República Argentina - Poder Ejecutivo Nacional
2020 - Año del General Manuel Belgrano

Nota

Número: NO-2020-47326285-APN-AAIP

CIUDAD DE BUENOS AIRES
Jueves 23 de Julio de 2020

Referencia: Respuesta a Nota NO-2020-41096462-APN-UGA-MSG - Mesa Consultiva para la evaluación y seguimiento del Protocolo General para la Prevención Policial del Delito con uso de Fuentes Digitales Abiertas

A: María Cecilia Rodríguez (UGA#MSG),

Con Copia A: Eduardo Hernán Cimato (DNPDP#AAIP), Mauro Meloni (DNPDP#AAIP),

---

De mi mayor consideración:

Me dirijo a Uds. con relación a la nota NO-2020-41096462-APN-UGA-MSG por la que el Ministerio de Seguridad de la Nación (el "MSG") convocó a la Agencia de Acceso a la Información Pública (en adelante, la "AAIP" o "Agencia") -en su carácter de Autoridad de Control de la Ley Nº 25.326 de Protección de los Datos Personales- a participar de la primera reunión de la Mesa Consultiva para la evaluación y seguimiento del Protocolo General para la Prevención Policial del Delito con uso de Fuentes Digitales Abiertas (en adelante, el "Protocolo" y la "Mesa Consultiva", respectivamente), que fuera elaborado y aprobado por el MSG.

A la reunión, que tuvo lugar en las oficinas del Ministerio de Seguridad el pasado 1 de julio de 2020, asistieron actores de distintas áreas del Estado así como organizaciones de la sociedad civil. En esa oportunidad, la AAIP aclaró (i) que agardecía la invitación y resaltaba la importancia de que la autoridad de control de la ley de protección de datos personales hubiera sido convocada, pero manifestó que no recibió consultas ni participó en la redacción del Protocolo o la Resolución MSG Nº 144/2020, (ii) que, sin perjuicio de que el Protocolo prevé que los miembros de la Mesa Consultiva -entre los cuales se incluyó la AAIP- puedan proponer recomendaciones y sugerencias al Protocolo, la obligaciones y facultades conferidas por ley a la AAIP le otorgan competencia para evaluar el cumplimiento de las normas en materia de protección de datos personales, y (iii) que la AAIP remitiría al MSG un documento preliminar para determinar si el Protocolo se adecua a la Ley N° 25.326 y el Convenio para la Proteccion de las Personas con respecto al Tratamiento Automatizado de Datos de Caracter Personal (mayormente conocido como "Convenio 108"), aprobado mediante la Ley N° 27.483. En tal sentido es que la AAIP envía la presente comunicación.

I. <u>Características del Protocolo</u>

El Protocolo tiene por finalidad el 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 MSG, con vigencia durante el plazo de la emergencia pública en materia sanitaria, establecida por Ley N° 27.541 y el Decreto DNU Nº 260/2020.

El ámbito de aplicación de las tareas de prevención, será únicamente a través de "fuentes digitales abiertas", definidas como "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 2 del Protocolo).

Los delitos objeto de la prevención listados en el artículo 3 del Protocolo son los siguientes:

a) 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 DNU N° 260/2020 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.

b) 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.

c) Indicios relativos a los delitos del Decreto DNU N° 260/2020 y su modificatorio, previstos en los artículos 205, 239 y concordantes del Código Penal.

d) En tanto se advierta que resulten sensibles al desarrollo de la emergencia pública en materia sanitaria establecida por Ley N° 27.541 y las normas especiales que la amplían, podrán definirse como objeto de las posibles conductas delictivas cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos, con el fin de realizar acciones tipificadas penalmente como: (i) trata de personas, (ii) tráfico de estupefacientes, (iii) lavado de dinero, (iv) terrorismo, (v) conductas que puedan comportar situaciones de acoso y/o violencia por motivos de género, (vi) amenaza y/o extorsión de dar publicidad a imágenes no destinadas a la publicación; (vii) 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.

Por último, y como fuera mencionado anteriormente, el Protocolo establece una Mesa Consultiva en el ámbito de Jefatura de Gabinete de Asesores del Ministerio de Seguridad que se reunirá, al menos, cada dos meses con la finalidad de "evaluar la observancia del Protocolo General y de las reglamentaciones específicas adoptadas por los cuerpos policiales y fuerzas de seguridad para darle cumplimiento; elaborar 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" (artículo 3, Resolución MSG Nº 144/20).

II. <u>Aplicación de la Ley Nº 25.326 al Protocolo y competencia de la AAIP</u>

Previo a analizar su contenido, es necesario explicar brevemente por qué al Protocolo le es aplicable la normativa vigente en materia de protección de datos personales.

El artículo 2 de la Ley N° 25.326 define al dato personal como aquella "[i]nformacion de cualquier tipo referida a personas fisicas o de existencia ideal determinadas o determinables". Por su parte, el termino tratamiento de datos personales es definido en el artículo 2 de la Ley N° 25.326 como aquellas "[o]peraciones y procedimientos sistematicos, electronicos o no,

que permitan la recoleccion, conservacion, ordenacion, almacenamiento, modificacion, relacionamiento, evaluacion, bloqueo, destruccion, y en general el procesamiento de datos personales, asi como tambien su cesion a terceros a traves de comunicaciones, consultas, interconexiones o transferencias."

Dado que la finalidad del Protocolo es realizar tareas de prevención del delito en el espacio cibernético, y que para determinar si una persona cometió o no un delito las Fuerzas Policiales van a consultar, recolectar, ceder y/o almacenar información referida a la conducta de personas determinadas -es decir, datos personales-, no cabe duda que el Protocolo se encuentra sometido a la regulación de la Ley N° 25.326.

Por último, resulta pertinente aclarar que la AAIP es el órgano competente para controlar que el Protocolo se ajuste a la Ley Nº 25.326. Ello surge de lo establecido en el artículo 44 de la mencionada ley, en cuanto dispone que "[l]a jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional". Dado que el Protocolo parecería constituir un instrumento jurídico por el que el MSG pretender realizar operaciones de tratamiento de datos personales en todo el territorio de la Nación, la AAIP es el órgano competente para pronunciarse sobre su observancia respecto de la Ley Nº 25.326.

III. <u>Análisis, consultas y sugerencias de la AAIP</u>

1. <u>Base legal para realizar tratamiento de datos personales</u>

El MSG, en tanto responsable de tratamiento, debe realizar sus operaciones de procesamiento de datos personales amparándose en alguna de las bases legales previstas en el artículo 5 de la Ley Nº 25.326.

En relación con ello, es pertinente mencionar el artículo 2 del Protocolo, que establece que "[l]as tareas de prevencion policial del delito en el espacio cibernetico se llevaran a cabo unicamente 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".

De acuerdo al artículo del Protocolo anteriormente citado, en el caso objeto de análisis el MSG parecería realizar sus operaciones de tratamiento bajo las bases legales de los apartados (a) y (b) del artículo 5, inciso 2 la Ley Nº 25.326, que establecen, respectivamente, que "[n]o será necesario el consentimiento [del titular de los datos] cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".

Habiendo identificado las bases legales que el MSG utilizaría para procesar datos personales (los apartados (a) y (b) del artículo 5, inciso 2 la Ley Nº 25.326) es necesario aclarar que, si bien la verificación de una base legal es necesaria, ello no significa que el tratamiento realizado sea automáticamente compatible con la Ley Nº 25.326. En este sentido, que un dato personal se encuentre en una fuente digital abierta o una fuente de acceso público irrestricto, no implica de ninguna manera, que quien trate ese dato no deba cumplir con los restantes principios y obligaciones de la Ley Nº 25.326 (principio de calidad del dato, principio de información, los principios de seguridad y confidencialidad, entre otros). La observancia a estos principios y reglas será examinada en las secciones subsiguientes.

1.1. <u>Datos sensibles</u>

Por otro lado, es necesario mencionar que la Ley Nº 25.326 otorga una protección especial a los datos sensibles. Entre otros requisitos, dicha ley restringe las bases legales mediante las cuales se puede realizar tratamiento de datos sensibles. El artículo 7 inc. 2 de la Ley Nº 25.326 establece que "[l]os datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares."

Ello es relevante, ya que, no es claro si el MSG realizará tratamiento de datos sensibles. El Protocolo establece que las tareas de prevencion policial se llevaran a cabo a través del uso de “medios y plataformas de información y comunicación digital de carácter público, **no sensible** y sin clasificación de seguridad” (el énfasis es propio). De este modo, parecería surgir que el tratamiento de datos sensibles se encuentra excluido del ámbito de aplicación del Protocolo.

Sin embargo, no es claro si la mención a “información no sensible” en el artículo 2 del Protocolo se refiere a la definición legal de datos sensibles sentada en el artículo 2 de la Ley Nº 25.326: “datos que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual”.

En el mismo sentido, el artículo 7 inciso f del Protocolo (“Principio de protección de los datos personales”) tampoco establece una prohibición clara respecto del tratamiento de datos sensibles, sino que exige lo siguiente: “El personal policial interviniente deberá ajustarse a lo normado en la Ley de Proteccion de Datos Personales N° 25.326, con particular atencion respecto de aquellos datos considerados sensibles, que revelan origen racial y etnico, opiniones politicas, convicciones religiosas, filosoficas o morales, afiliacion sindical e informacion referente a la salud o a la vida sexual; y de las publicaciones efectuadas por ninas, ninos y adolescentes”

Por último, el Articulo 8 del Protocolo pareciera prohibir el tratamiento de datos sensibles bajo un supuesto particular: “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."

Teniendo en cuenta que no es claro si el Protocolo prohíbe el tratamiento de datos sensibles, la AAIP entiende que el propio Protocolo debe confirmar de manera expresa que no se realizará tratamiento de datos sensibles. En caso contrario, se deberá indicar cuales serían las “razones de interés general autorizadas por ley” que habilitaría ese tratamiento, y demostrar el cumplimiento de los restantes principios de la Ley N° 25.326; cuyo escrutinio es más estricto en caso que se procesen categorías de datos sensibles.

2. <u>Principio de proporcionalidad</u>

El artículo 4, inciso 1 de la Ley N° 25.326 establece que “[l]os datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido”.

Esta norma supone que debe haber una relación proporcional entre las categorías de información que procese el responsable de tratamiento y los fines que este persiga.

Por un lado, ello implica que el responsable no trate más datos de los necesarios para llevar adelante las tareas que se propuso. Es decir, que la información recolectada debe ser la estrictamente indispensable para que realice sus fines y no debe exceder el ámbito de dichos fines. No es suficiente, en este sentido, que la información sirva a los propósitos del responsable. El *test* es más estricto, pues exige que la consecución de tales propósitos requiera la información recolectada como de una causa *sine qua non* sin la cual no pueden cumplirse.

Por otro lado, la norma exige que las operaciones de tratamiento guarden un equilibrio entre la magnitud de la afectación a la privacidad de las personas y la legitimidad de las finalidades pretendidas. En otras palabras, el fin debe revestir la suficiente importancia legal como para justificar una intrusión en la esfera privada de las personas, en particular, a través de la recolección y el tratamiento de sus datos personales. En este último caso, habitualmente es necesario realizar un *test* de ponderación entre el derecho a la privacidad -en cabeza del titular de los datos- y algún otro derecho fundamental -en cabeza del responsable de tratamiento, del titular de los datos o de terceros.

Por último, y en concordancia con el principio anteriormente mencionado, la Ley N° 25.326 establece en su artículo 23 inciso 2 que el tratamiento de datos a realizar por las Fuerzas de Seguridad debe limitarse únicamente a los supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las finalidades establecidas legalmente. Además, dicha norma establece que los archivos de las Fuerzas de Seguridad deberán ser específicos, creados al efecto y debidamente clasificados en función de su grado de fiabilidad.

2.1 Finalidad

El artículo 1 del Protocolo establece como finalidad "la prevención policial del delito en el espacio cibernético cuyo acaecimiento sea previsible en función de la pandemia" y, por ello, la vigencia del documento se encuentra sujeta a la duración de la emergencia sanitaria. Sin embargo, en su objeto se incluyen otras posibles conductas delictivas (p. ej. trata de personas, lavado de dinero y terrorismo) que tengan como medio comisivo principal o accesorio la utilización de sistemas informáticos para cometer el delito. En este orden, la AAIP advierte que el MSG incorpora a la finalidad del Protocolo un listado de delitos que no están estrechamente vinculados con la pandemia.

En este sentido, el primer conjunto de delitos objeto de prevención detallados en el artículo 3 del Protocolo parecería ser notoriamente diferente del otro conjunto de delitos mencionados en el segundo párrafo del mismo artículo. Por un lado, en el primer párrafo, aparecen delitos vinculados, por ejemplo, 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 (sin aprobación ni certificación de la autoridad competente) y a los ataques informáticos a infraestructura crítica (especialmente a hospitales y a centros de salud). Por otro lado, en el segundo párrafo, el Protocolo amplía su objeto de prevención a delitos 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."

Es de notar que, en el primer caso, las penas máximas no se asemejan en gravedad a las penas de los delitos mencionados en el segundo apartado del artículo 3 del Protocolo y, al mismo tiempo, los delitos del segundo párrafo no poseen un vínculo estrecho con la emergencia sanitaria que funda al Protocolo. Esto pareciera indicar que la finalidad del tratamiento podría ser demasiado amplia, y debería restringirse únicamente a aquellos casos en los que una intrusión a la privacidad sea estrictamente necesaria para alcanzar el objetivo propuesto por el MSG.

Por lo anteriormente expuesto, la AAIP estima que, en principio, la finalidad del Protocolo resulta muy amplia y por ello debería estudiarse su restricción.

2.2. Categorías de datos involucradas y detalle sobre la modalidad de tratamiento de los datos

Como se desarrollará a continuación, la redacción actual del Protocolo no cuenta con información suficiente para que la AAIP pueda expedirse apropiadamente sobre el cumplimiento de los artículos. 4 inciso 1 y 23 inciso 1 de la Ley N° 25.326.

El artículo 4 del Protocolo (Procedimiento estandarizado y definición de indicadores delictivos) establece que a los fines de realizar las tareas de prevención "[...] 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 [...]".

Por su parte, el artículo 5 del Protocolo (Objetivo) establece que "[l]a 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.”

Por último, el artículo 6 del Protocolo (Criterios de judicialización) establece que “[l]os 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.”

Como surge de los artículos anteriores, el Protocolo no especifica cómo las tareas de prevención realizadas por el MSG funcionarán en la práctica; ni en particular (i) que categorías de datos se recolectarán, (ii) cómo se asegurará que la información recopilada sea fiable, y (iii) qué consecuencias tendrá el tratamiento de los datos para sus titulares.

Para adecuar el Protocolo a la legislación vigente y evitar potenciales riesgos para la privacidad de las personas, y que se cumpla no el principio de proporcionalidad del tratamiento, la AAIP entiende que debería incuirse de manera expresa y clara: (i) cuál será el procedimiento mencionado en el artículo 4 del Protocolo y cuáles son los “indicadores delictivos” o criterios que utilizará el MSG, atendiendo a los principios de necesidad y proporcionalidad; (ii) informar si se empleará una herramienta de tratamiento automatizado de datos para recopilar información de fuentes digitales abiertas (para mayor detalle sobre esta cuestión, ver apartado 5 sobre tratamiento automatizado); (iii) informar qué mecanismos o criterios se emplearán para asegurar que, al clasificar la conducta de un individuo, dicha clasificación sea fiable (por ejemplo, que la conducta de un individuo no sea clasificada como sospechosa cuando en realidad la persona está haciendo un chiste).

3. Principio de Información

En tercer lugar, cabe referirse al principio de información, sentado en el artículo 6 de la Ley N° 25.326. Este principio es importante en el presente caso, tanto desde el punto de vista del derecho de la protección de los datos personales y la privacidad, como desde el punto de vista del derecho de acceso a la información pública, regido por la Ley N° 27.275.

Las provisiones relevantes de dicho principio son las siguientes: “Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: (a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; (b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; [...] (d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; (e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.”

A continuación se formularán algunas aclaraciones respecto de la aplicabilidad de esas reglas al presente caso:

(i) Tal como ha interpretado la AAIP en numerosas oportunidades, la información detallada en el artículo 6 de la Ley Nº 25.326 debe ser provista al titular de los datos en todos los casos, es decir, independientemente de la base legal que utilice el responsable de tratamiento para justificar sus actividades de procesamiento. Ello así ya que, si los titulares de los datos no tuvieran la oportunidad de conocer que sus datos personales están siendo procesados, no podrían ejercer sus derechos de acceso, rectificación y supresión, tutelados en los artículos 14 y 16 de la Ley N° 25.326, ni de iniciar un reclamo -administrativo (ante la AAIP) o judicial- en caso que el titular del dato entienda que sus derechos no fueron respetados. Por lo tanto, el Protocolo deberá prever de qué manera el MSG informará a la ciudadanía sobre el tratamiento de sus datos, y en particular, a través de qué medios podrán ejercer sus derechos.

(ii) A pesar de que el inciso (d) del artículo 6 de la Ley Nº 25.326 fue redactado para casos en los que el tratamiento se realiza con el consentimiento del titular, la AAIP entiende que en el caso objeto de análisis, dicha norma implica que los responsables de tratamiento deberán informar a la ciudadanía, en tanto titulares de los datos objeto del tratamiento, cuáles son las consecuencias del tratamiento de los datos. Para ello, es fundamental que los responsables de tratamiento (el MSG y las Fuerzas Policiales) den a conocer a la ciudadanía y a la AAIP exactamente cuáles serán las operaciones de

procesamiento de datos personales que llevarán a través de la Resolución MSG N° 144/2020.

En función de lo expuesto anteriormente, y de acuerdo a lo desarrollado en el apartado 2.2, la AAIP advierte que si bien la Resolución MSG N° 144/2020 establece de forma general cuál es su objetivo, quienes llevarán a cabo las tareas de prevención en el ciberespacio, así como una serie de principios aplicables a la materia, no se detalla cómo funcionará en la práctica. Por ello, para cumplir con los estándares exigidos por la Ley N° 25.326 en materia de información, el Protocolo debería brindar un mayor grado de detalle sobre las operaciones de tratamiento que el MSG y los cuerpos policiales llevarán a cabo (ver información solicitada al MSG en al apartado 2.2. de la presente, a la que se remite para mayor brevedad).

A mayor abundamiento, la AAIP entiende que la información solicitada en este apartado también constituye información de interés público en tanto se encuentra referida al marco normativo e institucional que gobiernan a la sociedad, y en tanto es necesaria para que la ciudadanía pueda ejercer un control del accionar de los funcionarios que implementaran las tareas de prevención.

4. Retención y destrucción de los datos

El artículo 4 inc. 7 de la Ley N° 25.326 sostiene que "[l]os datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados." En este sentido, la AAIP entiende que todo aquél que efectúe tratamiento de datos, debe realizar una evaluación de pertinencia y necesidad de forma periódica para determinar la retención, actualización o destrucción de los datos bajo tratamiento.

Al respecto, se advierte que el Protocolo establece que "[l]os datos recolectados 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). Es decir, el MSG afirma que procedería la destrucción de los datos en aquellos casos que no se de lugar a una actuación judicial. Sin embargo, del Protocolo no surge ningún otro tipo de instancia de revisión de los datos respecto de la finalidad para la que fueron recolectados.

En este sentido, la AAIP entiende que el Protocolo debería (i) aclarar cuál sería el plazo para la revisión según el principio de material prevenido no judicializado, (ii) establecer una revisión periódica para analizar la pertinencia y necesidad de los datos según las finalidades para las que fueron recolectados y, por último, (iii) expresar durante cuánto tiempo se almacenaría la información procesada.

5. Salvaguardas en casos de toma de decisiones basadas en tratamiento automatizado

En quinto lugar, cabe hacer mención a las salvaguardas que serían aplicables en caso que se adopten decisiones únicamente basadas en tratamiento automatizado. A continuación se hace mención a dos criterios que la AAIP entiende que podrían ser aplicables al presente caso:

(i) En su Resolución AAIP N° 4/2019 la Agencia ha establecido que "[e]n caso que el responsable de la base de datos tome decisiones basadas únicamente en el tratamiento automatizado de datos que le produzcan al titular de los datos efectos jurídicos perniciosos o lo afecten significativamente de forma negativa, el titular de los datos tendrá derecho a solicitar al responsable de la base de datos una explicación sobre la lógica aplicada en aquella decisión, de conformidad con el artículo 15, inciso 1 de la Nº 25.326."

(ii) En otras oportunidades (ver nota NO-2018-10433281-APN-AAIP) la AAIP ha opinado que: "es fundamental se tenga en cuenta que, conforme estándares internacionales en la materia, los responsables de tratamiento [...] no deben tomar decisiones que afecten gravemente a los titulares de los datos únicamente en razón del tratamiento automatizado de datos. Cualquier resultado positivo obtenido a raíz de un tratamiento automatizado de datos debe reexaminarse individualmente por medios no automatizados antes de adoptar una medida individual que le produzca al titular efectos jurídicos perniciosos o lo afecte significativamente de forma negativa."

Como fuera desarrollado en la sección 2.2 de la presente, el Protocolo no contiene un detalle sobre las operaciones de tratamiento de datos personales, y en particular, si se realizarán a través de sistemas que utilicen inteligencia artificial. Si ese fuese el caso, el Protocolo debería informar como esa herramienta clasificaría la información recopilada, qué categorías de datos procesaría, y si tomaría decisiones de manera automatizada (p. ej. enviando alarmas o mensajes a dependencias del Ministerio Público Fiscal de forma automática), todo ello de modo que se de cumplimiento a los criterios anteriormente mencionados al presente caso.

5.1 Salvaguardas para la protección de datos personales de niños

En relación con la sección anterior cabe mencionar que, respecto de la protección de los derechos de las niñas, niños y adolescentes, el Protocolo establece que **"**[c]uando 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."(artículo 15 del Protocolo)

En este sentido, si el MSG al aplicar el Protocolo utilizare sistemas de tratamiento automatizado para efectuar las actividades de prevención del delito, sería necesaria la implementación de salvaguardas estrictas que impidan la recolección de datos personales de los menores de edad. Por ello, la AAIP considera pertinente que el Protocolo incluya mecanismo/s o salvaguardas para garantizar que los datos de los menores de edad no sean interpretados (por los sistemas automatizados) como si pertenecieren a un adulto.

6. Principio de finalidad y operaciones ulteriores de tratamiento

El principio de finalidad establecido en el artículo 4 inc. 3 de la Ley Nº 25.326 expresa que "[l]os datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención." En los casos donde los responsables de tratamiento son organismos públicos, el principio de finalidad no solo implica que la información no sea procesada de formas distintas a las que hubieran sido declaradas sino también, implica que la finalidad del tratamiento no exceda las competencias otorgada por ley al organismo público.

Tanto el MSG como los otros organismos responsables de tratamiento listados en los artículos 12 y 13 del Protocolo, deberán respetar dicho principio y no realizar operaciones de tratamiento que excedan sus competencias ni las finalidades declaradas en la Resolución MSG Nº 144/2020.

En el mismo sentido, cabe aclarar que toda operación ulterior de tratamiento no incluida en la finalidad original -como, por ejemplo, cesiones de datos personales hacia otros organismos públicos que no estuvieren mencionados en los artículos 12 y 13 del Protocolo- requerirá que se acredite una nueva base legal así como el cumplimiento de los restantes principios aplicables en materia de protección de datos.

Respecto a este punto, esta Agencia sugiere al MSG la revisión de las reglas sentadas en la Ley N° 25.326 sobre las condiciones de licitud relativas a las cesiones de datos personales entre organismos públicos (artículos 5 y 11) así como lo dispuesto por el criterio N° 5 de la Resolución AAIP N° 4/2019: "En relación a la cesión de datos personales entre organismos públicos, no se requiere el consentimiento del titular de los datos y se cumple con las condiciones de licitud, en la medida en que (i) el cedente haya obtenido los datos en ejercicio de sus funciones, (ii) el cesionario utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de su competencia y, por último, (iii) los datos involucrados sean adecuados y no excedan el límite de lo necesario en relación a esta última finalidad."

La AAIP destaca que, si el MSG tuviere previsto realizar cesiones a otros organismos públicos ajenos a los mencionados por el Protocolo, deberá (i) informarlo a la ciudadanía y (ii) informarle a esta Agencia, a los efectos de determinar si dichas cesiones cumplen con el principio de finalidad y los criterios de cesiones ulteriores.

7. Transferencias internacionales

El artículo 12 de la Ley Nº 25.326 y la Disposición DNPDP Nº 60/2016 establece la obligación de brindar salvaguardas de datos personales en caso que los datos fueran objeto de transferencias internacionales hacia el exterior de Argentina. En el mismo sentido, cabe aclarar que el alojamiento de datos personales fuera del territorio argentino constituye una transferencia internacional.

En caso se tenga previsto (i) transferir datos personales procesados en el marco del Protocolo hacia alguna jurisdicción fuera del territorio argentino o (ii) alojar datos en el exterior, el MSG deberá asegurarse que los datos transferidos reciban un nivel de protección igual o mayor que el aplicable según la ley argentina. Podrán hacerlo ya sea (i) realizando la transferencia hacia alguna jurisdicción que posea legislación adecuada conforme a la Disposición DNPDP Nº 60/2016 y la Resolución AAIP Nº 34/2019, o (ii) brindando salvaguardas de datos personales a través de alguno de los mecanismos previstos por el artículo 12 de la Ley Nº 25.326 y/o el Art. 12 del Decreto Nº 1558/2001.

8. Evaluación de impacto

Dado que el Protocolo parecería prever un tratamiento de datos personales a gran escala, la AAIP sugiere que se lleve a cabo una evaluación de impacto en materia de datos personales en la que el MSG (i) detalle exhaustivamente el funcionamiento del Protocolo, incluyendo los puntos consultados en la presente nota, (ii) identifique los riesgos para la privacidad de las personas, y (iii) explique qué salvaguardas se emplearán para mitigar dichos riesgos. En este sentido, cabe mencionar que la AAIP ha aprobado una guía para la elaboración de evaluaciones de impacto en materia de protección de datos personales que encuentra disponible en el sitio web oficial de la Agencia.[1]

Por último, es necesario destacar que, si bien actualmente la elaboración de una evaluación de impacto no es obligatoria bajo la normativa vigente en la materia, la AAIP considera que en casos complejos -como el presente- la presentación de una evaluación de impacto ante la autoridad de control puede contribuir a que el responsable de tratamiento demuestre el cumplimiento de la Ley Nº 25.326.

9. Medidas de seguridad

Conforme a los artículos 9 y 10 de la Ley Nº 25.326, sobre medidas de seguridad y confidencialidad, respectivamente, el MSG deberá adoptar medidas de seguridad para la protección de la confidencialidad e integridad de la información que contiene datos de carácter personal en todo el proceso de tratamiento, desde su recolección hasta su destrucción.

A esos efectos, la AAIP sugiere al MSG tener en cuenta lo dispuesto por la Resolución AAIP Nº 47/2018, en la que se establecen medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados y no informatizados.

IV. Conclusión

La AAIP entiende que, a efectos de cumplir con la regulación vigente en materia de protección del derecho humano a la privacidad, el Protocolo debería ser revisado conforme a las consideraciones vertidas en los apartados anteriores.

Por todo lo expuesto, se sugiere al MSG evalúe la suspensión de la aplicación del Protocolo hasta tanto se revise nuevamente su adecuación a la normativa vigente en materia de protección de datos personales. Esta Agencia queda a su entera disposición para las consultas que pudieran surgir al respecto.

---

[1] https://www.argentina.gob.ar/sites/default/files/guia_final.pdf

Sin otro particular saluda atte.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2020.07.23 10:15:27 -03:00

Eduardo Andrés Bertoni
Director
Agencia de Acceso a la Información Pública

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2020.07.23 10:15:28 -03:00