"Aplicaciones de la inteligencia artificial en el ámbito de la seguridad ciudadana"

Webinar
Relato de la jornada
2 de diciembre de 2020

Este documento es un resumen de los puntos clave de la segunda sesión del ciclo de encuentros virtuales participativos sobre "Nuevas tecnologías aplicadas a la seguridad urbana". Estos *webinars* han sido organizados por el Foro Español para la Seguridad Urbana (FEPSU) y están dirigidos principalmente a técnicos y responsables municipales y de otras administraciones, y a entidades implicadas en la gestión de la seguridad urbana.

Este segundo debate ha girado en torno a las potencialidades de la aplicación de la inteligencia artificial (IA) en el ámbito de la seguridad urbana, los criterios éticos que deben guiar su uso por parte de las fuerzas y cuerpos de seguridad, y la evaluación de casos prácticos que se pueden dar hoy en día a esta tecnología para mejorar la seguridad de las personas. La sesión ha contado con las intervenciones iniciales de:

- **Felip Manyà,** Subdirector del Instituto de Investigación en inteligencia artificial. CSIC. Universidad Autónoma de Barcelona.
- **Fernando Miró Llinares,** Catedrático de Derecho Penal de la Universidad Miguel Hernández de Elche y Director del Centro CRÍMINA para el estudio y prevención de la delincuencia.
- **Ainoa Torrado,** Criminóloga participante del proyecto Magneto de la iniciativa Horizonte 2020 de la Comisión Europea.

La conversación ha sido moderada por **Francesc Guillén Lasierra,** jurista, criminólogo y estudioso de las políticas públicas de seguridad.

Actualmente, en el ámbito de la seguridad pública, la IA se utiliza para diversos fines; desde la detección de matrículas de vehículos con tasas o denuncias pendientes, el reconocimiento facial, el análisis del lenguaje en las redes, la regulación y planificación del tráfico, hasta la prospección futura de incidentes de seguridad o la robotización de funciones policiales. La velocidad de innovación de estas tecnologías y el entusiasmo acrítico que genera en algunos operadores dificulta un análisis sosegado sobre la conveniencia de su utilización, circunstancia que puede afectar la toma de decisiones acertadas en este campo. Por otro lado, la incorporación de la inteligencia artificial tiende a transformar el proceso de toma de decisiones operativas en una operación puramente mecánica, lo cual plantea retos de diversa índole. Para profundizar en estos temas, se han planteado los siguientes interrogantes durante la sesión:

¿Cómo la IA puede mejorar la seguridad de las personas?

- **Actuaciones concretas.** Desde su desarrollo como disciplina en la década de los años 50, la inteligencia artificial ha buscado utilizar ordenadores para realizar tareas que se relacionan con un comportamiento inteligente: razonar, tomar decisiones, reconocer patrones, resolver problemas matemáticos, etc. Sin embargo, aunque en las últimas dos décadas ha habido un incremento exponencial en la generación de datos y en la potencia de cálculo de los ordenadores, la IA aún no ha conseguido superar un nivel específico de funcionamiento. Esto quiere decir que, a día de hoy, la inteligencia artificial solo permite construir sistemas capaces de realizar una única tarea y, aunque la puedan desarrollar mejor que un ser humano, aún no son capaces de tener conciencia del entorno en que se desarrollan o de tener creatividad en sus acciones, mucho menos de superar la propia inteligencia humana. En este sentido, como ha asegurado Felip Manyà, en el contexto de la seguridad pública este tipo de herramientas permitirá realizar únicamente tareas concretas, combinando técnicas de IA simbólica (basada en el razonamiento lógico) y de IA subsimbólica (como las redes neuronales o el *deep learning*).

- **Proyecto Magneto, un caso de aplicación práctica.** La criminóloga Ainoa Torrado ha presentado un caso concreto de aplicación práctica de la IA en el ámbito de la seguridad, el proyecto Magneto de la iniciativa Horizonte 2020 financiada por la Comisión Europea. El objetivo de este proyecto es el desarrollo de un motor de correlación que permita la elaboración de hipótesis para la toma de decisiones en la prevención e investigación del crimen organizado. Magneto utiliza diversas herramientas de IA, como la transcripción automática de audio-texto, reconocimiento facial, razonamiento semántico avanzado, inteligencia aumentada de visualización 3D de datos georeferenciados, entre otras tecnologías. Para Torrado, el uso de estas herramientas permite a los agentes de las fuerzas y cuerpos de seguridad centrarse más en el análisis de la información que en el tratamiento de los datos y, de esta manera, mejorar la capacidad de investigación y solucionar los delitos de forma más rápida, reduciendo la angustia social y el gasto en investigación. En España, este programa se está implementando de forma experimental en Sabadell (Catalunya).

- **¿Cómo puede contribuir la IA a la realización de programas comunitarios de prevención de la delincuencia?** Una de las posibilidades que brinda la IA es conocer concretamente los lugares donde existen problemas específicos. Esto supone una ventaja para la realización de programas de prevención, ya que si se identifican localmente los problemas se pueden desarrollar también mejores soluciones que no supongan únicamente un incremento de la presencia policial.

¿En qué contextos mejora la intervención pública con estos mecanismos?

- **Áreas de la seguridad con potencial para el uso de la IA**. Para Felip Manyà, existen áreas específicas de actuación de las agencias de seguridad pública donde hoy en día la utilización de herramientas de inteligencia artificial tienen más potencial. Una de ellas es la **videovigilancia**, ya que en la actualidad se recogen muchos datos a través de cámaras de vigilancia que no se procesan. En este sentido, el reconocimiento de imágenes puede servir para detectar paquetes sospechosos, personas en búsqueda y captura, personas desaparecidas, etc. Otro ámbito es la **robótica**, ya que los robots son capaces de moverse en entornos donde hay un mayor riesgo para la seguridad de los agentes de las fuerzas y cuerpos de seguridad, como es el caso de los TEDAX; pero también se puede pensar en el desarrollo de robots asistenciales para víctimas. El **control del tráfico** es otro ámbito de aplicación de la IA que puede ser muy interesante, ya que los sistemas actuales son deficientes comparados con los que podría brindar esta tecnología.

- **Un complemento, no un sustituto.** Una idea clave para entender mejor la intervención pública con herramientas que utilicen IA es comprender que estos sistemas son más bien un complemento a la labor policial que un sustituto. “A corto plazo, os dará más trabajo del que os quitará”, ha asegurado Manyà. Sin embargo, de momento se podría utilizar la inteligencia artificial para facilitar tareas burocráticas en el ámbito de las fuerzas y cuerpos de seguridad, como por ejemplo la gestión de documentación, la toma de declaraciones o la selección de personal. Estos procesos pueden automatizarse a través de técnicas de IA.

¿La inteligencia artificial es siempre neutral o puede equivocarse?

- **Entre la utopía y la distopía.** Fernando Miró Llinares ha explicado que cuando se habla de IA en el ámbito de la delincuencia y seguridad siempre se plantea una dicotomía entre aquellas visiones optimistas, que creen que es una tecnología que va a solucionar todos los problemas, y una visión más pesimista, centrada en la discriminación algorítmica y que ve a la inteligencia artificial como una herramienta para el control y la vigilancia. La realidad se situaría en un punto medio entre estas dos visiones, según el experto. Por este motivo, para establecer criterios éticos que mejoren la aplicación de la IA en el ámbito de la seguridad, primero hay que deshacerse de la visión optimista de que la tecnología es neutral, pero también hay que huir de la visión distópica que considera que su uso únicamente incrementará el control y limitará las posibilidades de la libertad humana.

- **Desmontar mitos.** Para Miró Llinares es importante deshacerse de los mitos sobre la IA para empezar a plantear los debates éticos sobre su uso. Por un lado, hay que desmontar el mito de la predicción del futuro con la inteligencia artificial, ya que lo único que se consigue con estos sistemas es hacer estimaciones. También habría que abandonar el mito de la decisión totalmente autónoma de las máquinas, ya que su acción siempre se da en contextos determinados. Sobre todo, se debe tener en cuenta que la IA no es una especie de "alquimia matemática", sino que la clave son los datos que se introducen, con lo cual, si los datos son malos, también lo será su análisis. Además, se debe resaltar que la distopía del control estatal no es el único peligro del uso de la inteligencia artificial, ya que actualmente las empresas privadas ya tienen acceso a nuestros datos e información y ejercen ese control a través de sus algoritmos. Finalmente, hay que entender que la mente humana también tiene sus sesgos, como lo tienen también los sistemas de IA. En conclusión, hay que buscar el desarrollo de algoritmos que nos ayuden a tomar mejores decisiones.

- **¿Cuáles son los principales riesgos que supone el uso de IA por parte de la policía?** Según Manyà, el principal riesgo ahora mismo es la violación de la privacidad de la ciudadanía, ya que los sistemas actuales tienen una enorme capacidad de control sobre las personas y reducen a gran escala la libertad individual. El otro gran peligro es caer en lo que se denomina "discriminación algorítmica", ya que si se introducen datos con sesgo de cualquier tipo, los resultados que arrojará su análisis también serán sesgados. Finalmente, hay que tomar en cuenta que existe la posibilidad de que estos sistemas puedan ser hackeados.

- **El origen y el tratamiento de los datos, clave.** Si hablamos especificamente de sistemas de predicción policial, por ejemplo, el problema de la discriminación algorítmica se debe principalmente al sesgo de los datos, ya sea porque el modelo de recolección de los mismos no está bien diseñado o no es imparcial, ya sea porque los seres humanos que interpretan los datos antes de introducirlos en el algoritmo lo hacen repitiendo ciertos sesgos y estigmas o simplemente porque la realidad misma de donde se recogen los datos tiene ciertos sesgos que se reproducen en la información que se recoge. Es por este motivo que los algoritmos deben poder ser corregibles, para poder reducir el sesgo de sus datos, aunque esto suponga reducir su capacidad predictiva.

- **¿Cuáles son las consecuencias para las personas del uso de software de reconocimiento facial por parte de la policía?** En diversos casos se ha visto que la aplicación de herramientas de reconocimiento facial en la actuación de las fuerzas y cuerpos de seguridad ha cambiado la forma de patrullar. En cuerpos policiales donde se ha empezado a usar estos sistemas (como la Policía Metropolitana de Londres, que recientemente ha admitido el funcionamiento deficiente de su sistema

de reconocimiento facial)) se ha detectado que los agentes se centraban más en la búsqueda del delincuente, se olvidaban del resto de funciones de la acción policial y se producía una hiperreacción frente a las detecciones de esta herramienta de IA. Además, también aumentaban las detenciones con los mismos sesgos de los datos introducidos en el algoritmo, por ejemplo los sesgos raciales. “Una cosa es para qué sirve la herramienta y otra para qué se usa. Una cosa es el diagnóstico y la otra es el tratamiento”, advierte Miró Llinares.

- **¿Cómo soluciona la IA los obstáculos en el reconocimiento facial cuando la cara está parcialmente tapada, por ejemplo por el uso de una mascarilla?** Torrado explica que es muy complicado la identificación de una persona únicamente por rasgos como los ojos o la nariz, a pesar que actualmente se está trabajando en mejorar el reconocimiento facial de las personas cuando llevan mascarilla, debido al uso generalizado de las mismas ahora mismo en la pandemia del coronavirus. Sin embargo, Torrado subraya que para superar estos obstáculos se puede recurrir a otras herramientas, como la tecnología de reconocimiento de patrones o regiones que utilizan en el proyecto Magneto, la cual permite localizar logos, marcas o colores identificativos de una persona y luego identificar esos mismos rasgos en otras imágenes. Esta herramienta tiene sus limitaciones, ya que permite hacer un seguimiento de la persona que reúne estos rasgos, pero no su identificación.

¿La IA puede ayudarnos a proteger los derechos?

- **¿Puede la IA hacer una policía o una judicatura más justa, en el sentido de tener menos errores, o, por el contrario, son los elementos de valoración inherentes a la condición humana los que garantizan su buen funcionamiento?** Miró Llinares asegura que él es bastante optimista en este sentido, ya que cree que la inteligencia artificial puede ayudar a mejorar determinadas tomas de decisiones si se aplica bien. La IA puede ayudar precisamente a reducir determinados sesgos que se dan en la toma de decisiones de policías y jueces en el día a día, pero es necesario que el ser humano esté ahí para tomar las decisiones sobre la base de principios éticos, valores y humanidad. Manyà, por su parte, destaca que es importante que estas herramientas se vean como un soporte y ha señalado que “un punto para el optimismo” es el hecho que Europa tiene una legislación más avanzada en materia de protección de datos de las que pueden haber en China o Estados Unidos, donde la IA está tecnológicamente más desarrollada. Finalmente, Torrado ha destacado que no sirve de nada que las herramientas de inteligencia artificial brinden resultados si no hay un profesional que los analice en conjunto con los resultados de otras herramientas y partiendo de la base de su propia experiencia profesional.

La decisión de la máquina, ¿ha de gozar de presunción de veracidad? ¿Qué instrumentos hay que establecer para prevenir/controlar errores?

- **Una visión realista, empírica y crítica.** La actitud filosófica ante el uso de la IA en el ámbito policial y la justicia debe ser realista, informada empíricamente (se debe conocer el impacto que va a tener su uso) y crítica, con el objetivo de establecer criterios éticos que permitan una mejor aplicación de estas herramientas en las actuaciones policiales. Para Miró Llinares, este proceso de análisis se debe hacer sobre cada una de las tecnologías a aplicar, no en general.

- **Normas mutables, principios éticos rígidos.** Para regular el uso de la IA en el ámbito de la seguridad se deben construir normas que sean rígidas en la esencia ética de las mismas, pero lo suficientemente flexibles como para permitir dar lugar a las diferentes opciones para su aplicación que surjan con el tiempo. Los principios éticos que se deben tener en cuenta para la elaboración de estas normativas son: el respeto a la autonomía humana y, por lo tanto, la prohibición de subordinación a la máquina; la supervisión constante de los sistemas de IA por parte de una persona; la prevención del daño que pueda ocasionar su uso; la prohibición de la discriminación y la estigmatización como resultado de estos procesos; y la explicabilidad de su funcionamiento, lo que incluye la obligación de trazabilidad de los datos, la auditabilidad de sus procedimientos y la participación democrática de su uso. La Unión Europea, por ejemplo, plantea que la inteligencia artificial tiene que ser lícita, ética y robusta para ser utilizada.

- **¿Qué riesgo concreto hay de la manipulación o envenenamiento de datos que alimentan a sistemas de Machine Learning para producir un daño buscado? ¿Qué tipo penal se debería usar conforme a la regulación existente?** En este sentido, Miró Llinares señala que para este tipo de crímenes se podría utilizar la normativa actual sobre delitos de daños informáticos. Pero, más importante aún, es tener en cuenta los aspectos éticos en la prohibición de los elementos maliciosos desde el desarrollo de los mismos software, no solo a partir de su implementación.

¿En qué términos hay que situar la rendición de cuentas en intervenciones llevadas a cabo siguiendo los dictados de la máquina?

- **La privacidad, el principal reto.** Ahora mismo, el principal reto a resolver en el uso de la IA en el ámbito de la seguridad es el cumplimiento de las normas de privacidad, sobre todo en lo que se refiere a la exigencia de trazabilidad de la información. Un ejemplo de estos problemas es la sentencia del 5 de febrero de 2020 del Tribunal de Distrito de la Haya sobre la utilización del algoritmo SyRI en los Países Bajos para detectar el riesgo de los ciudadanos de cometer fraude contra la

seguridad social. Se declaró ilegal este sistema por violar el derecho a la privacidad, por la desproporcionalidad en los medios, la falta de transfarencia y la indefensión de los interesados.

- **Falta de transparencia en el *deep learning*.** Uno de los problemas de los sistemas de IA basados en redes neuronales es que no tienen capacidad explicativa. Son cajas negras. Esto quiere decir que no dan explicaciones de las decisiones que toman y, por lo tanto, esto puede ser un peligro, ya que si las actuaciones policiales se basan únicamente en sistemas de este tipo, que no dan explicaciones sobre sus decisiones, se puede perder la confianza de los ciudadanos y ciudadanas. Por este motivo, para Manyà, en según qué temas, no se puede delegar la decisión a un ordenador; sino que estos procesos siempre deben ser analizados por humanos. Miró Llinares añade, además, que en todo caso siempre se debe exigir la trazabilidad de los datos y debe hacerse una reflexión profunda sobre el uso que se dará a esta información, sin que la predicción signifique una actuación policial inmediata.

Recursos compartidos

- ¿Hacia una nueva Ilustración? Una década trascendente. El futuro de la IA: hacia inteligencias artificiales realmente inteligentes, Ramón López de Mántaras.
- Estrategia española de I+D+I en Inteligencia Artificial. Ministerio de Ciencia, Innovación y Universidades, 2019