MINISTERIO DE SEGURIDAD

Resolución 428/2024

RESOL-2024-428-APN-MSG

Ciudad de Buenos Aires, 27/05/2024

Visto el expediente EX-2024-46438216- -APN-DNCYAC#MSG, la Ley de Ministerios Nº 22.520 (t.o. Decreto N° 438 del 12 de marzo de 1992) y sus modificatorias, la Ley de Seguridad Interior N° 24.059, la Decisión Administrativa N° 340 del 16 de mayo de 2024 y la Resolución del Ministerio de Seguridad Nº 75 del 10 de febrero de 2022, y

CONSIDERANDO:

Que la Ley Nº 22.520 de Ministerios (T.O Decreto N° 438/92) y sus modificatorias asignan al MINISTERIO DE SEGURIDAD la facultad de entender en la determinación de la política criminal y en la elaboración de planes y programas para su aplicación, así como para la prevención del delito, incluyendo la investigación sobre el crimen organizado y los ilícitos complejos.

Que la Ley Nº 24.059 establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior.

Que el artículo 2° de la Ley Nº 24.059 define a la seguridad interior como “la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional”; y el artículo 8° asigna el ejercicio de la conducción política del esfuerzo nacional de policía al MINISTERIO DE SEGURIDAD.

Que los ciberdelitos son una manifestación delictiva en constante expansión que afecta cada día a más personas físicas y jurídicas, economías, sistemas, servicios, infraestructuras críticas y, en consecuencia, es necesario generar mecanismos coordinados y proactivos para la investigación por parte de las fuerzas policiales y de seguridad federales.

Que la UNODOC - Oficina de las Naciones Unidas contra la Droga y el Delito- establece que la ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito.

Que la ciberdelincuencia se distingue de los delitos comunes en que no posee limitantes físicas ni geográficas y puede cometerse de manera ágil y, en general, con menores riesgos para quien delinque.

Que la Agencia de la Unión Europea para la Cooperación Policial (EUROPOL) considera que el ciberdelito es todo delito que solo se puede cometer usando computadoras, redes computarizadas, video juegos y todo tipo de

tecnología que permita un manejo de situaciones a distancia.

Que el uso de esas herramientas incluye la posibilidad de comisión de delitos comunes facilitados por Internet y las tecnologías digitales.

Que la Ley Nº 26.388, de delitos informáticos, ha incorporado al sistema penal argentino las siguientes modalidades delictivas: a) Daño informático; b) Fraude informático; d) Difusión de imágenes de abuso sexual infantil; e) "Violación de Secretos y de la Privacidad"; f) Delitos contra la seguridad pública e interrupción de las comunicaciones; g) Falsificación de documentos electrónicos.

Que la Ley N° 27.411 aprobó el CONVENIO SOBRE CIBERCRIMINALIDAD del CONSEJO DE EUROPA adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, el cual tiene por objeto 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.

Que el citado convenio busca garantizar un 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 la materia que garantizan 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.

Que, a nivel internacional, se observa que la ciberdelincuencia y los delitos tecnológicos cobran mayor relevancia y, en consecuencia, organismos internacionales, regionales y los países adoptan medidas para prevenirlo e investigarlo.

Que INTERPOL ha expresado que en el ciberespacio las amenazas y los ataques pueden provenir de cualquier lugar y producirse en cualquier momento, lo que implica un gran desafío para el poder de policía.

Que, asimismo, en abril de 2021, los Estados Miembros de la ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU) concluyeron en que los Estados deberían reforzar las actividades de investigación y aplicación de las leyes relacionadas con los actos de asociación, complicidad y preparación para cometer delitos cibernéticos, con vistas a confrontar eficazmente a la cadena de la ciberdelincuencia y que, además, deberían mejorar la capacidad de las autoridades judiciales y de las fuerzas del orden para investigar y perseguir los delitos cibernéticos.

Que la Resolución del MINISTERIO DE SEGURIDAD Nº 977/19, aprobó el Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos, el cual fuera actualizado por Resolución MS Nº 75/22.

Que dicho plan establece los lineamientos generales de las políticas públicas relacionadas con las responsabilidades referentes al ciberespacio y su impacto en la seguridad nacional

Que se necesitan adoptar acciones sostenibles y estratégicas que permitan afrontar de la forma más práctica los flagelos relacionadas con los delitos informáticos de manera integral.

Que, en virtud de lo expuesto, se aplicarán las pautas generales cuyo objetivo es dotar de herramientas jurídicas las técnicas investigativas en materia de ciberdelitos o delitos con presencia de la tecnología o utilización de tecnologías.

Que, en otro orden, el artículo 183 del CÓDIGO PROCESAL PENAL DE NACIÓN dispone que “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”.

Que el artículo 235 del nuevo CÓDIGO PROCESAL PENAL FEDERAL establece en su parte pertinente que la investigación de un hecho que revistiera carácter de delito se podrá iniciar a consecuencia de la prevención de alguna de las Fuerzas de Seguridad.

Que, a su vez, el artículo 243 del mismo código establece que los funcionarios y agentes de la policía u otra fuerza de seguridad que tomaren conocimiento de un delito de acción pública deben informarlo al representante del MINISTERIO PÚBLICO FISCAL inmediatamente después de su primera intervención y continuar, en su caso, la investigación, bajo control y dirección de este órgano.

Que, mediante la Resolución de la 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 con la aplicación de la Ley Nº 23.737. 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 con 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 N° 26.388. lavado de activos, o cualquier delito

Que, los actos investigativos deberán limitarse a sitios de acceso público, especialmente en redes sociales de cualquier índole, fuentes, bases de datos públicas y abiertas, páginas de Internet, Dark-Web y espacios de relevancia de acceso público, bajo los parámetros de la ley 25.326.

Que la Resolución de la SECRETARÍA DE SEGURIDAD N° 2018-31-APN-SECSEG#MSG fue derogada y reemplazada por la Resolución del MINISTERIO DE SEGURIDAD N° 144/2020 que aprobó el “PROTOCOLO GENERAL PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS”.

Que por medio de la Resolución MS N° 720/22 se derogó la Resolución MS N° 144/20, que adolecía de serios defectos de hermenéutica, con lo cual la materia quedó sin regulación.

Que resulta necesario brindar a las Fuerzas Policiales y de Seguridad Federales que dependen de este Ministerio herramientas técnico legales adecuadas que simplifiquen sus tareas cotidianas de investigación.

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°.- Las Fuerzas Policiales y de Seguridad Federales deberán adecuar su conducta a las siguientes pautas, principios, criterios, recomendaciones y directivas para las labores preventivas de los delitos que se desarrollan en ambientes cibernéticos. Dichas tareas preventivas se llevarán a cabo únicamente mediante el uso de sitios web de acceso público y fuentes digitales abiertas entendiéndose estas como los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implica una transgresión 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 2°.- Las Fuerzas Policiales y de Seguridad Federales desarrollarán labores preventivas en el espacio cibernético en relación con los siguientes temas:

a. Infracciones y conductas contempladas en la Ley N° 23.737.

b. Amenazas y otras formas de intimidación o coacción.

c. Infracciones a la Ley N° 20.429.

d. Hechos contemplados en la Ley N° 26.388.

e. Venta o permuta de artículos cuyo origen, presumiblemente, provenga de la comisión de un acto o de un hecho ilícito, de violaciones a la Ley N° 22.362 u obtenidos en infracción a las disposiciones aduaneras.

f. Falsificación y comercialización de instrumentos públicos en sitios web y otros espacios virtuales.

g. Infracciones a la Ley N° 14.346.

h. Conductas que puedan comportar situaciones de acoso o violencia por motivos de género.

i. Amenaza o extorsión de dar publicidad a imágenes o datos no destinados a la publicación o sin consentimiento de quienes figuran en tales imágenes.

j. Delitos relacionados con el acoso sexual y la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes.

k. Trata de personas y Tráfico de Personas.

l. Lavado de dinero.

m. Terrorismo.

n. Venta libre de elementos para los cuales se requiera autorización o dispensa legal.

o. Cualquier otro delito del que se pueda obtener noticia a través del ciberespacio.

p. Búsqueda de personas incluidas en el “PROGRAMA NACIONAL DE COORDINACIÓN PARA LA BÚSQUEDA DE PERSONAS ORDENADA POR LA JUSTICIA” o el que en el futuro lo reemplace.

q. Búsqueda de personas desaparecidas y extraviadas en el marco del Sistema Federal de Búsqueda de Personas Desaparecidas y Extraviadas.

ARTÍCULO 3º.- La labor preventiva se deberá adecuar con estricto acatamiento a los siguientes lineamientos:

a. Las actividades preventivas deberán ajustarse a las facultades dispuestas por la Constitución Nacional, Pactos Internacionales de Derechos Humanos, Leyes Nacionales y sus reglamentaciones, Leyes y Decretos orgánicos de las Fuerzas Policiales y de Seguridad Federales y sus normas reglamentarias y complementarias.

b. Utilización de fuentes digitales abiertas.

c. La judicialización de las conductas prevenidas requerirá de un análisis en función de las características comunicacionales propias del medio en que se realizan y del presunto infractor.

d. Se excluirán de la lista para su presunta judicialización aquellas conductas susceptibles de ser consideradas regulares, usuales o inherentes al uso de Internet y que no evidencien la intención de transgredir alguna norma.

e. La utilización de un “agente revelador” deberá contar con autorización judicial y ajustarse a las pautas de la ley 27.319, sus ampliaciones y modificaciones.

f. Las Fuerzas Policiales y de Seguridad Federales no podrán acumular información recabada con motivo de las investigaciones previas realizadas y, una vez concluida la actividad preventiva o decidida la no judicialización, deberá destruirse el material y datos obtenidos.

g. El personal policial interviniente deberá ajustarse a lo normado en la Ley de Protección de Datos Personales N° 25.326. Queda expresamente prohibido el tratamiento sin autorización judicial de datos sensibles -en los términos del artículo 2° de la ley precitada- y de las publicaciones efectuadas por niñas, niños y adolescentes. Cuando surja la certeza 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 y dejará constancia de ello en el libro de registro con aviso a la autoridad responsable de la tarea, excepto cuando en el mismo momento se advirtiere que existe riesgo de vida para el menor.

h. El ciber-patrullaje no podrá interferir con la libertad de expresión constitucionalmente garantizada.

i. El personal de las Fuerzas Policiales y de Seguridad Federales estará capacitado en procedimientos, herramientas y metodologías adecuados a los principios establecidos en el presente.

j. El MINISTERIO DE SEGURIDAD publicará la presente normativa en sus redes sociales. Asimismo, se dará a conocer regularmente toda información relacionada con la cantidad de casos y personas objeto de la prevención.

ARTÍCULO 4º.- 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.

b. Emplear métodos ilegales, prohibidos, invasivos y violatorios de la dignidad de las personas para la obtención de información.

c. Comunicar o publicitar información que viole los principios descriptos en el artículo anterior, como así también incorporar datos o información falsos.

ARTÍCULO 5°.- El uso de softwares o cualquier dispositivo o herramienta tecnológica de tratamiento de la información automatizada basada en inteligencia artificial, aprendizaje automático, sistema experto, redes neuronales, aprendizaje profundo o cualquier otra que en el futuro se desarrolle se ajustará a las estrictas necesidades de la actividad regulada en este protocolo. Su uso deberá ser supervisado por el MINISTERIO DE SEGURIDAD.

ARTÍCULO 6°.- El MINISTERIO DE SEGURIDAD establecerá los lineamientos y prioridades estratégicas para las tareas preventivas. Para ello servirán como indicador, entre otras fuentes, las estadísticas de los reportes enviados a la Dirección de Ciberdelito y Asuntos Cibernéticos, o el área que en el futuro la reemplace, y las denuncias ciudadanas recibidas a la Línea 134 que versaren sobre los delitos mencionados en el presente.

ARTÍCULO 7°.– La presente norma será de aplicación obligatoria para las Fuerzas Policiales y de Seguridad Federales.

ARTÍCULO 8°.- Las labores preventivas se desarrollarán en el marco de las directivas u órdenes de servicio emitidas por los responsables de las respectivas Fuerzas Policiales y de Seguridad Federales, las que deberán adoptar las medidas conducentes a garantizar:

a. El registro y resguardo de las directivas de puesto u órdenes de servicio elaboradas para el ejercicio de esta función.

b. El asiento y seguridad de los informes producidos por el área.

c. La trazabilidad y auditoría de las labores realizadas.

d. La comunicación de las actuaciones de prevención realizadas a las autoridades jurisdiccionales competentes.

e. La destrucción de la información obtenida y recabada cuando esta no fuera judicializada.

f. La adopción de medidas de resguardo de la información obtenida y su protección frente a posibles filtraciones.

ARTÍCULO 9°.- Mensualmente, las Fuerzas Policiales y de Seguridad Federales deberán remitir un informe de gestión a la Dirección de Ciberdelito y Asuntos Cibernéticos, o el área que en el futuro la reemplace, sobre las denuncias que hayan realizado en el transcurso del mes anterior. Dicho informe deberá contener individualizadas las causas que hayan sido iniciadas en virtud del presente protocolo.

ARTÍCULO 10.- Instrúyase a los Titulares de la POLICÍA FEDERAL ARGENTINA, la POLICÍA DE SEGURIDAD AEROPORTUARIA, la GENDARMERÍA NACIONAL, la PREFECTURA NAVAL ARGENTINA y el SERVICIO PENITENCIARIO FEDERAL a adecuar sus procedimientos a las directrices impartidas en la presente normativa.

ARTÍCULO 11.- La Dirección de Ciberdelito y Asuntos Cibernéticos, o el área que en el futuro la reemplace, conformará equipos interdisciplinarios de trabajo, los cuales podrán incluir a otras agencias del Estado, asociaciones civiles sin fines de lucro, personas de relevancia en el campo de las ciencias informáticas o empresas comerciales, a los efectos de actualizar la normativa o complementarla.

ARTÍCULO 12.- La presente medida entrará en vigencia a partir de su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

ARTÍCULO 13.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Patricia Bullrich

e. 28/05/2024 N° 33171/24 v. 28/05/2024

BOLETÍN OFICIAL
de la República Argentina

PRESIDENCIA DE LA NACIÓN
Secretaría Legal y Técnica | Dra. María Ibarzabal Murphy
Dirección Nacional del Registro Oficial | Dr. Walter Rubén Gonzalez