MINISTERIO DE SEGURIDAD

Resolución 144/2020

RESOL-2020-144-APN-MSG

Ciudad de Buenos Aires, 31/05/2020

VISTO el Expediente EX-2020-31145951- -APN-UGA#MSG del registro del MINISTERIO DE SEGURIDAD, el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, la Resolución de la ex SECRETARÍA DE SEGURIDAD N° RESOL-2018-31-APN-SECSEG#MSG del 26 de julio de 2018, la Resolución de la COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS (CIDH) N° 1 del 10 de abril de 2020 sobre Pandemia y Derechos Humanos en las Américas, la Ley N° 27.411 —por la que se aprueba el CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001—, el Estatuto de la Policía Federal aprobado por el Decreto N° 333 del 14 de enero de 1958 y sus modificaciones, la Ley de Seguridad Aeroportuaria N° 26.102, la Ley de Gendarmería Nacional N° 19.349 y sus modificatorias, la Ley General de la Prefectura Naval Argentina N° 18.398 y sus modificatorias, la Ley N° 23.849 —por la que se aprueba la CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO, adoptada por la ASAMBLEA GENERAL DE LAS NACIONES UNIDAS en NUEVA YORK (ESTADOS UNIDOS DE AMÉRICA) el 20 de noviembre de 1989, y que goza de jerarquía constitucional en virtud del artículo 75, inciso 22, de la CONSTITUCIÓN NACIONAL—, la Ley de Protección de Datos Personales N° 25.326 y sus normas reglamentarias, la Ley de Seguridad Interior N° 24.059 y sus modificatorias, la Ley N° 18.711, la Ley Nacional de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes Nº 26.061, y

CONSIDERANDO:

Que mediante el Decreto N° DECNU-2020-260-APN-PTE del 12 de marzo de 2020 y su modificatorio, se amplió la emergencia pública en materia sanitaria establecida por Ley N° 27.541, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus COVID-19, por el plazo de UN (1) año a partir de la entrada en vigencia de dicho decreto.

Que mediante la Resolución de la ex SECRETARÍA DE SEGURIDAD N° RESOL-2018-31-APN-SECSEG#MSG del 26 de julio de 2018, se instruyó a las áreas de investigación de ciberdelitos de las fuerzas policiales y de seguridad que se encuentran bajo la órbita del MINISTERIO DE SEGURIDAD, "…a tomar intervención, específicamente, en todo lo inherente a los siguientes tópicos: Venta o permuta ilegal de armas por Internet. Venta o permuta de artículos cuyo origen, presumiblemente, provenga de la comisión de un acto o de un hecho ilícito. Hechos que presuntamente, se encuentren vinculados a la aplicación de la Ley 23737. Difusión de mensajes e imágenes que estimulen o fomenten la explotación sexual o laboral, tanto de mayores como de menores de edad, y que prima facie parecieran estar vinculados a la trata y tráfico de personas. Hostigamiento sexual a menores de edad a través de aplicaciones o servicios de la web. Venta o permuta de objetos que, presumiblemente, hayan sido obtenidos en infracción a las disposiciones aduaneras. Hechos que presuntamente, transgredan lo normado en los artículos 4, 5,

6, 7, 8 y 9 de la Ley 26388. Los actos investigativos deberán limitarse a sitios de acceso público, haciendo especial hincapié en redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de internet, darkweb y demás sitios de relevancia de acceso público. En ningún momento se permitirán acciones que vulneren o entorpezcan el derecho a la intimidad, Ley 25326 y normativa reglamentaria" (art. 1°).

Que la resolución precitada también dispone que, "…una vez reunidos los medios probatorios necesarios, deberá procederse a efectuar la denuncia del hecho ante el MINISTERIO PÚBLICO FISCAL o PODER JUDICIAL DE LA NACION. Radicada la denuncia, las Fuerzas de Seguridad deberán informar inmediatamente la nomenclatura de la causa a la Dirección de Investigaciones del Ciberdelito, dependiente de la Dirección Nacional de Investigaciones de la Secretaría de Seguridad de la Nación" (art. 2°); y que "las Fuerzas de Seguridad, en ningún momento podrán hacer acopio de la información recabada con motivo de las investigaciones previas realizadas, en virtud de la posible comisión de un ilícito" (art. 3°).

Que se consideró necesario proceder al análisis y estudio, por parte de las diversas áreas del MINISTERIO DE SEGURIDAD competentes en la temática, de la Resolución de la ex SECRETARÍA DE SEGURIDAD N° RESOL2018-31-APN-SECSEG#MSG del 26 de julio de 2018, a fin de evaluar la consistencia de sus disposiciones con los lineamientos y estándares del modelo de seguridad democrática y ciudadana que orientan a esta gestión ministerial.

Que a tal fin resulta pertinente tener en consideración lo dispuesto por la COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS (CIDH) en su Resolución N° 1 del 10 de abril de 2020 sobre Pandemia y Derechos Humanos en las Américas, en la que señaló que "Las Américas y el mundo se enfrentan actualmente a una emergencia sanitaria global sin precedentes ocasionada por la pandemia del virus que causa el COVID-19, ante la cual las medidas adoptadas por los Estados en la atención y contención del virus deben tener como centro el pleno respeto de los derechos humanos". También recomendó a los Estados miembros, entre otras directivas, "Asegurar que, en caso de recurrir a herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia y el seguimiento de personas afectadas, éstas deben ser estrictamente limitadas, tanto en términos de propósito como de tiempo, y proteger rigurosamente los derechos individuales, el principio de no discriminación y las libertades fundamentales. Los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones" (núm. 36, parte resolutiva, resol. cit.).

Que, asimismo, es importante señalar que, mediante la Ley N° 27.411, se aprobó el CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001. Este Convenio persigue como objetivo la prevención de los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando su detección. Además, reconocida tal necesidad, busca garantizar un equilibrio adecuado respeto de los derechos fundamentales del hombre, como los garantizados en el Pacto internacional relativo a los derechos civiles y políticos de las Naciones Unidas (1966), así como en otros convenios internacionales aplicables en materia de derechos del

hombre, que reafirman el derecho de no ser perseguido por la opinión, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada. A tal fin, el artículo 15 del Convenio estipula que “las Partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación […] del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad.” También dispone que cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, “…formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión” y que las Partes examinarán la repercusión de los poderes y procedimientos sobre los derechos, responsabilidades e intereses legítimos de terceros, en la medida que sea consistente con el interés público.

Que, en ese marco, se ha consultado a organizaciones de la sociedad civil vinculadas a la problemática, y a otros organismos e instituciones, con intención de elaborar en forma participativa una nueva normativa ajustada a aquellos lineamientos y estándares, focalizando y tematizando las actividades de prevención del delito en el escenario de las fuentes digitales abiertas del espacio cibernético, 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.

Que, así, se han recibido aportes, críticas y sugerencias de AMNISTÍA INTERNACIONAL ARGENTINA, de la ASAMBLEA PERMANENTE POR LOS DERECHOS HUMANOS (APDH), de la ASOCIACIÓN DE DERECHOS CIVILES (ADC), del CENTRO DE ESTUDIOS LEGALES Y SOCIALES (CELS), de la COMISIÓN PROVINCIAL POR LA MEMORIA (CPM), de la DEFENSORÍA DEL PUEBLO de la CIUDAD AUTÓNOMA DE BUENOS AIRES, de la FUNDACIÓN VÍA LIBRE y del INSTITUTO LATINOAMERICANO DE SEGURIDAD Y DEMOCRACIA (ILSED), de GROOMING ARGENTINA, del OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (ODIA) y de la RED DE CARRERAS DE COMUNICACIÓN SOCIAL Y PERIODISMO DE LA ARGENTINA (REDCOM).

Que, fruto del análisis y estudio de la problemática abordada, puede concluirse que resulta necesaria la aprobación de un “PROTOCOLO GENERAL PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS”, que establezca 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.

Que es preciso indicar que la observación para conocer y prevenir delitos no es monopolio exclusivo de la inteligencia criminal, toda vez que una de las funciones esenciales de los cuerpos policiales y fuerzas de seguridad es la prevención de los delitos, tal como está regulado por sus respectivas leyes orgánicas. En efecto, según el Estatuto de la Policía Federal, son funciones de ella, entre otras, prevenir los delitos de la competencia de los jueces de la Nación y averiguar los delitos de la competencia de los jueces de la Nación, practicar las diligencias

para asegurar su prueba, descubrir a los autores y partícipes, entregándolos a la Justicia, con los deberes y atribuciones que a la policía confiere el Código de Procedimientos en lo Criminal (art. 3°). En virtud de la Ley de Seguridad Aeroportuaria N° 26.102, corresponde a la POLICÍA DE SEGURIDAD AEROPORTUARIA prevenir delitos e infracciones en el ámbito aeroportuario, llevando a cabo las acciones tendientes a impedirlos, evitarlos, obstaculizarlos o limitarlos (arts. 12 y 13). La Ley de Gendarmería Nacional N° 19.349 y sus modificatorias determina que dicha fuerza de seguridad tiene la función de prevenir delitos e infracciones, poseyendo, para ello, funciones de policía de prevención en su respectiva jurisdicción (arts. 2° y 3°). Y, finalmente, de acuerdo con la Ley General de la Prefectura Naval Argentina N° 18.398 y sus modificatorias, dicha fuerza de seguridad se halla facultada para prevenir la comisión de delitos y contravenciones (art. 5°, inc. c], ap. 3°).

Que, aclarado ello, procede señalar que el Protocolo General de cuya aprobación se trata regulará el uso de fuentes digitales abiertas sólo a los fines de esa prevención policial del delito, toda vez que una regulación del uso que de esas fuentes pudiera hacerse para tareas de inteligencia es una cuestión que excede las competencias normativas del MINISTERIO DE SEGURIDAD (v. arts. 7 y 13, Ley N° 25.520; y art. 4°, Anexo I, Dto. N° 950/02).

Que las tareas que realizan los cuerpos policiales y fuerzas de seguridad en cumplimiento de su función preventora del delito no requieren autorización judicial, porque ello es parte de su tarea específica como cuerpos policiales, y sus leyes orgánicas, según se ha visto, les imponen desarrollar y sustanciar la prevención del delito, mediante despliegues adecuados a la naturaleza y modalidad de cada delito o grupo de delitos. Esta labor de prevención del delito, para el caso de obtenerse, como resultado de ella, elementos que permitan sospechar o presumir la comisión de actividades delictivas, concluye con la puesta en conocimiento de la notitia críminis a los magistrados competentes del poder judicial o del ministerio público, según corresponda. Esta es la hipótesis de trabajo contemplada en el artículo 183 del Código Procesal Penal de la Nación, cuando prescribe que “la policía o las fuerzas de seguridad deberán investigar, por iniciativa propia, en virtud de denuncia o por orden de autoridad competente, los delitos de acción pública, impedir que los hechos cometidos sean llevados a consecuencias ulteriores, individualizar a los culpables y reunir las pruebas para dar base a la acusación.” Por lo demás, el artículo 243 del Código Procesal Penal Federal, en forma análoga, determina que “los funcionarios y agentes de la policía u otra fuerza de seguridad que tomaren conocimiento de un delito de acción pública, lo informarán al representante del Ministerio Público Fiscal inmediatamente después de su primera intervención, continuando la investigación bajo control y dirección de éste.” Las tareas de investigación criminal, en cambio, sí presuponen la habilitación o, más precisamente, el requerimiento del órgano jurisdiccional; tratándose de tareas de investigación y análisis del delito que áreas especializadas de las fuerzas policiales y de seguridad sustancian como órgano auxiliar de la justicia. Por otro lado, las tareas de inteligencia criminal son extrañas a la labor policial preventora del delito en entornos abiertos y públicos del ciberespacio; responden a otro sistema institucional —programado por la Ley de Inteligencia Nacional N° 25.520 y sus modificaciones— y a otros objetivos estratégicos y tácticos; están a cargo de organismos específicos y diferenciados —incluso en el seno de las fuerzas, donde las tareas de inteligencia están circunscriptas a las “áreas de inteligencia criminal” de ellas (v. art. 9°, Ley N° 25.520), que no pueden, por ende, realizar tareas preventoras del delito—; y están sujetas a un ciclo de tareas y métodos de producción y análisis informativo del delito, diferenciado y separado orgánicamente de la prevención policial. Pero cabe advertir que tampoco la realización de tareas de inteligencia requiere autorización judicial, a menos que se las confunda, inapropiadamente, con las tareas de investigación criminal que llevan a cabo áreas específicas de los cuerpos policiales cuando operan como órgano auxiliar de la justicia. El sistema legal argentino veda que los cuerpos o áreas de inteligencia

realicen tareas de investigación criminal (v. art. 4°, inc. 1°], Ley N° 25.520).

Que el protocolo objeto de la presente medida es un protocolo de carácter “general”, que prevé su desarrollo y concreción sucesivos a través de lineamientos y prioridades estratégicas del MINSITERIO DE SEGURIDAD, de directrices y procedimientos de la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL, de regulaciones de cada cuerpo policial o fuerza de seguridad relativas a las tareas de prevención policial del delito con uso de fuentes digitales abiertas, y, finalmente, de directivas y órdenes de servicio impartidas por las autoridades responsables de cada cuerpo policial y fuerza de seguridad. Además, y como se indicará más adelante, una Mesa Consultiva que, entre otras funciones, evaluará su funcionamiento, podrá proponer modificaciones o disposiciones complementarias del Protocolo General.

Que las tareas de prevención policial del delito en el espacio cibernético se llevarán a cabo únicamente mediante el uso de fuentes digitales abiertas, entendiéndose por tales 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.

Que 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.

Que aunque no todos los delitos precedentemente enumerados sean de naturaleza federal, no debe perderse de vista que se tomará conocimiento de su posible preparación o acaecimiento a través de fuentes digitales abiertas disponibles en el espacio cibernético, implicando la Internet un supuesto de comunicación interjurisccional en los

términos del artículo 75, inciso 13, de la Constitución Nacional, donde tal supuesto se halla itemizado como materia federal. A todo evento, si resultase que el delito del que se tome conocimiento fuera un delito común, en lugar de darse intervención a la justicia federal, se lo hará a la ordinaria. Además, en el caso de los ciberdelitos, de los delitos contra niñas, niños y adolescentes, y de otros de los delitos mencionados, hay tratados internacionales que obligan al Estado Argentino —en su condición de Estado federal— a velar por su cumplimiento, con medidas legislativas o de cualquier otro carácter. Por otra parte, y a mayor abundamiento, el artículo 19 de la Ley N° 18.711, prescribe que “Efectivos de cualesquiera de los organismos de seguridad podrá actuar en jurisdicción de las otras en persecución de delincuentes, sospechosos de delitos e infractores, o para la realización de diligencias urgentes relacionadas con su función, debiendo darse conocimiento a la autoridad policial correspondiente. Análogas obligaciones y facultades regirán con respecto a las policías de provincia, con sujeción a los convenios existentes en la actualidad o que se acuerden en adelante.”

Que la enunciación en el Protocolo General de los delitos que podrán ser objeto de las tareas de prevención policial con uso de fuentes digitales abiertas es sólo un primer recaudo de legalidad que, de todas maneras, no habilita tareas de prevención policial genéricas y masivas que abarquen la totalidad de aquellos delitos y de los diversos indicadores delictivos que de ellos se pudieran derivar. Al contrario, y como garantía contra el riesgo de una vigilancia discrecional, masiva, generalizada e indiscriminada de fuentes digitales abiertas, se prevé que 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.

Que 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 Protocolo General, 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 a tal fin.

Que tales 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.

Que 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 diversos principios de actuación, a los que se hará mención en los considerandos siguientes.

Que, así, 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 expresamente en el Protocolo General —principio de legalidad—.

Que 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 —principio de necesidad—.

Que las tareas de prevención deberán ser idóneas y necesarias para evitar el peligro que se pretende repeler, ajustándose al logro de ese objetivo —principio de proporcionalidad—.

Que la judicialización de las conductas prevenidas requerirá de un análisis en función de las características comunicacionales propias del medio en que se realizan —principio de razonabilidad—.

Que 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 —principio de protección de la razonable expectativa de privacidad—.

Que 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 —principio de protección de los datos personales—.

Que 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 —principio de protección de la libertad de expresión—.

Que 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 —principio de no criminalización de las protestas en línea—.

Que el personal policial debe estar sujeto a un cuadro completo de lineamientos, prioridades, directrices, procedimientos y órdenes de servicio —principio de restricción de la discrecionalidad en el cumplimiento de las

tareas preventoras—.

Que 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 metodologías adecuados a los principios establecidos en el Protocolo General —principio de profesionalización del personal afectado a las tareas de prevención del delito con uso de fuentes digitales abiertas—.

Que 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 —principio de destrucción del material prevenido no judicializado—.

Que 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 Protocolo General —principio de publicidad—.

Que 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 —principio de transparencia y rendición de cuentas—.

Que 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 —principio de control y de responsabilidad por el uso abusivo y violatorio—.

Que, asimismo, en las tareas de prevención policial del delito con uso de fuentes digitales abiertas se encontrará prohibido: 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; emplear métodos ilegales o violatorios de la dignidad de las personas para la obtención de información; comunicar o publicitar información sin autorización; incorporar datos o información falsos; 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; 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; y 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.

Que también se encontrará 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 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.

Que 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. 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. A su turno, 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. Al final de la secuencia, 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 antes mencionados, que quedarán debidamente asentadas y registradas en cada dependencia.

Que los responsables de las tareas de prevención policial del delito con uso de fuentes digitales abiertas deberán adoptar las medidas que correspondan para garantizar: 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; el asiento y seguridad de los informes producidos por el área; la trazabilidad y auditoría de las tareas realizadas; 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; la comunicación de las actuaciones de prevención realizadas a las autoridades jurisdiccionales competentes, en función de los criterios de judicialización establecidos; y la destrucción de la información obtenida cuando no diere motivo al inicio de una actuación judicial.

Que 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, 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.

Que 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.

Que las actividades de formación y capacitación deben contemplar, expresamente, la perspectiva de derechos humanos e entornos digitales; los principios, criterios y directrices generales del Protocolo General; los lineamientos

y prioridades estratégicas para la prevención policial del delito con uso de fuentes digitales abiertas establecidos 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 aludido Protocolo General.

Que los principios, criterios y directrices generales del 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.

Que, en virtud de los principios de publicidad y de transparencia y rendición de cuentas antes enunciados, se dispondrá el funcionamiento, en el ámbito de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD, de una Mesa Consultiva con la finalidad de efectuar la evaluación de la observancia del Protocolo General y de las reglamentaciones específicas adoptadas por los cuerpos policiales y fuerzas de seguridad para darle cumplimiento; y de elaborar los lineamientos de un mecanismo de auditoría, transparencia y publicidad que el MINISTERIO DE SEGURIDAD aplicará para el control administrativo y la rendición de cuentas de las tareas desarrolladas por aquellos cuerpos y fuerzas. La Mesa Consultiva podrá, asimismo, proponer modificaciones o disposiciones complementarias del Protocolo General. Se reunirá, al menos, cada dos (2) meses.

Que dicha Mesa Consultiva estará integrada por la Titular de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD —quien la presidirá y coordinará—; por el Secretario de Seguridad y Política Criminal, por el Secretario de Articulación Federal de la Seguridad y la Subsecretaria de Programación Federal y Articulación Legislativa, y por otros funcionarios del Ministerio que la Titular de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD determine en función de su competencia. Que, asimismo, se invitará a participar de la Mesa, en condición de miembros de la misma, al Director Nacional de Ciberseguridad dependiente de la JEFATURA DE GABINETE DE MINISTROS, y al Director de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA —ente autárquico en el ámbito de la JEFATURA DE GABINETE DE MINISTROS—; y a representantes de ambas Cámaras de H. CONGRESO DE LA NACIÓN, de los Ministerios Públicos, de los Poderes Judiciales y de las Defensorías del Pueblo —o del organismo que las nuclee—, y de la SECRETARÍA DE DERECHOS HUMANOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS. Además, la Titular de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD podrá solicitar opiniones y dictámenes a otros organismos de Derechos Humanos, a representantes del COMITÉ NACIONAL DE PREVENCIÓN DE LA TORTURA Y OTROS TRATOS O PENAS CRUELES, INHUMANOS O DEGRADANTES u otros representantes del SISTEMA NACIONAL DE PREVENCIÓN DE LA TORTURA, y a otros actores de la sociedad civil; y podrá, asimismo, invitarlos a participar de las reuniones de la Mesa Consultiva.

Que por todo lo precedentemente expuesto procede derogar la Resolución de la ex SECRETARÍA DE SEGURIDAD N° RESOL-2018-31-APN-SECSEG#MSG del 26 de julio de 2018.

Que, asimismo, resultará necesario difundir, en el ámbito del CONSEJO DE SEGURIDAD INTERIOR, el Protocolo General aprobado por la presente resolución; y articular y coordinar en dicho ámbito, con los gobiernos provinciales, la adopción de los principios previstos en el Protocolo General para mejorar los procedimientos y la calidad del

desempeño del servicio policial en lo concerniente a la prevención del delito con uso de fuentes digitales abiertas.

Que el servicio permanente de asesoramiento jurídico de la jurisdicción ha tomado la intervención que le corresponde.

Que la suscripta es competente para el dictado de la presente medida en virtud del artículo 22 bis de la Ley de Ministerios (t.o. 1992) y sus modificaciones.

Por ello,

LA MINISTRA DE SEGURIDAD

RESUELVE:

ARTÍCULO 1°.- Apruébase el “PROTOCOLO GENERAL PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS” que, como Anexo (IF-2020-34308714-APN-SSCYTI#MSG), forma parte integrante de la presente medida.

Dicho Protocolo General tendrá vigencia durante el plazo 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 2°.- Instrúyese a los Jefes de la POLICÍA FEDERAL ARGENTINA, la POLICÍA DE SEGURIDAD AEROPORTUARIA, la GENDARMERÍA NACIONAL y la PREFECTURA NAVAL ARGENTINA a ajustar a los principios, criterios y directrices generales establecidos en el Protocolo General aprobado por la presente resolución, las regulaciones de cada cuerpo policial o fuerza de seguridad relativas a las tareas de prevención policial del delito con uso de fuentes digitales abiertas.

Asimismo, instrúyeselos a designar los responsables a los que hace referencia el artículo 12 del Protocolo General, dentro del plazo de VEINTE (20) días hábiles administrativos posteriores a la entrada en vigencia de la presente resolución; y a comunicar dichas designaciones al Secretario de Seguridad y Política Criminal.

ARTÍCULO 3°.- En el ámbito de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD funcionará una Mesa Consultiva con la finalidad de efectuar la evaluación de la observancia del Protocolo General y de las reglamentaciones específicas adoptadas por los cuerpos policiales y fuerzas de seguridad para darle cumplimiento; y de elaborar los lineamientos de un mecanismo de auditoría, transparencia y publicidad que el MINISTERIO DE SEGURIDAD aplicará para el control administrativo y la rendición de cuentas de las tareas desarrolladas por aquellos cuerpos y fuerzas. La Mesa Consultiva podrá, asimismo, proponer modificaciones o disposiciones complementarias del Protocolo General.

La Mesa se reunirá, al menos, cada DOS (2) meses.

ARTÍCULO 4°.- Dicha Mesa Consultiva estará integrada por la Titular de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD —quien la presidirá y coordinará—; por el Secretario de Seguridad y Política Criminal, por el Secretario de Articulación Federal de la Seguridad y la Subsecretaria de Programación Federal y Articulación Legislativa, y por otros funcionarios del Ministerio que la Titular de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD determine en función de su competencia. Asimismo, se invitará a participar de la Mesa, en condición de miembros de la misma, al Director Nacional de Ciberseguridad dependiente de la JEFATURA DE GABINETE DE MINISTROS, y al Director de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA —ente autárquico en el ámbito de la JEFATURA DE GABINETE DE MINISTROS—; y a representantes de ambas Cámaras de H. CONGRESO DE LA NACIÓN, de los Ministerios Públicos, de los Poderes Judiciales y de las Defensorías del Pueblo —o del organismo que las nuclee—, y de la SECRETARÍA DE DERECHOS HUMANOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

La Titular de la UNIDAD DE GABINETE DE ASESORES del MINISTERIO DE SEGURIDAD podrá solicitar opiniones y dictámenes a otros organismos de Derechos Humanos, a representantes del COMITÉ NACIONAL DE PREVENCIÓN DE LA TORTURA Y OTROS TRATOS O PENAS CRUELES, INHUMANOS O DEGRADANTES u otros representantes del SISTEMA NACIONAL DE PREVENCIÓN DE LA TORTURA, y a otros actores de la sociedad civil; y podrá, asimismo, invitarlos a participar de las reuniones de la Mesa Consultiva.

ARTÍCULO 5°.- Derógase la Resolución de la ex SECRETARÍA DE SEGURIDAD N° RESOL-2018-31-APNSECSEG#MSG del 26 de julio de 2018.

ARTÍCULO 6°.- Instrúyese al Secretario de Articulación Federal de la Seguridad a difundir, en el ámbito del CONSEJO DE SEGURIDAD INTERIOR, el Protocolo General aprobado por la presente resolución; y a articular y coordinar en dicho ámbito, con los gobiernos provinciales, la adopción de los principios previstos en el Protocolo General para mejorar los procedimientos y la calidad del desempeño del servicio policial en lo concerniente a la prevención del delito con uso de fuentes digitales abiertas.

ARTÍCULO 7°.- La presente medida entrará en vigencia a partir de su publicación en el Boletín Oficial de la República Argentina.

ARTÍCULO 8°.- Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese. Sabina Andrea Frederic

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 02/06/2020 N° 21811/20 v. 02/06/2020

Fecha de publicación 02/06/2020

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.

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