Sobre el “Proyecto de protocolo de ciberpatrullaje”

22 ABRIL 2020

CELS
CENTRO DE ESTUDIOS LEGALES Y SOCIALES

Piedras 547, p1º (C1070AAK) CABA, Argentina
tel/fax (+5411) 4334-4200
consultas@cels.org.ar
www.cels.org.ar

Observaciones del CELS a la Resolución 31/2018 y al “Proyecto de protocolo de ciberpatrullaje”

En este documento presentamos nuestras consideraciones sobre la Resolución 31 del 26 de julio de 2018, que instruye a las áreas de investigación de Ciberdelitos de las fuerzas de seguridad federales a intervenir en una serie de delitos, y sobre el Proyecto de Protocolo de “Ciberpatrullaje”, propuesto por el Ministerio de Seguridad de la Nación el 17 de abril de 2020.

Resolución 31/2018

La resolución es una instrucción de carácter general en la que el secretario de Seguridad instruye a las áreas de Ciberdelito de las fuerzas federales para “tomar intervención” en un conjunto definido de delitos a través de “actos investigativos” que deben realizarse en sitios digitales de acceso público.

Por su nivel de generalidad, esta resolución no puede ser considerada un protocolo de actuación: no define claramente las características de los “actos investigativos” ni los escenarios en los que podrían iniciarse. Por un lado, se infiere que podría tratarse de actuaciones sin orden ni control judicial ya que según el artículo 2 una vez “reunidos los medios probatorios necesarios” se establecería el contacto con los funcionarios judiciales. Por otro lado, la definición acotada de los delitos enumerados impediría las tareas de vigilancia indiscriminada.

Sin embargo, el carácter general y difuso de este instrumento genera zonas grises al no aclarar qué tipo de decisión (y tomada por qué actor) es la que podría iniciar las intervenciones de las áreas dedicadas a los ciberdelitos.

El caso de Kevin Guerra fue iniciado por la Subdirección de Investigación de delitos tecnológicos de Gendarmería con un informe (adjunto) que muestra todas estas falencias y el riesgo que supone habilitar este tipo de prácticas per se. La GNA justifica su intervención en la resolución de Bullrich, pero lo hace excediendo por completo lo que allí se habilitaba. Realiza una expedición de pesca. Luego emite un informe ilegal que da inicio a una causa por intimidación pública. Los problemas de esta actuación se multiplicarán si se avanza con el proyecto de protocolo en estudio que no solo no limita la intervención policial sino que la amplia.

Proyecto de Protocolo de Ciberpatrullaje

El proyecto del 17 de abril de 2020 busca constituirse como un protocolo de actuación que especifique y clarifique lo dispuesto en la resolución anterior. Sin embargo, acumula varios problemas: de legalidad de las acciones que define y busca regular, así como de proporcionalidad y de necesidad. Al mismo tiempo, implica amenazas directas e indirectas para la vigencia de la libertad de expresión y el derecho a la privacidad.

I. UNA ANALOGÍA PROBLEMÁTICA: NO ES PREVENCIÓN SINO INTELIGENCIA SOBRE FUENTES ABIERTAS

El Ministerio presenta a la noción de “ciberpatrullaje” como sinónimo de la “prevención del delito en entornos digitales”. Implícitamente, se busca trazar una analogía entre la tarea policial de patrullaje en las calles y el espacio físico - desde hace años, las gestiones de distinto signo político, basan sus políticas en la “presencia policial” y la “prevención situacional” por sus efectos disuasorios- y una supuesta “prevención del delito” en el ciberespacio. Esta última descansaría en la posibilidad de que las fuerzas policiales monitoreen y vigilen de manera indiscriminada y sistemática las fuentes abiertas buscando a quienes están cometiendo un delito o a quienes expresen que estarían por hacerlo. Esta analogía es engañosa y busca presentar al “ciberpatrullaje” como una actividad distinta a las de inteligencia.

El proyecto define las tareas de “ciberpatrullaje” como prácticas de monitoreo, observación y análisis de información de la actividad de las y los ciudadanos en las redes sociales (inc. 1º) para detectar hechos que configuren delitos, actividades que eventualmente pueden resultar criminales o aportar información sobre la comisión de delitos. En los considerandos se explica que “el ciberpatrullaje debe ser entendido como una técnica policial profesional y específica, la cual implica para su desarrollo el empleo de saberes y tecnologías tendientes a la recolección y análisis de información general y pública, obtenida de fuentes abiertas y digitales por personal calificado para dicha tarea, con la finalidad de identificar hechos, prácticas y eventos que afecten la seguridad interior, según establece la ley 24.059”**.**

Lo que se desprende de los artículos 2, 3 y 4 del proyecto de protocolo es que habilita a los organismos de las fuerzas de seguridad a buscar información en fuentes de internet abiertas para detectar y alertar sobre la comisión de eventuales delitos. Esto no es “patrullaje”, son tareas de inteligencia criminal.

¿Pueden las áreas de seguridad y policías realizar tareas de inteligencia criminal? Pueden, pero bajo ciertos límites y autorizaciones legales. Ni este reglamento, ni una ley podrían autorizar una herramienta para realizar vigilancia indiscriminada, sin hipótesis delictivas previstas, lo que se conoce como “excursiones de pesca”, para ver si alguien está cometiendo delitos en el entorno digital. Eso está prohibido.

Las definiciones del proyecto de protocolo sobre lo que no se puede hacer, como la “observación de individuos” es meramente retórica y técnicamente incorrecta. Los casos que se hicieron públicos con la regulación anterior y con esta lo demuestran. La habilitación es tan amplia que no hay forma de que se restrinja su uso frente a personas porque el objetivo del protocolo es justamente identificar autores de delitos y no un análisis de posibles fenómenos criminales. Como ejemplo volvemos al caso de Kevin Guerra: la Gendarmería buscó en redes sociales las palabras “saquear-cuarentena-argentina” y en base a lo que encontró en la cuenta personal de un individuo, sin ningún otro análisis de contexto, inició una causa penal. Esto no es legal.

Por lo tanto, el marco conceptual y jurídico para analizar si son legales las tareas denominadas de “ciberpatrullaje” no es el de la prevención del delito, sino el de la inteligencia criminal. Por lo tanto, la regulación de estas tareas debe atenerse a la normativa sobre seguridad e inteligencia.

La cuestión central a definir es con qué alcance los organismos de seguridad pueden realizar actividades de inteligencia criminal a través de la vigilancia e inteligencia de fuentes abiertas (OSINT) y particularmente de medios sociales (SOCMINT). Pueden hacerlo únicamente cuando están enmarcadas en hipótesis de fenómenos delictivos específicos. Y, aún así, es necesario que esta actividad sea regulada por ley para definir su alcance, herramientas tecnológicas permitidas y controles. Este es un debate que está pendiente en nuestro país, donde no hay nada regulado en este aspecto.

II. EL MARCO NORMATIVO NO HABILITA ESTA PRÁCTICA

La ley 25.520 de Inteligencia Nacional define a la inteligencia como "*la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación*" (art. 2 inciso 1). A su vez, el segundo inciso conceptualiza la inteligencia criminal como "*la parte de la Inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional*".

Es decir: que se trate de información de "fuentes abiertas" no le quita a la actividad de inteligencia su condición de tal. Por ejemplo, la "Estructura orgánica y funcional de la Agencia Federal de Inteligencia" aprobada por decreto 1311/2015 establece que "*la información de inteligencia es aquella que comprende las observaciones y mediciones obtenidas o reunidas de* ***fuentes públicas*** *o reservadas, referidas a eventos o problemáticas relevantes del ámbito de la defensa nacional o de la seguridad interior, o que tienen incidencia en estas esferas, y cuya recolección, sistematización y análisis permite elaborar un cuadro de situación del conjunto de las problemáticas en el nivel estratégico o en el nivel táctico*" (el destacado es propio).

La diferencia con la obtención de información que no es pública se encuentra, en todo caso, en la protección acentuada que la Constitución y la ley le dan a ese tipo de datos y no en la naturaleza de la práctica. (art. 5 de ley 25.520: "*Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario*")

En la ley de Seguridad Interior, la Ley de Ministerios y la Ley de Inteligencia Nacional sólo se habilitan las actividades de inteligencia en relación con "actividades criminales específicas" que afecten determinados bienes jurídicos (la libertad, la vida, el sistema representativo y republicano de gobierno, etc.). Lo mismo sucede si analizamos los artículos del Código Procesal Penal de la Nación sobre las actividades policiales orientadas a la investigación criminal. Según los arts. 183 y subsiguientes, las fuerzas de seguridad y policiales no sólo deben investigar “delitos de acción pública” (es decir, un delito en concreto), sino que cumplen un rol de auxiliares de la justicia.

De acuerdo al marco normativo vigente, la inteligencia criminal no implica una facultad amplia de reunir información de manera indiscriminada, para luego analizar si alguno de los datos obtenidos constituye un indicio de una actividad delictiva. Se requiere de un mínimo grado de sospecha sustantiva respecto de la existencia de determinado fenómeno criminal (de ahí la expresión "específica"), con cierta delimitación espacial, temporal y/o personal, y en relación a la probabilidad de encontrar datos relevantes en la fuente abierta de que se trate.

Nuestro país no tiene una regulación específica sobre estos temas. Los problemas graves de funcionamiento del sistema de inteligencia y de seguridad asociados al espionaje ilegal, al seguimiento de organizaciones, referentes sociales y activistas, a las restricciones a la protesta, a la privacidad, a libertad de expresión y al acceso a la información pública requieren que habilitaciones para hacer inteligencia criminal en el entorno digital (de fuentes abiertas y no abiertas) sean sustentadas en leyes que definan claramente facultades, impongan límites específicos y regulen controles adecuados.

III. PROBLEMAS DE DEFINICIÓN Y DELIMITACIÓN

Establecido que consideramos que las prácticas de “ciberpatrullaje” constituyen una forma de inteligencia criminal y que, por lo tanto, son ilegales de la manera en las habilita en el proyecto, detallamos otros problemas:

En primer lugar, no se define qué se considera que es un “ciberdelito” ni qué artículos del Código Penal y leyes especiales lo comprenden. En este aspecto, el proyecto es un retroceso en relación con la resolución de 2018. Aquella habilitaba las “intervenciones” para un listado cerrado de delitos. En el protocolo en discusión, si bien se manifiesta y se deja asentado en los considerandos un interés relacionado con delitos informáticos, aquellos que se cometen utilizando el acceso a redes sociales e internet en general y se hace mención a la resolución precitada, se permite el “ciberpatrullaje” para todo tipo de delito, por más leves que sean (por ejemplo, en el inciso a del art. 5 del protocolo).

Es particularmente preocupante que se incluya en forma explícita en los considerandos el delito de “intimidación pública” entre los que son de interés. Este delito, de graves problemas de legalidad, es el más utilizado, junto con el de instigar a cometer delitos, por las fuerzas de seguridad a la hora de criminalizar expresiones en

las redes sociales. También fue especialmente utilizado por el gobierno anterior para amedrentar a manifestantes. La inclusión de ese delito en este protocolo solo puede entenderse como una validación del modo en que las policías vienen realizado hasta el momento la práctica de ciberpatrullaje, vinculada a casos de nula relevancia en términos de política criminal o de detección de amenazas, como quedará en evidencia más adelante con el listado de casos que relevamos. La confección de protocolos debe apuntar a mejorar las prácticas policiales y a profesionalizar su trabajo, y no a convalidar o dar cobertura a lo que ya hacen.

Otros problemas de definición se observan en la falta de precisión con la que se refiere a aquellas tareas concretas que comprende el "ciberpatrullaje". De esta manera se deja a discreción de cada fuerza la elección de aquellas maneras que entiende útiles para cumplir con los objetivos de "*identificar delitos; establecer alertas tempranas…; e investigar de formar preliminar posibles hechos delictivos*" (art. 5). En este punto, además de mezclar tareas de vigilancia indiscriminada, de inteligencia criminal y de investigación, tampoco se aclara si estas tareas se realizarán de manera artesanal o si se cuenta con softwares especializados, lo cual abriría todo otro frente de discusión en términos de las herramientas con las que el Estado puede realizar este tipo de vigilancia y la publicidad que debe tener esta información.

También se hace mención a que esta herramienta es necesaria en el marco de la pandemia por el "auge" de la necesidad de "prevención del delito en entornos digitales". En primer lugar, no queda claro el diagnóstico ni por qué este tipo de herramienta puede ser eficaz. Al mismo tiempo, se aprecia una contradicción entre los principios generales invocados, como el de "proporcionalidad", y lo que implica, en términos de intervención policial, habilitar la vigilancia indiscriminada de las redes sociales con el fin genérico de "prevenir delitos".

IV. AFECTACIONES A LA LIBERTAD DE EXPRESIÓN Y EL DERECHO A LA PRIVACIDAD

La vigilancia estatal de las expresiones vertidas en el espacio público y su persecución penal tiene, como es obvio, efectos directos e indirectos en el espacio público, en la libertad de expresión y en la circulación de informaciones y opiniones. La vigilancia de las redes sociales por parte de las fuerzas de seguridad es un tipo de injerencia estatal en el debate público. Los casos judicializados que hemos visto, que además han sido como suele ocurrir con las medidas de "seguridad" profusamente espectacularizados, tienen un efecto indiscutible de amedrentamiento de las expresiones públicas. Esto no puede tener otro efecto que el debilitamiento de una esfera pública amplia y plural.

En la medida en la que toda información que las personas colocan en sus redes sociales es pasible de ser sometida a la vigilancia de las fuerzas de seguridad estamos frente a un nivel de intrusión del Estado en la privacidad que no respeta los estándares internacionales en materia de libertad de expresión y privacidad, dos derechos relacionados de manera estrecha. En particular, respecto del ejercicio pleno de estos derechos en la Internet, en 2019 el Relator Especial para la libertad de

expresión de Naciones Unidas alertaba que “la privacidad y la libertad de expresión están entrelazadas en la era digital, y la privacidad en línea es el punto clave para garantizar el ejercicio de la libertad de opinión y de expresión (Informe de 2019, A/HRC/41/35, pár. 24).

Al mismo tiempo, el argumento que reiteradas veces ha usado el Ministerio de Seguridad sobre que las personas colocan la información en el espacio público ignora las consideraciones del Alto Comisionado de Naciones Unidas para los Derechos Humanos de 2018. En un informe específico sobre el derecho a la privacidad en la era digital reunió los estándares de derechos humanos que se deben tener en cuenta a la hora de reglamentar los derechos en línea. En particular, el Alto Comisionado recordó que “la protección del derecho a la privacidad no se limita a los espacios privados, aislados, como el domicilio de una persona, sino que se extiende a los espacios públicos y a la información de acceso público”. Así les recordaba a los Estados que “el derecho a la vida privada también se ve afectado cuando se reúne y analiza la información sobre una persona que se ha hecho pública en las redes sociales”. Es que, explicó, conforme el derecho internacional de los derechos humanos, “el intercambio público de información no implica que la información sustantiva quede desprotegida” (Informe 2018, A/HRC/39/29, pár.6).

Respecto del derecho a la privacidad garantizado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, el Alto Comisionado para los Derechos Humanos recordó que, conforme al Pacto “las injerencias solo serán admisibles si no son arbitrarias o ilegales y que “los mecanismos de derechos humanos han interpretado sistemáticamente que esas palabras apuntan a los principios generales de legalidad, necesidad y proporcionalidad”. De esta forma, explica, las injerencias de los Estados en el derecho a la privacidad de las personas “sólo puede hacerse en la medida prevista por la ley, y en la legislación pertinente se deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias” (Informe 2018, A/HRC/39/29, pár. 10). Es decir que cualquier injerencia en el derecho a la privacidad de las personas debe cumplir con un criterio de legalidad formal, esto es, debe estar previsto en la ley, debe ser necesario para alcanzar un fin legítimo y debe ser proporcional. Nada de esto se cumple en el proyecto de protocolo sometido a discusión.

V. LA EVIDENCIA EMPÍRICA: PARA QUÉ SE USA EL “CIBERPATRULLAJE”

Los casos que presentamos a continuación ocurrieron en los últimos días, a partir de que las fuerzas policiales comenzaron recibieran algún tipo de orden o mensaje de utilizar las técnicas de “ciberpatrullaje” para identificar supuestas amenazas a la seguridad en el contexto del aislamiento preventivo y obligatorio. Muestran que el “ciberpatrullaje” en la práctica deriva en un uso desproporcionado de la respuesta penal y de los recursos del Estado.

El artículo 6 del proyecto, que establece principios de actuación, se desdibuja completamente a la luz de los casos que surgieron en el último mes. No hay ningún

motivo por el cual se pueda considerar que se cumple con el objetivo buscado ni que las tareas de “ciberpatrullaje” fueron idóneas y necesarias.

Causas penales iniciadas a partir de tareas de “ciberpatrullaje” en las últimas semanas:

>Balcarce, Buenos Aires

El caso de Kevin Guerra implica una tarea de ciberpatrullaje de la Subdirección de Investigación de Delitos Tecnológicos de la Gendarmería Nacional Argentina que se materializó en una denuncia penal por el delito de intimidación pública, basada exclusivamente en el siguiente tweet: “che que onda los que no cobramos el bono de 10mil pesos, sigue en pie lo del saqueo no?”. Se llegó a ese tweet luego de una búsqueda con parámetros de búsqueda “saquear – cuarentena - argentina”. En este caso, se trata de un meme/chiste que surge de Facebook y que Kevin Guerra copió el texto y lo hizo tweet. Guerra hoy enfrenta un proceso penal, luego de haber sido notificado del inicio de las actuaciones.

>Pilar, Buenos Aires

El 8 de abril el juez federal de Morón Néstor Barral ordenó a la Policía Bonaerense realizar un allanamiento en una casa humilde del barrio Agustoni, en el partido de Pilar. El motivo era un supuesto delito de "intimidación pública". Cuando la policía llegó al domicilio señalado, una mujer salió a recibirlos para abrirles la puerta, pero los efectivos le dijeron que se corra y procedieron a romper la entrada. Varias decenas de policías ingresaron a la casa, acompañados por el ministro de seguridad de la provincia, Sergio Berni, por el periodista Rolando Graña y las cámaras de TV del canal América. Secuestraron computadoras y celulares y se llevaron detenida a una sobrina de la mujer, quien habría subido a su cuenta de Facebook un meme con la leyenda "¿Sale este saqueo?". El desproporcionado y violento despliegue, convalidado por la máxima autoridad política en seguridad de la provincia, fue luego emitido en el canal de TV y se puede consultar en Youtube bajo el título "Exclusivo: allanamientos contra agitadores en las redes". La mujer detenida fue liberada al día siguiente.

>Junín, Buenos Aires

El 30 de marzo, luego de tareas de ciberpatrullaje de la policía local, allanaron el domicilio y detuvieron a un habitante de Junín, quién posteó en Facebook "Hay que agarrar y saquear hasta que se vaya Cambiemos de Junín. No ayudan, no dejan laburar. Los ricachones van y vienen y nadie dice nada. Que se pudra todo”. La imputación es por instigación a cometer delitos.

>Colón, Buenos Aires

El 2 de abril, por orden del juez Julio Alfredo Caturla, fue detenido por el delito de “incitación a la violencia colectiva” un joven de la localidad de Colón, luego de tareas de ciberpatrullaje realizadas en su perfil personal. Aparentemente, el joven habría dejado mensajes en Facebook instando a saquear comercios.

>Jujuy

En Jujuy, el 29 de marzo fue detenido un hombre por “instigar” a saqueos en las redes sociales al postear "la estamos haciendo re larga para los saqueos ke onda la gente de Jujuy? Somo' chorro o somo' gile'?". Las tareas de ciberpatrullaje las realizaron la fuerza provincial a partir de una investigación de oficio del Ministerio Público de la Acusación junto con la Agencia Provincial para los Delitos Complejos. Allanaron su domicilio, le secuestraron el celular y quedó detenido acusado por instigación a cometer delitos.

>Santa Fe

Luego de tareas de ciberpatrullaje realizadas por la Gendarmería Nacional, convalidadas por el poder judicial local, el 2 de abril fueron allanados dos domicilios y detenidas dos personas, quienes habrían instigado a saquear. La primera de ellas posteó "Mi sueño es reventar un Coto. Walmart y ahora sumo un Alvear. Cuando haya que saquear que sea a esos hijos de yuta”. Alguien respondió con un comentario “Coto es la deuda del 2001". Ambos fueron imputados por el delito de instigación a cometer delitos.

>Chaco

Un joven fue detenido a principios de abril por un posteo en Facebook, en donde expresó que “si no funca la vacuna, al chino de la 33 pinta saqueo a full”. La policía local realizó tareas de ciberpatrullaje, lo identificó y procedió a detenerlo por varias horas. La imputación sería por instigación a cometer delitos.

>Santiago del Estero

En Santiago del Estero el pastor evangélico Julio Fernando Pablo Luna fue imputado por instigación a cometer delitos. En un grupo de trueque en la red social Facebook realizó un posteo manifestándose en contra de la cuarentena y expresando que no la iba a cumplir. Fue detenido, junto con la administradora del grupo de Facebook. Las tareas de ciberpatrullaje las realizaron la fuerza de seguridad provincial, que culminaron con una autorización judicial para allanar su domicilio, secuestrar teléfonos celulares y notebooks, ocurrido el 20 de marzo. Luego de ello la investigación continuó

hacia la administradora del grupo, a quien luego de ser identificada, el 29 de marzo su domicilio fue allanado y ella detenida.

VI. CONCLUSIONES Y PROPUESTAS

El Ministerio de Seguridad señaló en la presentación del protocolo que el "ciberpatrullaje" tiene como fin el control del aislamiento social preventivo y obligatorio. El proyecto además circunscribe el protocolo a la vigencia del DNU 297/2020. Sin embargo, no está realmente explicado por qué este protocolo es una herramienta específica para intervenir en estos momentos de emergencia. Las fuerzas de seguridad tienen herramientas normativas suficientes para hacer cumplir las medidas sanitarias. Si lo que se necesita es mejorar la prevención e investigación de delitos informáticos, no parece ser esta tampoco la herramienta correcta, tal como lo demuestran los casos relevados. Si de lo que se trata es de mejorar las capacidades de inteligencia criminal para la detección de fenómenos concretos, tampoco es este el protocolo adecuado. Tampoco parece necesario instrumentar regulaciones de emergencia que puedan afectar el derecho a la privacidad y a la libertad de expresión sin un debate público y legislativo.

A partir de estas observaciones, y con el objetivo de aportar a una política de seguridad acorde con valores democráticos y estándares de derechos humanos, recomendamos:

1. Que el Ministerio de Seguridad de la Nación derogue la Resolución 31/2018.
2. Que no se apruebe este proyecto de protocolo y que, con la participación de otros especialistas y actores relevantes, el Ministerio promueva una discusión legislativa.
3. Que, hasta tanto se discuta y clarifiquen los alcances de esta herramienta y sus adecuados controles, las fuerzas federales de seguridad dejen de realizar las actividades de vigilancia indiscriminada en fuentes abiertas que denominan "ciberpatrullaje".
4. Que se convoque al Consejo de Seguridad Interior para evitar que las policías del país continúen realizando este tipo de vigilancia indiscriminada de fuentes abiertas.
5. Que a partir de una normativa general se discutan protocolos para todas las policías provinciales.

A ARGENTINA
ERÍA NACIONAL

"Gral. Martín Miguel de Güemes Héroe de la Nación Argentina"
"2020 – AÑO DEL GENERAL MANUEL BELGRANO"

VRO-5000 140

EÑOR FISCAL

Tengo el agrado de dirigirme a Ud., a los fines de elevar un informe realizado por personal de la Subdirección de Investigación de Delitos Tecnológicos de la Fuerza, en el marco de la Resolución 31/18 del 26 de julio de 2018, de la Secretaría de Seguridad del Ministerio de Seguridad de la Nación, en un cómputo de TRES (3) fojas de que consta, llevando a su conocimiento la detección de un presunto hecho delictivo.

Dicho informe, contiene el resultado de las actividades de ciberpatrullaje correspondientes al día 07 de abril del corriente año realizado por dicha Subdirección, en cumplimiento a la cita Resolución, que instruye a las áreas de investigación de ciberdelitos de las Fuerzas Federales de Seguridad, que una vez detectados presuntos delitos en sitios de internet de acceso público (redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de internet, dark web y demás sitios de relevancia de acceso público); se proceda a efectuar la denuncia del hecho.

Al respecto, llevo a su conocimiento que la Subdirección de Delitos Tecnológicos de nuestra Fuerza, se encuentra en capacidad de llevar adelante la investigación sobre el presunto delito detectado, a los fines de identificar a los presuntos responsables de la publicación.

Solicito, que en caso de promoverse la acción penal para desarrollar una investigación se libre oficio a la **Subdirección de Delitos Tecnológicos** de Gendarmería Nacional, dirección postal Av. Gendarmería Nacional 717, CP 1104, CABA, casilla de correo **dpto-delitosinformaticos@gendarmeria.gob.ar**, a los fines de realizar tareas investigativas, tendientes al esclarecimiento de los extremos denunciados e identificación de presuntos responsables.

Saludo a Ud., atentamente.

Campo de Mayo (Bs As) 09 de abril de 20

GENDARMERÍA NACIONAL
SUBPRODUCTORA

ARIEL SINDULFO SOLAR
COMANDANTE
JUNTA DE COMPLYMOC J.D. CAMPO

INFORME DE CIBERPATRULLAJE
ALERTA TEMPRANA
Dirección de Investigación Criminal

EN EL MARCO DE TAREAS DE CIBERPATRULLAJE EN REDES SOCIALES, SE OBTUVO LA SIGUIENTE INFORMACIÓN DE INTERÉS:

Presunta incitación a saqueos

CASO: "KevinGuerra99":

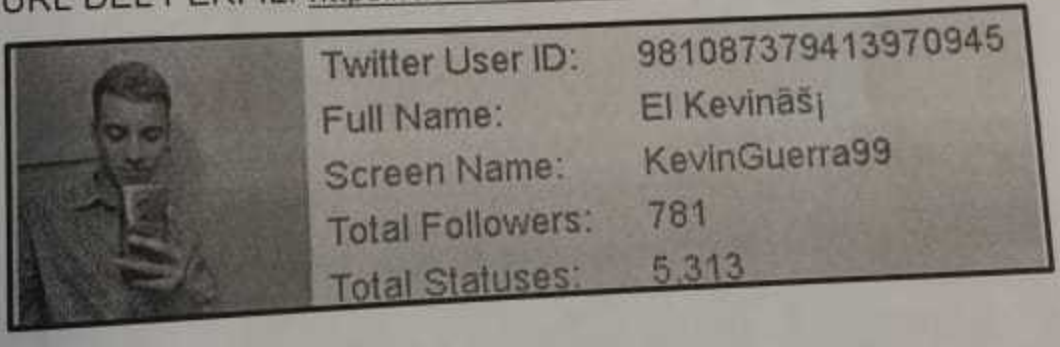
1. De compulsas efectuadas en la red social de Twitter, usando como parámetro de búsqueda "**saquear / cuarentena / argentina**", se obtuvo un perfil público (**@KevinGuerra99**) en el que se observa que posee una publicación donde manifiesta **"che que onda los que no cobramos el bono de 10mil pesos, sigue en pie lo del saqueo no?**", la misma fue realizada el día 7 de abril del corriente año a las 23:16 horas. Conforme se expone a continuación:

   Link: https://twitter.com/KevinGuerra99/status/1247709948554903554

CAPTURA 1: COMENTARIO PÚBLICO DE TWITTER @KevinGuerra99.-

CAPTURA 2: PERFIL PÚBLICO DE TWITTER DE "@KevinGuerra99"

URL DEL PERFIL: https://twitter.com/KevinGuerra99



Se observa que el perfil público de twitter "**@KevinGuerra99** SETESCIENTOS OCHENTA Y UNO (781) seguidores y QUINIENTOS N Y UNO (591) siguiendo, lo que daría cuenta del impacto social o visual su comportamiento en esta red social.

3. Del análisis a la información, se observa, en la captura Nro 2 del perfi twitter de "KevinGuerra99", la información "Balcarce – Argentina" cor ubicación en la provincia de Buenos Aires.

4. Al momento de verificar la cuenta de Instagram expuesta en el perfil, que la cuenta ya no existe.