Anexo

Número: IF-2020-34308714-APN-SSCYTI#MSG

CIUDAD DE BUENOS AIRES
Martes 26 de Mayo de 2020

Referencia: Expediente EX-2020-31145951- -APN-UGA#MSG. PROTOCOLO GENERAL PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS

PROTOCOLO GENERAL PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS

CAPÍTULO I

DE LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS

ARTÍCULO 1º.- OBJETO. ÁMBITO SUBJETIVO DE APLICACIÓN. El presente Protocolo General tiene por finalidad establecer principios, criterios y directrices generales para las tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad dependientes del MINISTERIO DE SEGURIDAD.

ARTÍCULO 2°.- ÁMBITO MATERIAL DE APLICACIÓN. Las tareas de prevención policial del delito en el espacio cibernético se llevarán a cabo únicamente mediante el uso de fuentes digitales abiertas.

Se entiende por “fuentes digitales abiertas” a los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales N° 25.326 y sus normas reglamentarias.

ARTÍCULO 3°.- DELITOS CONCRETOS OBJETO DE LA PREVENCIÓN. La prevención policial del delito en el espacio cibernético procurará el conocimiento de posibles conductas delictivas cuyo acaecimiento sea previsible en función de la emergencia pública en materia sanitaria establecida por Ley N° 27.541, ampliada por el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus COVID-19; atendiendo al desarrollo de la criminalidad vinculada a la comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos; a la venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al COVID-19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente; y a los ataques informáticos a infraestructura crítica —especialmente a hospitales y a centros de salud—; y,

también, al desarrollo de indicios relativos a los delitos a los que hace referencia el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, previstos en los artículos 205, 239 y concordantes del Código Penal.

Asimismo, en tanto se advierta que resulten sensibles al desarrollo de la emergencia pública en materia sanitaria establecida por Ley N° 27.541, ampliada por el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus COVID-19, podrán definirse como objeto de las tareas de prevención policial con uso de fuentes digitales abiertas, posibles conductas delictivas cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos con el fin de realizar acciones tipificadas penalmente como la trata de personas; el tráfico de estupefacientes; el lavado de dinero y terrorismo; conductas que puedan comportar situaciones de acoso y/o violencia por motivos de género, amenaza y/o extorsión de dar publicidad a imágenes no destinadas a la publicación; y delitos relacionados con el *grooming* y la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes.

ARTÍCULO 4°.- PROCEDIMIENTO ESTANDARIZADO Y DEFINICIÓN DE INDICADORES DELICTIVOS. A los fines previstos en el artículo precedente, la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL dispondrá el procedimiento estandarizado y la definición de los indicadores delictivos que orientarán la actividad preventora de los cuerpos policiales y fuerzas de seguridad en el marco de la política criminal del MINISTERIO DE SEGURIDAD durante la emergencia pública en materia sanitaria establecida por Ley N° 27.541, ampliada por el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus COVID-19.

ARTÍCULO 5°.- OBJETIVO. La prevención policial del delito con uso de fuentes digitales abiertas tendrá como objetivo la comunicación del material prevenido en función de los indicadores delictivos derivados de los delitos contemplados en el artículo 3°, al órgano jurisdiccional que se entienda competente, en el caso de así derivarse de la aplicación de los criterios para la judicialización que establezca la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL, en virtud de los estándares regulados en el artículo siguiente.

ARTÍCULO 6°.- CRITERIOS DE JUDICIALIZACIÓN. Los criterios de judicialización deben ceñirse a los estándares que para la prevención policial del delito establece la legislación procesal penal, e incluir explícitas salvaguardas para asegurar que no se criminalicen conductas regulares, usuales o inherentes al uso de Internet. Los hechos definidos como judicializables deben comportar un daño efectivo, o el riesgo actual, real y efectivo de su producción; y sólo se considerarán presuntamente delictivas aquellas conductas a cuyo respecto pueda evaluarse que están dirigidas a incitar o producir una inminente acción delictiva.

CAPÍTULO II

DE LOS PRINCIPIOS DE ACTUACIÓN

ARTÍCULO 7º.- PRINCIPIOS. La prevención policial del delito con uso de fuentes digitales abiertas será llevada a cabo por los cuerpos policiales y fuerzas de seguridad con estricta sujeción a los siguientes principios de actuación:

a. Principio de legalidad. Las actividades deberán ajustarse a las facultades dispuestas por la Ley de Seguridad Interior N° 24.059 y sus modificatorias y por las leyes orgánicas de los cuerpos policiales y seguridad; sus normas reglamentarias y complementarias, especialmente en materia de prevención del delito; por las demás

normas sustanciales y procesales que resulten de aplicación y, en general, por los principios y normas constitucionales y convencionales y por los estándares elaborados por sus respectivos órganos jurisdiccionales de aplicación. Sólo podrán ser objeto de la prevención policial con uso de fuentes digitales abiertas los delitos enumerados en el artículo 3°.

b. Principio de necesidad. Sólo podrán efectuarse tareas de prevención del delito con uso de fuentes digitales abiertas en los casos en que ello sea el medio más adecuado para el objetivo buscado.
c. Principio de proporcionalidad. Las tareas de prevención deberán ser idóneas y necesarias para evitar el peligro que se pretende repeler, ajustándose al logro de ese objetivo.
d. Principio de razonabilidad. La judicialización de las conductas prevenidas requerirá de un análisis en función de las características comunicacionales propias del medio en que se realizan.
e. Principio de protección de la razonable expectativa de privacidad. Las tareas de prevención deberán omitir aquellas conductas susceptibles de ser consideradas regulares, usuales o inherentes al uso de Internet y que no evidencien una intención de delinquir. Asimismo, se descartará toda posibilidad de acumulación de registros relativos a las personas, debiéndose proceder a su efectiva destrucción luego de concluida la actividad preventora.
f. Principio de protección de los datos personales. El personal policial interviniente deberá ajustarse a lo normado en la Ley de Protección de Datos Personales N° 25.326, con particular atención respecto de aquellos datos considerados sensibles, que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual; y de las publicaciones efectuadas por niñas, niños y adolescentes.
g. Principio de protección de la libertad de expresión. Los indicadores establecidos para las tareas de prevención del delito con uso de fuentes digitales abiertas cuidarán de no implicar una afectación a la libertad de expresión garantizada por los principios y normas constitucionales y convencionales y por los estándares elaborados por sus respectivos órganos jurisdiccionales de aplicación. Las tareas de prevención policial se llevarán a cabo con las salvaguardas necesarias para evitar el autocontrol discursivo y la autocensura resultantes de una vigilancia masiva, genérica e indiscriminada, de modo que se preserve el debate plural y el intercambio democrático de las ideas.
h. Principio de no criminalización de las protestas en línea. La protesta a través de redes sociales no formará parte de ningún indicador delictivo establecido para las tareas de prevención policial del delito con uso de fuentes digitales abiertas.
i. Principio de restricción de la discrecionalidad en el cumplimiento de las tareas preventoras. El personal policial debe estar sujeto a un cuadro completo de lineamientos, prioridades, directrices, procedimientos y órdenes de servicio.
j. Principio de profesionalización del personal afectado a las tareas de prevención del delito con uso de fuentes digitales abiertas. El personal al que se asignen dichas tareas será especialmente formado con perspectiva de derechos humanos en entornos digitales, y capacitado en procedimientos, herramientas y medotologías adecuados a los principios establecidos en el presente Protocolo General.
k. Principio de destrucción del material prevenido no judicializado. Los datos colectados de fuentes digitales abiertas y registrados con fines de prevención policial se cancelarán cuando la prevención no hubiera dado lugar a actuaciones judiciales.
l. Principio de publicidad. El MINISTERIO DE SEGURIDAD dará a conocer los alcances y limitaciones de las tareas de prevención policial del delito con uso de fuentes digitales abiertas, que surgen del presente Protocolo General.
m. Principio de transparencia y rendición de cuentas. Se propenderá a la publicación regular de la información relacionada con la cantidad de casos y personas prevenidos junto con la duración de dichas actividades; las redes sociales y sitios web en general que fueron relevados; y las herramientas y las metodologías utilizadas

para cada caso investigado.

n. Principio de control y de responsabilidad por el uso abusivo y violatorio. Se controlará la estricta observancia de los lineamientos, prioridades, directrices, procedimientos y órdenes de servicio impartidas; y se sancionará administrativamente la vigilancia ilegal por parte del personal policial, sin perjuicio de las responsabilidades de orden penal y civil que pudieran asimismo corresponder.

CAPÍTULO III

DE LAS PROHIBICIONES

ARTÍCULO 8º.- CONDUCTAS Y CRITERIOS PROHIBIDOS. En las tareas de prevención policial del delito con uso de fuentes digitales abiertas se encuentra prohibido:

a. Obtener información, producir inteligencia o almacenar datos sobre personas o usuarios por el sólo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.
b. Emplear métodos ilegales o violatorios de la dignidad de las personas para la obtención de información.
c. Comunicar o publicitar información sin autorización.
d. Incorporar datos o información falsos.
e. Considerar como fuente de información a los sistemas de envío de objetos o transmisión de imágenes, voces o paquetes de datos, información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público; o datos que han sido publicados en fuentes abiertas como resultado de una filtración de información privada.
f. Utilizar fuentes digitales abiertas para monitorear y observar detenidamente individuos o asociaciones, como así también para obtener información sobre cualquier acción que implique el ejercicio de los derechos a la protesta social y a la disidencia política.
g. Almacenar los datos personales relevados a través del uso de fuentes digitales abiertas en registros o bases de datos, cuando no dieran lugar a actuaciones judiciales.

ARTÍCULO 9°.- PROHIBICIÓN DE INTERVENCIÓN DE ÁREAS DE INTELIGENCIA CRIMINAL Y DEL PERSONAL DE INTELIGENCIA. Se encuentra prohibida la intervención o participación de cualquier tipo, en la realización de las tareas de prevención policial del delito con uso de fuentes digitales abiertas reguladas por el presente Protocolo General, de las áreas de inteligencia criminal de los cuerpos policiales y fuerzas de seguridad y de la Dirección Nacional de Inteligencia Criminal del MINISTERIO DE SEGURIDAD, y del personal de inteligencia que revistare en las mismas.

CAPÍTULO IV

DE LAS DIRECTRICES GENERALES

ARTÍCULO 10.- LINEAMIENTOS Y PRIORIDADES ESTRATÉGICAS. El MINISTERIO DE SEGURIDAD establecerá los lineamientos y prioridades estratégicas para la prevención policial del delito con uso de fuentes digitales abiertas en el marco de la emergencia pública en materia sanitaria establecida por Ley N° 27.541, ampliada por el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus COVID-19.

ARTÍCULO 11.- DIRECTRICES Y PROCEDIMIENTOS. La SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL ejercerá la dirección, supervisión y control operativo del uso policial de fuentes digitales abiertas; y dispondrá, por ende, el procedimiento estandarizado y la definición de los indicadores delictivos que orientarán la actividad preventora de los cuerpos policiales y fuerzas de seguridad.

ARTÍCULO 12.- ADECUACIÓN A LOS LINEAMIENTOS Y DIRECTRICES DEL MINISTERIO DE SEGURIDAD. Los Jefes de la POLICÍA FEDERAL ARGENTINA, la POLICÍA DE SEGURIDAD AEROPORTUARIA, la GENDARMERÍA NACIONAL y la PREFECTURA NAVAL ARGENTINA, o los responsables que ellos determinen, deberán adecuar su actuación a los lineamientos y prioridades estratégicas que establezca el MINISTERIO DE SEGURIDAD y a las directrices y procedimientos dispuestos por la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL.

ARTÍCULO 13.- DIRECTIVAS U ÓRDENES DE SERVICIO DE LOS RESPONSABLES. Las tareas de prevención policial del delito con uso de fuentes digitales abiertas se desarrollarán en el marco de las directivas u órdenes de servicio emitidas por los responsables a los que alude el artículo precedente, que quedarán debidamente asentadas y registradas en cada dependencia.

ARTÍCULO 14.- RECAUDOS EXIGIBLES. Los responsables de las tareas de prevención policial del delito con uso de fuentes digitales abiertas deberán adoptar las medidas que correspondan para garantizar:

a. El registro y resguardo de las directivas u órdenes de servicio elaboradas para el ejercicio de esta función, así como de los datos individualizados de los agentes intervinientes.
b. El asiento y seguridad de los informes producidos por el área.
c. La trazabilidad y auditoría de las tareas realizadas.
d. El envío de los informes elaborados a las áreas policiales y ministeriales que correspondan, a fin de que se adopten las medidas que se estimen procedentes.
e. La comunicación de las actuaciones de prevención realizadas a las autoridades jurisdiccionales competentes, en función de los criterios de judicialización establecidos.
f. La destrucción de la información obtenida cuando no diere motivo al inicio de una actuación judicial.

ARTÍCULO 15.- PROTECCIÓN INTEGRAL DE LOS DERECHOS DE LAS NIÑAS, NIÑOS Y ADOLESCENTES. Cuando surja certeza, probabilidad o presunción de que la tarea de prevención policial del delito en el espacio cibernético se esté desarrollando ante un menor de edad, se suspenderá la misma dejando constancia de ello en el libro de registro e informando a la autoridad responsable de la tarea. Si existieren manifiestos elementos que objetivamente hagan presumir que se está llevando a cabo alguno de los delitos vinculados con niñas, niños y adolescentes a los que hace referencia el segundo párrafo del artículo 3°, se procederá de acuerdo con los estándares establecidos en la Ley Nacional de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes Nº 26.061, notificando de manera inmediata a los órganos estatales locales con competencia en la aplicación dicha ley, y al órgano jurisdiccional correspondiente.

CAPÍTULO V

DE LA FORMACIÓN Y CAPACITACIÓN PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS

ARTICULO 16.- PLANIFICACIÓN E IMPLEMENTACIÓN DE ACTIVIDADES. Las áreas de formación y capacitación de los cuerpos policiales y fuerzas de seguridad deberán planificar e implementar actividades de formación y capacitación específicas para el personal que desarrolla tareas de prevención del delito con uso de

fuentes digitales abiertas, bajo la coordinación y supervisión de la SUBSECRETARÍA DE FORMACIÓN Y CARRERA de la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL.

ARTÍCULO 17.- PERSPECTIVA DE DERECHOS HUMANOS. Las actividades de formación y capacitación deben contemplar, expresamente, la perspectiva de derechos humanos en entornos digitales; los principios, criterios y directrices generales del presente Protocolo General; los lineamientos y prioridades estratégicas para la prevención policial del delito con uso de fuentes digitales abiertas establecidas por el MINISTERIO DE SEGURIDAD; y las directrices y procedimientos dispuestos por la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL. Atenderán, asimismo, a las recomendaciones que formule la Mesa Consultiva para la evaluación y seguimiento del presente Protocolo General.

CAPÍTULO VI

DE LA APLICACIÓN SUBSIDIARIA A LAS TAREAS DE INVESTIGACIÓN CRIMINAL

ARTÍCULO 18.- APLICACIÓN SUBSIDIARIA A LAS TAREAS DE INVESTIGACIÓN CRIMINAL. Los principios, criterios y directrices generales del presente Protocolo General serán de aplicación subsidiaria, en lo pertinente, a las tareas de investigación criminal que realizan los cuerpos policiales y fuerzas de seguridad como órganos auxiliares de la justicia, en tanto impliquen una doctrina compatible con las instrucciones que impartan los magistrados y permitan su mejor ejecución.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2020.05.26 19:14:47 -03:00

Esteban José Rosa Alves
Subsecretario
Subsecretaría de Control y Transparencia Institucional
Ministerio de Seguridad

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2020.05.26 19:15:49 -03:00