Ciudad Autónoma de Buenos Aires, 21 de agosto de 2024

A la Ministra de Seguridad de la Nación
Dra. Patricia Bullrich
S_____/_____D

REF.: Solicitud de acceso a la información pública

Nos dirigimos a usted en representación de Amnistía Internacional Argentina, Access Now, el Centro de Estudios Legales y Sociales (CELS), Democracia en Red, la Fundación Vía Libre, el Instituto Latinoamericano de Seguridad y Democracia (ILSED) y el Observatorio de Derecho Informático Argentino (O.D.I.A.) para solicitar acceso a información pública relacionada con la Resolución 710/2024 del Ministerio a su cargo, publicada el 26/07/2024 en el Boletín Oficial, mediante la cual se crea la Unidad de Inteligencia Artificial Aplicada a la Seguridad (UIAAS). De acuerdo a la Resolución indicada, esta Unidad tendrá como misión "la prevención, detección, investigación y persecución del delito y sus conexiones mediante la utilización de la inteligencia artificial".

A continuación acercamos una serie de consultas sobre los supuestos en que puede desarrollarse la actividad, bajo qué pautas, con qué sistemas automatizados y bajo qué controles, entre otras. En este escenario es que nos dirigimos a Ud. para acceder a información al respecto. En detalle, solicitamos:

1. Informe si las actividades comprendidas en los supuestos del art. 4 se desarrollan bajo hipótesis criminales en concreto. En caso afirmativo, informe qué organismo es el encargado de formularlas dentro de cada fuerza y/o del Ministerio a su cargo.

2. Indique bajo qué marcos normativos intervendrá la UIAAS en las tareas de prevención, detección, investigación y persecución de delito y de qué manera se vincula con el Sistema Nacional de Inteligencia.

3. Con respecto al art. 4 inciso “a” que faculta a la Agencia a “Patrullar las redes sociales abiertas, aplicaciones y sitios de Internet, así como la llamada “Internet profunda” o “Dark-Web”, en orden a la investigación de delitos e identificación de sus autores, así como la detección de situaciones de riesgo grave para la seguridad, en el marco de la Constitución Nacional y legislación vigente”, indique:
    a. ¿Qué mecanismos de supervisión externa o auditoría están establecidos para monitorear el uso de la inteligencia artificial por la UIAAS?
    b. ¿El patrullaje en redes sociales abiertas que realizará la agencia, se dará bajo el marco de prevención policial o en el marco de investigaciones criminales concretas?
    c. ¿Qué criterios/indicadores se utilizan para identificar situaciones de “riesgo grave” para la seguridad en estos entornos virtuales?
    d. Explique el alcance del concepto “redes sociales abiertas”.
    e. Explique el alcance del concepto “Dark-Web”.
    f. Explique el alcance del concepto “Internet profunda”
    g. ¿Cuáles son los criterios de preservación de la evidencia digital obtenida en el ciclo de información obtenida de la “Internet profunda”, “Dark-Web” y “redes sociales abiertas” para garantizar su validez en un proceso judicial? Adjunte protocolos.
    h. ¿Qué acciones garantizan que se respeten los derechos constitucionales y la legislación vigente en Argentina?

4. Con respecto al art. 4 inciso “b” que faculta a la Agencia a “Identificar y comparar imágenes en soporte físico o virtual”, indique:
    a. ¿Cuáles son las fuentes de origen de las imágenes que se pretenden identificar y comparar?
    b. ¿Cuáles son los métodos o tecnologías utilizadas para la identificación y comparación de imágenes en soporte físico y virtual?
    c. ¿Cuáles serán los usos de la información obtenida?
    d. ¿Cuáles son los criterios de preservación de la información obtenida? Informe si existen protocolos y, en caso afirmativo, adjúntelos.

5. Con respecto al art. 4 inciso “c” que faculta a la Agencia a “Analizar imágenes de cámaras de seguridad en tiempo real a fin de detectar actividades sospechosas o identificar personas buscadas utilizando reconocimiento fácil”, indique:

a. Si se refiere a imágenes captadas por las cámaras de la Ciudad de Buenos Aires con tecnología de reconocimiento facial destinado a la identificación de prófugos.
b. Si existen convenios entre el Ministerio de Seguridad de la Nación y las distintas jurisdicciones que pueden tener instalada este tipo de tecnología en sus cámaras. En caso afirmativo, acompáñelos.
c. ¿Cuántas cámaras existen con esta tecnología instalada a nivel país y dónde están ubicadas?
d. ¿Qué protocolos de seguridad, privacidad y confidencialidad serán utilizados a efectos de mantener la privacidad de la información recopilada desde su captura hasta su procesamiento?
e. ¿Durante cuánto tiempo son almacenadas las imágenes capturadas por las cámaras y que son procesadas?
f. ¿Quién, cómo y cuándo se determina qué hacer con aquellas imágenes procesadas? ¿Dónde se las almacena?
g. ¿Quién es propietario de aquellos servidores donde se almacenan las imágenes?
h. ¿Cuándo, cómo y de qué manera se las suprime o elimina?
i. ¿Qué técnica de eliminación es utilizada? ¿Cómo se audita y de qué manera se asegura que las imágenes son efectivamente eliminadas?
j. ¿Dónde se realiza físicamente el emparejamiento o la coincidencia de los puntos de los rostros capturados por las cámaras con los puntos de los rostros contenidos en la base de datos utilizada para realizar dicho procesamiento?

6. Con respecto del art. 4 inc. “d” que faculta a la Agencia a “Utilizar algoritmos de aprendizaje automático a fin de analizar datos históricos de crímenes y de ese modo predecir futuros delitos y ayudar a prevenirlos”, informe:
    a. Detalle a qué refiere específicamente el uso de esta herramienta con fines de “prevención, detección, investigación y persecución del delito”.
    b. ¿Qué tipos de datos históricos se utilizan en estos algoritmos de aprendizaje automático?
    c. ¿Cuáles serán las fuentes de origen de estos datos históricos de crímenes?
    d. Bajo qué parámetros se efectuará el análisis allí mencionado.
    e. Si se prevé alguna instancia de revisión humana sobre las tareas realizadas mediante sistemas informáticos automatizados.

f. Qué tipo de auditorías se prevén sobre las herramientas que permitan utilizar algoritmos de aprendizaje automático y sobre su uso por parte de los agentes.
g. Bajo qué parámetros y con qué fuentes de datos se entrenarán.

7. Con respecto del art. 4 inc. “e” que faculta a la Agencia a “Identificar patrones inusuales en las redes informáticas y detectar amenazas cibernéticas antes de que se produzcan ataques. Esto incluye la identificación de malware, phishing y otras formas de ciberataque”, informe:
    a. ¿Qué indicadores se utilizan para detectar patrones inusuales en las redes informáticas?
    b. ¿Qué indicadores se utilizan para detectar un ataque cibernético en preparación?
    c. ¿Qué acciones se despliegan para prevenir los ataques cibernéticos una vez que se detectan?

8. Con respecto del art. 4 inc. “f” que faculta a la Agencia a “Procesar grandes volúmenes de datos de diversas fuentes para extraer información útil y crear perfiles de sospechosos o identificar vínculos entre diferentes casos”, informe:
    a. ¿Qué fuentes se utilizan?
    b. ¿Cómo se accede a estas fuentes?
    c. Los perfiles son confeccionados por personal de la Agencia?

9. Con respecto del art. 4 inc. “g” que faculta a la Agencia a “Patrullar mediante drones áreas extensas, proporcionar vigilancia aérea y responder a emergencias”, informe:
    a. ¿Mediante qué criterios se seleccionan las áreas donde se utilizarán los drones para patrullar?
    b. ¿Quienes controlan los drones durante sus misiones de patrullaje?
    c. ¿Qué información recogen los drones durante las patrullas? ¿Bajo qué criterios y con qué finalidad lo hacen?
    d. ¿De qué manera se utiliza la información recopilada por los drones para mejorar la seguridad?
    e. ¿Qué medidas se llevan a cabo para asegurar que los drones no invadan la privacidad de las personas?

10. Con respecto del art. 4 inc. “i” que faculta a la Agencia a “Mejorar la comunicación y coordinación entre diferentes Fuerzas Policiales y de Seguridad Federales y asegurar

así que la información crítica se comparta de manera rápida y eficiente", informe mediante qué acciones se supervisa y audita el intercambio de información crítica entre las Fuerzas Policiales y de Seguridad Federales.

11. Con respecto del art. 4 inc. "j" que faculta a la Agencia a "Analizar actividades en redes sociales para detectar amenazas potenciales, identificar movimientos de grupos delictivos o prever disturbios", informe:
    a. ¿Qué criterios se utilizan para detectar potenciales amenazas en redes sociales?
    b. ¿Qué tipo de publicaciones o comportamientos en redes sociales son considerados señales de alerta?
    c. ¿Qué medidas se toman para proteger la privacidad de las personas mientras se analizan las redes sociales?

12. Con respecto del art. 4 inc. "j" que faculta a la Agencia a "Detectar transacciones financieras sospechosas o comportamientos anómalos que podrían indicar actividades ilegales", informe:
    a. ¿Qué características definen una transacción financiera sospechosa?
    b. ¿Qué acciones se llevarán a cabo para proteger la información financiera de las personas durante el proceso de detección?
    c. ¿Cuáles son los protocolos que se utilizaran para detectar transacciones financieras sospechosas?
    d. ¿Esta información será cotejada con otras agencias del estado que se abocan a actividades similares?

13. Considerando la Ley de Inteligencia Nacional N° 25.520, indique:
    a. De qué manera prevé cumplir con las previsiones de materias prohibidas para la obtención de información, producción de inteligencia y/o almacenamiento de datos personales (art. 4 inc. 2), en tanto la Resolución 428/2024 de este mismo Ministerio, que sirve como antecedente a esta, sólo contempla algunas de ellas.
    b. ¿De qué manera se realiza la supervisión o auditoría para asegurar que se respeten las materias prohibidas establecidas en la Ley N° 25.520?

14. Considerando Ley Nacional de Protección de Datos Personales N° 25.326, indique:

a. De acuerdo con los arts. 6, 9, 10 y concordantes de mencionada ley, qué medidas de seguridad prevé aplicar este Ministerio sobre el conjunto de datos que las Fuerzas de Seguridad recopilen y quiénes tendrán acceso a la respectiva base de datos, en tanto de las finalidades establecidas en la resolución se desprenden temas que competen a distintas dependencias estatales.
b. Qué medidas o directivas ha implementado el Ministerio a fines de cumplir con lo establecido por el Protocolo Modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal que fuera aprobado por Ley Nacional No 27.699 y entrará pronto en vigencia.
c. Si se ha tenido presente lo establecido por la "Guía de Evaluación de Impacto en la protección de datos" de la Agencia de Acceso a la Información Pública (AAIP). En caso de respuesta afirmativa, acompañe toda resolución o documento de trabajo existente relativo a este punto.
d. Qué estándar de *compliance* es el utilizado por las distintas unidades de compras responsables de la adquisición de las herramientas informáticas, a fin de cumplimentar con la norma citada.
e. Qué formato tienen los “libros de registro”, bajo qué procedimientos se completarán, dónde y cómo se conservarán.
f. Si se ha desarrollado una Evaluación de Riesgos de la medida que incluya un Plan de Tratamiento. En caso afirmativo, acompañe copias.

15. Sobre el debido control de las actividades:
    a. ¿Qué mecanismos de control externo se han establecido para supervisar la implementación de esta Resolución?
    b. ¿Cómo se asegura la transparencia en la aplicación de las directrices de esta Resolución si no se mencionan controles externos específicos?
    c. ¿Qué entidades u organismos son responsables de auditar el cumplimiento de esta Resolución?
    d. ¿Cómo se gestionan las posibles irregularidades o violaciones a las normativas establecidas por la Resolución?
    e. ¿Existen procedimientos para que los ciudadanos puedan presentar quejas o denuncias relacionadas con el cumplimiento de la Resolución?
    f. ¿Qué tipo de informes o revisiones se realizan para evaluar la efectividad y el cumplimiento esta Resolución?

16. Considerando que la Resolución se basa en parte en la experiencia de otros países, incluyendo miembros de la Unión Europea, y teniendo en cuenta el reciente Reglamento de Inteligencia Artificial de esta región (Reglamento 2024/1689 Del Parlamento Europeo y del Consejo - en adelante "Reglamento UE")[1]:
    a. ¿Se han tenido en cuenta las advertencias realizadas por la Unión Europea acerca de la presunción de inocencia y la prohibición de juzgar a las personas a partir de comportamientos predichos por la IA basados en rasgos/características de su personalidad (Reglamento UE, punto 42)? En caso afirmativo, responda de qué manera se contempla en la norma y en la práctica.
    b. ¿Se ha tenido en cuenta la prohibición general que prevé el mencionado reglamento en su artículo 5, que expresamente indica que "los sistemas de perfilamiento de personas con el objetivo de "*realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad*"?
    c. Considerando que los sistemas de IA funcionan de forma probabilística con márgenes de error variables y conllevan fuertes sesgos que suponen casos de discriminación contra poblaciones históricamente vulneradas, ¿se han realizado estudios de impacto para evitar posibles sesgos de discriminación en el uso de la IA? (Reglamento UE, punto 67 y otros) En caso afirmativo, compartirlos.

17. Sobre las herramientas informáticas enunciadas en la resolución, indique y acompañe:
    a. Toda información documental relativa a la adquisiciones de alguna de ellas proveniente de las distintas fuerza de seguridad, incluyendo:
        i) Actas de reuniones y documentos de trabajo.
        ii) Informes técnicos y toda documentación relativa al requerimiento cursado a la correspondiente unidad de compras.
        iii) Los requerimientos cursados a las correspondientes unidades de compras

[1] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689

b. Nombres, apellidos y cargos de los funcionarios abocados a diseñar los requerimientos técnicos específicos para su adquisición y/o implementación.
c. Qué tipo de tareas pueden ser requeridas por la conducción de cada una de las Fuerzas al personal a cargo del uso de los sistemas de investigación informática, en el marco de esta resolución.
d. Si en las evaluaciones previas a la adquisición de los sistemas informáticos se ha previsto la necesidad de herramientas de monitoreo, control y alarma. En caso afirmativo, detalle cuáles.
e. Si está prevista alguna instancia de control humano sobre la actividad de los sistemas informáticos automatizados. En caso afirmativo, detalle en qué consisten.

El presente pedido de acceso a la información pública se realiza en el marco de lo establecido por los arts. 1, 14, 33 y 75 inc. 22 de la Constitución Nacional, 13 de la Convención Americana sobre Derechos Humanos, 19 del Pacto de Derechos Civiles y Políticos, 19 de la Declaración Universal de Derechos Humanos y **la Ley nacional 27.275**. Conforme a lo establecido por la normativa vigente, solicitamos a Ud. tenga a bien responder este pedido de información y brindar la siguiente información **en el plazo de 15 (quince) días hábiles**.

Aprovechamos para saludar a Ud. atentamente,

Amnistía Internacional Argentina
Access Now
Centro de Estudios Legales y Sociales (CELS)
Democracia en Red
Fundación Vía Libre, el Instituto Latinoamericano de Seguridad y Democracia (ILSED)
Observatorio de Derecho Informático Argentino (O.D.I.A.)