos serán útiles para defenderse en caso de "cambios relevantes en la opinión pública, hacktivismo y disturbios sociopolíticos". Adicionalmente aseguran encontrar "discursos sospechosos en social media", promoción que está acompañada de imágenes referentes a protesta social. Es decir, herramientas OSINT diseñadas específicamente para vigilar y contrarrestar los derechos a la libertad de expresión y la protesta.

14. Disponible en: https://constellaintelligence.com/our-offer/cyber-investigation-software-hunter/
15. Disponible en: https://constellaintelligence.com/use-cases/geopolitical-intelligence-monitoring/



Finalmente, en los requerimientos técnicos adicionales mencionan que "el proveedor se compromete a garantizar la visualización geográfica en mapas para el análisis de tendencias de objetos en redes sociales".

4. Los agentes encubiertos de la Fiscalía General en internet. OSINT para la investigación criminal

Para los años 2022 y 2023, la Fiscalía adquirió con Deinteko SAS la actualización de 8 licencias, soporte técnico de Tangle y 1 módulo de Dark Web propiedad de la Fiscalía (en 2019 se adquirieron las licencias originales[16]). En este caso, Deinteko, actúa como filial de la empresa Israeli, COBWEBS TECHNOLOGIES LTD[17] y es su tercer contrato para proveer OSINT.

El sistema permite a los analistas del CTI hacer análisis por delitos (al parecer cualquier tipo de delito) y entregar datos para los perfiles de la Fiscalía a partir de información disponible en redes sociales, seguimiento de tendencias, rastreo de imágenes. Esta información, señala el contrato, será utilizada para investigaciones, judicializaciones, estudios de comportamiento humano, perfiles de seguridad, evaluación de mercado, opinión, sentimientos y contenido y

16. Véase en SECOP II, en: https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2707499&isFromPublicArea=True&isModal=False
17. Disponible en: https://cobwebs.com/

para determinar actividades online, direcciones de correo y celulares, páginas web, servidores y perfiles de redes sociales.

Tangle[18] monitorea buscadores como Google, Yahoo, BING, ASK, OAL y permite determinar nombre, perfiles, correo, teléfonos, hashtag y Alias de usuarios de redes sociales como Facebook, Twitter, Instagram, LinkedIn y Telegram. En esta ocasión se agregó un módulo para la Dark Web, pero la versión original opera desde el 2019 (adquirido en el contrato No. 0054 de 2019) la cual permitía buscar en fuentes abiertas de internet y en 2020 se compró un módulo para rastrear fuentes no indexadas a las cuales se accede mediante TOR.

La herramienta ya ha servido para búsqueda de personas en redes sociales y para la aplicación de la figura de agente encubierto virtual y las infiltraciones de estructuras criminales, según se especifica en los documentos del contrato. Estás búsquedas se realizan, para actividades de policía judicial, bajo la figura de agente virtual y utilizan técnicas de penetración e infiltración, respecto de delitos relacionados que afectan: medio ambiente, derechos humanos, administración pública, narcotrafico, los que implican extinción de dominio, terrorismo, delitos informáticos y priorizados.

El agente encubierto virtual, fue consagrado en el artículo 242B del Código Procesal Penal[19]. El agente encubierto, artículo 242, establece que en caso de que se sospeche de forma sustenta que un indiciado o imputado continúa cometiendo delitos y con previa autorización del Director Nacional o Seccional de Fiscalías, siempre y cuando resulte indispensable, podrá utilizar un agente encubierto "condición y realizar actos extrapenales con trascendencia jurídica". Es decir, de infiltrar un agente, que puede cometer ciertos delitos con el fin de recolectar pruebas. Ahora bien, el agente encubierto virtual, debe, además, verificar "la posible existencia de hechos constitutivos de delitos cometidos por organizaciones criminales que actúan a través de comunicaciones mantenidas en canales cerrados de comunicación virtual"[20] y, en todo caso, deberá contar con una autorización previa por parte del Juez de Control de Garantías para interferir en las comunicaciones, de conformidad con lo dispuesto en la jurisprudencia constitucional.

Ahora bien, en el caso de la Fiscalía hay un segundo contrato. Se trata de un curso de capacitación para sus funcionarios en el uso de herramientas OSINT y hacking ético. El curso tiene el rimbombante nombre de OSINT PRO: Búsqueda de información en fuentes abiertas AGENTE ENCUBIERTO EN MEDIOS DE COMUNICACIÓN VIRTUAL.[21]

---

18. Gobierno compró $2.2 millones en equipo de espionaje a empresa de amigo israelí de Bukele. El Faro. Disponible en: https://elfaro.net/es/202301/el_salvador/26687/Gobierno-compr%C3%B3-$22-millones-en-equipo-de-espionaje-a-empresa-de-amigo-israel%C3%AD-de-Bukele.htm
19. Ley 906 de 2004. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr005.html#242A
20. Código Procesal Penal. Art 242B. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr005.html#242
21. Véase en SECOP II en: https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.1876223&isFromPublicArea=True&isModal=False

El programa se justifica bajo la necesidad de aprender cómo operan los ciberdelincuentes para mejorar las técnicas, herramientas y metodologías con el objetivo de investigar a la Policía Judicial. La idea es enseñar a indagar en: "ataques informáticos al sector financiero, protección de la información y de los datos, transferencias no consentidas, hurto por medios informáticos, accesos abusivos, comercialización y tráfico de estupefacientes, sexting y sextorsión etc. También para investigar organizaciones criminales que utilicen medios informáticos, redes sociales y de telecomunicaciones para la comisión de conductas punibles".

En últimas, la Fiscalía contrató un programa académico para que sus agentes encubiertos tengan conocimientos tecnológicos especializados para analizar archivos ilícitos, redes sociales, recolectar información tanto en imágenes como en audios y tener la capacidad de analizar sus algoritmos.

THD- OSINT PRO (Búsqueda de Información en Fuentes Abiertas)

OSINT PRO

La Inteligencia de Fuente Abierta (OSINT) es un elemento crucial de todo tipo de organizaciones tanto gubernamentales como privadas. Las últimas dos décadas han visto a OSINT trascender desde las fuentes abiertas tradicionales, como los periódicos, la radio, a fuentes modernas como lo es internet.

En el **THD-OSINT PRO** el asistente aprenderá técnicas de inteligencia de código abierto de avanzada para la búsqueda de información de personas o empresas, este curso permitirá aprender de una forma práctica las distintas técnicas de inteligencia existentes en fuentes abiertas (Open Source Intelligence–OSINT), que en la actualidad proporcionan más del 80% de la información útil obtenida por los servicios de inteligencia. Este programa proveerá a los participantes involucrados en operaciones de inteligencia con lo último en conocimientos y potencial de OSINT, haciendo hincapié en la recuperación de inteligencia en línea.

La formación está pensada para ser ejecutada en forma de laboratorio, donde los asistentes puedan ejecutar las distintas herramientas y llevar a cabo ejercicios prácticos que les permitan conocer las capacidades de las mismas en procesos de investigación.

No obstante, resulta extraño que el curso consiste en la enseñanza de elementos básicos del uso de internet, para realizar búsquedas básicas y avanzadas en la red y diferenciar contenido real del falso. De forma tal que se enseña conceptos como qué es inteligencia, cómo funciona Google, cómo crear una cuenta encubierta, cómo usar Tor, se señalan motores y páginas para realizar búsquedas, uso de redes sociales básicas (incluida Tik Tok). De igual forma, el programa ciber para promocionar la página web ciberpatrulla.[22]

5. Policía Nacional contrató la implementación de un sistema de monitoreo masivo de internet

En 2021 la Policía Nacional adquirió con la Unión Temporal Phoenix[23] un "sistema de ciberinteligencia basado en inteligencia artificial" que incluye software, hardware y desarrollos necesarios. El sistema tiene integradas "diversas fuentes de información abiertas, información estructurada y no estructurada, así como información y contenido dispuesto en internet, con el fin de enriquecer el análisis y la elaboración de productos prospectivos y anticipativos" a través de la generación de gráficos y alertas. Una herramienta que Phoenix define como un "sistema de monitoreo masivo de internet".[24]

22. Disponible en: https://ciberpatrulla.com/
23. Integrada por Newsat SAS y por Mollitiam Industries SL
24. Búsquese en SECOP II, ingresando a la pestaña de búsqueda de procesos de contratación. Elimine los datos de fecha del formato e ingrese en la casilla de número del proceso: PN DIPOL SA MC 027-2021

PHOENIX EN EL CICLO DE INTELIGENCIA

PHOENIX es un sistema de monitoreo masivo en Internet para generar inteligencia a partir de la descarga anónima de datos provenientes de Redes Sociales, Darknets y otras fuentes abiertas o cerradas que se integren.

La herramienta recolecta datos de la web pública, la Deep Web y Darknet a través de "técnicas de OSINT", minería de datos y análisis de redes sociales siempre con el fin de apoyar operaciones de la policía. En las especificaciones del contrato se señalan entre las necesidades de la policía que suplirá el software las de hacer "seguimiento de tendencias mediáticas en redes sociales", "identificación de noticias falsas", "análisis de redes" y una inteligencia artificial predictiva.

N°	SUJETO	ARTICULOS	
1	Gestión de usuarios: 30 min	1.	Adicionar nuevos usuarios
		2.	Conectar un email a cada usuario
		3.	Defina usuarios regulares y administradores y podría cambiar el usuario correcta y fácilmente
		4.	Cambiar la contraseña
		5.	Bloquear y desbloquear usuarios
2	Asignación y Gestión del espacio de trabajo a usuarios- 10 min	6.	Adicionar nuevos espacios de trabajo, o asignar roles de los módulos
		7.	Definir usuario activo y no activo
		8.	Cambiar los usuarios en cada espacio de trabajo
		9.	Administre la política de retención para cada espacio de trabajo
3	Manejo de cuentas de navegación -15 min	10.	Importar números masivos de cuenta de navegación (al menos 500)
		11.	Sube cuenta de navegación configurados de todas las redes sociales
		12.	Definir si la cuenta de navegación se usa a través de API / o login
		13.	Crea cuenta de navegación con algunas redes sociales
4	Auditoria 10 min	14.	Mostrar el panel o módulo de administrador
		15.	Permite personalizar un tablero para administrar todos los datos de auditoria
		16.	Visualizar todas las acciones principales realizadas en el entorno divididas por tiempo, usuarios, espacios de trabajo o módulos y más
		17.	Auditar las actividades de todos los usuarios del sistema.
5	Capacidades de análisis: 1 hora y 50 min	18.	Análisis de temas y discursos
		19.	Línea de tiempo en un gráfico
		20.	Análisis de sentimientos
		21.	Influenciadores
		22.	Análisis geográfico en un mapa
		23.	Información demográfica
		24.	Principales interactores
		25.	Detección de cuentas falsas
		26.	hashtags principales
		27.	URL principales
		28.	Análisis de entidades: Cuentas de redes sociales
		29.	Contenido que incluye a los principales interactores, participantes
		30.	Acerca del Usuario: Conexión agrupada por lugar de trabajo, ciudad natal, educación, grupos internos, fuerza de conexión, cuentas falsas.
		31.	Análisis de grupo Intersección entre dos entidades.

	32.	Principales interactores de una página web o red social
	33.	Acerca de la página
	34.	Fans superiores de la página
	35.	Publicaciones principales
	36.	Análisis organizacional: cuentas de redes sociales, los mejores interactores, presencia web, posibles miembros
	37.	Demostrar la recolección de horarios: Recolectando la información cada X cantidad de tiempo, de acuerdo a la programación que tenga el sistema.
	38.	Nuevas fuentes: mostrar toda la información que se recopiló utilizando los nuevos buscadores que se crearon.
	39.	Recolección Dark Web: mostrar los diferentes filtros que se pueden usar, motores de búsqueda Darknet
Biblioteca algoritmos de búsqueda	40.	Algoritmos de búsqueda en redes sociales
El sistema Debe obtener una biblioteca de algoritmos de búsqueda a la que se pueda acceder fácilmente desde varias pantallas, Mostrar las siguientes fuentes: 15 min	41.	Facebook
	42.	Twitter
	43.	YouTube
	44.	Instagram
	45.	Algoritmos Surface web: Motores de búsqueda (por lo menos 5 al mismo tiempo)
	46.	49. Web pages
	47.	RSS
	48.	DarkNet: motores de búsqueda, web pages
Consulta: El usuario debe poder controlar la recopilación de datos: 20 min	49.	Insertar diferentes tipos de entrada (nombres de usuario, ID de usuario)
	50.	Cambiar el nombre de la consulta
	51.	Se puede definir qué agente virtual recogerá los datos.
	52.	Crear una tarea de recopilación programada
	53.	Definir la cantidad de tiempo que se realizará la recolección.
	54.	Escribir una descripción para cada consulta
	55.	Agregar múltiples consultas
	56.	Definir a qué caso va esta consulta
Reintentar mecanismo: 5 min	57.	Demuestre que el sistema sabe cómo superar el bloqueo de una cuenta de navegación propia para consultas y enviar al menos tres agentes virtuales diferentes de forma automatizada para realizar una sola consulta.
Geo-cercado: 7 min	58.	Generar una consulta señalando un área geográfica específica, devolviendo resultados de un área específica
Medios de comunicación – Búsqueda de cuenta: 10 min	59.	Encuentre diferentes nombres de identidad basados en palabras clave en las siguientes redes: Facebook Twitter Instagram
	60.	Recopilar información sobre las cuentas directamente desde la pantalla de búsqueda
	61.	Facebook identidad: feed (comentaristas, reacciones), conexiones, acerca de (ingresos, páginas), ubicaciones
	62.	Página de Facebook: feed (comentaristas, reacciones), interactores de página, acerca de la página
	63.	Grupo de Facebook: feed (comentaristas, reacciones), miembros del grupo
	64.	Facebook post, comentaristas, reacciones seguidores, búsqueda genérica – palabras claves

	61.	Facebook identidad: feed (comentaristas, reacciones), conexiones, acerca de (ingresos, páginas), ubicaciones
	62.	Página de Facebook: feed (comentaristas, reacciones), interactores de página, acerca de la página
	63.	Grupo de Facebook: feed (comentaristas, reacciones), miembros del grupo
	64.	Facebook post, comentaristas, reacciones seguidores, búsqueda genérica – palabras claves
	65.	Twitter: Identidad
	66.	Feed (comentaristas, reacciones)
	67.	Seguidores
Colección de redes sociales: 20 min	68.	Hashtags
	69.	Cuenta mencionada
	70.	Retweets
Venta de autopartes de carros motos y bicicletas	71.	Búsqueda genérica – palabras claves
	72.	Instagram: Identidad
	73.	Feed (comentaristas, reacciones)
	74.	Hashtags
	75.	User location
	76.	Seguidores
	77.	Page locations
	78.	YouTube: identidad
	79.	YouTube búsqueda – Avanzada
	80.	YouTube búsqueda
Web Page: 5 min	81.	Elija cualquier sitio web normal y muestre las capacidades de recopilación
Motores de búsqueda: 5 min	82.	Mostrar la colección de los motores de búsqueda: esto debe incluir al menos 5 diferentes
RSS: 5 min	83.	Colección RSS Feeds
Motores de búsqueda: 5 min	84.	Mostrar la colección de los motores de búsqueda de dark net
Web page: 5 min	85.	Mostrar la colección de un sitio web oscuro específico (TOR)
Telegram: 5 min	86.	Mostrar la colección de un canal de Telegram público con una cuenta de navegación dedicada
	87.	El sistema debe poder agregar nuevas fuentes a la lista.
Adicionar nuevas fuentes: 10 min	88.	Crear y agregar Foros – dark web y surface web
	89.	Crear y agregar noticias webste
	90.	Data base Online
	91.	Crear y agregar un Excel
	92.	Búsqueda por un parámetro que tenga la herramienta
Parámetros de búsqueda de entidad: 10 min	93.	Búsqueda por Email
	94.	Búsqueda por número de cédula
	95.	Búsqueda por Facebook ID
	96.	Búsqueda por Twitter ID
	97.	Búsqueda por Instagram ID
	98.	Crear un informe dentro del sistema.
	99.	Imágenes de entidad
	100.	Nombres

	106.	Visualiza el flujo de investigación y muestre la conexión entre las diferentes pruebas encontradas.
	107.	Medios de comunicación
Exportar: 8 min	108.	Exportar el informe en formato PDF
	109.	Exportar informe en formato JSON
	110.	Exportar informe en otro formato
	111.	Mostrar los reportes
Extracción de entidad: 10 min	112.	Organizaciones
	113.	Nombres de entidad
	114.	URL
	115.	Etiquetas
	116.	Localizaciones
	117.	Idiomas
	118.	Fuentes
Búsqueda basada en palabras: 5 min	119.	Crear una lista dedicada de palabras para buscar en una de las consultas
	120.	Muestre que el sistema lo extrajo
Clasificación cuentas falsas: 8 min	121.	Clasificar las cuentas en Facebook y Twitter como falsas
	122.	Mostrar los motivos de clasificación
Clasificación: 5 min	123.	Ordenar la información según tiempo de publicación
	124.	Ordenar la información según fuente
	125.	Ordenar la información según Compromiso
	126.	Ordenar la información leído / No leído
Exporte: 8 min	127. formatos.	Mostrar las capacidades de exportación del feed y de otras características del sistema, incluidos CSV, PNG, i2 y otros
Medios y Display: 5 min	128.	Mostrar imágenes y videos.
	129.	Mostrar cómo el usuario puede descargar todas las imágenes y videos.
	130.	Mostrar los resultados en "Modo de chat" en aplicaciones.
Datos resumidos: 8 min	131.	Nube de palabras
	132.	Línea de tiempo en un gráfico
	133.	Sentimiento
	134.	Conexiones de hashtags en un gráfico
	135.	Demografía en un gráfico
	136.	Mejores influenciadores
	137.	Distribución de cuenta falsa
Geo-Analysis: 10 min	138.	Muestra la información en un mapa que se puede cambiar.
	139.	Mostrar puntos calientes en función de la cantidad de resultados
Análisis de relaciones – Análisis link: 15 min	140.	Agrupar los resultados por ciudad de nacimiento
	141.	Agrupar los resultados por ciudad actual
	142.	Agrupar los resultados por lugar de trabajo
	143.	Agrupar los resultados por nombre y apellido
	144.	Grupos internos – mostrar la relación entre las conexiones de grupos para encontrar aquellos que sean de interés
	145.	Fuerza de conexión – muestra la fuerza de la conexión basada en me gusta, comentarios, pariente, etc.
	146.	Intersección – muestra la intersección de las conexiones de algunas cuentas para encontrar conexiones mutuas.
Lista de entidades con actividad inusual: 5 min	147.	Marcar cuenta
	148.	Gestionar lista
Alertas: 10 min	149.	Generar como mínimo 4 tipos de alertas y vistas guardadas
	150.	Alerta basada en geografía
	151.	Alerta basada en feed
	152.	Alerta indicativa basada en palabras

Análisis de relaciones – Análisis link: 15 min	140.	Agrupar los resultados por ciudad de nacimiento
	141.	Agrupar los resultados por ciudad actual
	142.	Agrupar los resultados por lugar de trabajo
	143.	Agrupar los resultados por nombre y apellido
	144.	Grupos internos – mostrar la relación entre las conexiones de grupos para encontrar aquellos que sean de interés
	145.	Fuerza de conexión – muestra la fuerza de la conexión basada en me gusta, comentarios, pariente, etc.
	146.	Intersección – muestra la intersección de las conexiones de algunas cuentas para encontrar conexiones mutuas.
Lista de entidades con actividad inusual: 5 min	147.	Marcar cuenta
	148.	Gestionar lista
Alertas: 10 min	149.	Generar como mínimo 4 tipos de alertas y vistas guardadas
	150.	Alerta basada en geografía
	151.	Alerta basada en feed
	152.	Alerta indicativa basada en palabras
	153.	Envío de alerta por correo electrónico
Visualizando el flujo de investigación: 10 min	154.	Muestra una visualización gráfica del flujo de investigación completo.
	155.	Conectar diferentes tipos de entidades (cuentas sociales, teléfonos, correos electrónicos, etc.)

Las redes sociales cuyas dinámicas son monitoreadas son Facebook, Telegram, Twitter, Instagram y las de mensajería instantánea que cuenten con links públicos, pero podrán incorporar nuevas fuentes. Respecto de cada publicación, hashtag, comentario, imagen en redes, el sistema determina: cuenta de la primera publicación, impacto y reacciones, cuentas de mayor interacción, geolocalización de las cuentas en función de información pública y cantidad de seguidores. Es importante señalar que este sistema no solo usa fuentes abiertas sino que cruza información y usa fuentes cerradas de la policía. Dado que el sistema genera alertas automáticas, este debe hacer monitoreo en vivo todo el tiempo.

Llama la atención que el sistema también está dirigido a mapear y extraer información de redes sociales de entidades. De las cuales determina su entorno social e interacciones, esto implica el seguimiento de algunas organizaciones concretas. Además, el sistema de la policía debe determinar qué perfiles son un bot, es decir, si la cuenta es real o falsa. La clasificación se realiza a partir de los horarios, tiempos de interacción, fechas y tiempo de uso y la correlación con otras redes.

La herramienta recolecta datos de la web pública, la Deep Web y Darknet a través de "técnicas de OSINT", minería de datos y análisis de redes sociales siempre con el fin de apoyar operaciones de la policía. En las especificaciones del contrato se señalan entre las necesidades de la policía que suplirá el software las de hacer "seguimiento de tendencias mediáticas en redes sociales", "identificación de noticias falsas", "análisis de redes" y una inteligencia artificial predictiva.

20 años Fundación Karisma

PRIVACY INTERNATIONAL

Cuando el Estado vigila

Ciberpatrullaje y OSINT en Colombia

Un Informe de la Fundación Karisma que evalúa las capacidades tecnológicas del Estado colombiano para vigilar internet a través de software de inteligencia de fuentes abiertas de inteligencia (OSINT)