El sistema de teleprotección con inteligencia artificial del Gobierno, ¿nos protege realmente?

Valeska Fuentealba Sepúlveda
Docente Derecho Procesal UNAB, Sede Viña del Mar

COLUMNA DE OPINIÓN

Martes 26 septiembre de 2023 | 11:13

Ministerio del Interior y Seguridad Pública

Chile, por el momento, no cuenta con leyes sobre el uso de la inteligencia artificial en la prevención o investigación de delitos, pero sus límites pueden encontrarse en la regulación, entre otros derechos, de la vida privada y de la protección de datos personales.

El Gobierno, el 3 de agosto de este año, informó sobre la implementación de un programa de televigilancia con inteligencia artificial para mejorar la seguridad en 14 comunas de la Región Metropolitana, dando cumplimiento a un propósito mencionado en la Cuenta Pública del Presidente.

La iniciativa pretende conectar las cámaras de distintas entidades para permitir identificar a personas extraviadas o con orden de detención pendiente, así como para detectar vehículos con encargo por robo.

Para lograr el cometido, lo que se hace es utilizar datos biométricos de un sujeto. Estos corresponden a una categoría de dato personal, esto es, información relativa a una persona que permite identificarla, pudiendo ser un rasgo físico, fisiológico o de comportamiento de una persona (por ejemplo, la distancia entre los ojos, su estatura, su forma de caminar, etc.)

Lee también...

Boric anuncia sistema de televigilancia con inteligencia artificial para monitorear la RM

Específicamente, se trata de un dato sensible, que tiene un estatuto protector especial en nuestro derecho a la luz de tratados internacionales y normas chilenas, entre otras razones, por los derechos que puede afectar un tratamiento inadecuado de aquellos datos.

Los tratados internacionales toleran la intromisión de agentes externos (por ejemplo, el Estado en este caso) en la vida privada de un sujeto para la persecución de delitos, siempre que se trate de un supuesto regulado por ley, se persiga un fin legítimo y sea idónea, necesaria y proporcional.

La indeterminación del interés público, en este caso, hace imposible evaluar la necesidad, idoneidad y proporcionalidad de la afectación de los derechos mencionados y, ante tal imposibilidad, no resulta admisible entregar potestades ilimitadas a la autoridad estatal.

El asunto es que, para la investigación de la responsabilidad penal de imputados, se requiere una ley que dote a los órganos competentes de facultades para acceder a registros o datos almacenados para tratarlos con inteligencia artificial para obtener información útil para el proceso penal.

Dicha información debiese someterse a un régimen de legalidad que delimite la competencia estatal a la investigación precisa del ilícito de que se trate y la persecución de sujetos determinados, no pudiendo extenderse a otras conductas ni sujetos.

Los principios de minimización (tratamiento adecuado, relevante y limitado a su propósito o fines), integridad y confidencialidad (adopción de medidas apropiadas para garantizar la seguridad de los datos y sistemas de tratamiento de información) y responsabilidad (responsables deben rendir cuenta del cumplimiento de sus obligaciones) son de peculiar relevancia en este ámbito.

Esto, máxime considerando que, esta iniciativa, se aplicará a todas las personas que circulen por las 14 comunas mencionadas y, por lo mismo, también abarcará a niños, adolescentes y personas no involucradas en ilícitos.

Si se piensa en todos los datos que el sistema capturará y tratará, puede temerse que la autoridad tenga acceso a la rutina y estilo de vida de una persona, sin que necesariamente la persona cuyos datos se capta sepa de esto o conozca quién tendrá acceso a dicha información.

La vigilancia y el tratamiento de datos biométricos de las personas permite predecir y controlar riesgos, pero también la afectación de una serie de derechos como pueden ser los de vida privada, libertad e igualdad.

Esto último, sobre todo considerando que se ha comprobado que las distintas bases de datos contienen sesgos discriminatorios, por ejemplo, la generalidad de las bases de datos cuenta con menos fotografías y datos biométricos de mujeres de piel oscura, lo que hace que, tratándose de este grupo, los sistemas de vigilancia identifiquen falsos positivos con un porcentaje de error del 34,7%, versus un 0,8% en el caso de hombres blancos (Danesi, 2022, p. 215).

En la prensa no ha habido información de los datos con los que se nutrirá la policía para realizar el tratamiento de los datos biométricos que capte por las cámaras de vigilancia.

Esto es relevante, ya que la identificación de las personas se hace a través de estándares probabilísticos empleando los datos que pueden obtenerse de las plantillas de rostros, lo que deriva que este sistema sea esencialmente imperfecto (Garrido y Becker, 2017, p. 81).

El tratamiento de dichos datos puede implicar, entonces, la discriminación de la persona titular de ese dato biométrico y no asegura necesariamente una persecución eficaz, por lo que parece conveniente reflexionar si las eventuales afectaciones a derechos fundamentales resultan justificadas en este caso.

Y, de ser así, al menos debiésemos reflexionar sobre las razones de que esta tecnología no se implemente en todas las comunas de Santiago, sino que, de momento, en las de Santiago, Estación Central, Quinta Normal, Colina o Cerro Navia, entre otras.