El impacto de la inteligencia artificial en el mundo de la seguridad

Por Oriol Verdura, vocal de ADSI

En la última década, la inteligencia artificial (IA) ha transformado numerosos sectores de la sociedad, y el ámbito de la seguridad no ha sido la excepción. La IA ha logrado integrarse profundamente en sistemas de videovigilancia, alarmas, control de accesos y protección de activos, cambiando la forma en que las organizaciones y los individuos se protegen ante amenazas potenciales. Estos avances no solo han mejorado la eficiencia y eficacia de los sistemas de seguridad actuales, sino que también han permitido una capacidad de respuesta más rápida y precisa, elevando los estándares de protección.

Uno de los usos más significativos de la IA en seguridad es en los sistemas de videovigilancia. Tradicionalmente, estos sistemas dependían de la intervención humana para monitorear cámaras en tiempo real y detectar actividades sospechosas. Sin embargo, la IA ha automatizado este proceso. Gracias al aprendizaje automático y a la visión por computadora, los sistemas de videovigilancia pueden analizar de manera autónoma grandes cantidades de datos visuales, identificar comportamientos anómalos o potencialmente peligrosos y emitir alertas en tiempo real. Por ejemplo, en espacios públicos o empresas, la IA puede detectar situaciones como la presencia de objetos abandonados, movimientos inusuales o incluso podría identificar rostros de personas con antecedentes delictivos, mejorando notablemente la capacidad de prevenir incidentes antes de que estos ocurran.

En el ámbito de las alarmas y el control de accesos, la IA también ha dejado una huella considerable. Las alarmas modernas ya no son simplemente dispositivos que reaccionan ante una perturbación, como la apertura de una puerta o una ventana. Hoy en día, muchos sistemas de alarmas utilizan IA para analizar patrones de comportamiento y reducir la cantidad de falsas alarmas. Por ejemplo, un sistema de alarma inteligente puede aprender los hábitos de las personas en una vivienda o una oficina, permitiendo que distinga entre actividades normales y sospechosas, mejorando la precisión de la respuesta.

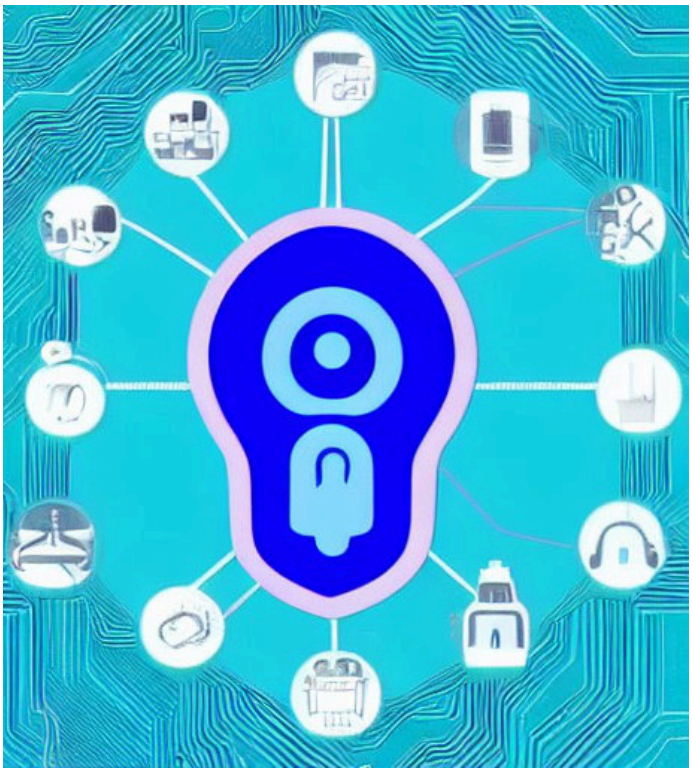
En cuanto al control de accesos, la IA ha facilitado la implementación de tecnologías avanzadas como el reconocimiento facial y la autenticación biométrica. Ya no se trata solo de tener una tarjeta o código de acceso, sino que las cámaras y los sensores pueden identificar automáticamente a las personas autorizadas para entrar en áreas restringidas, haciendo el proceso más seguro y sin fricciones. La autenticación multifactor basada en IA, como el reconocimiento del iris, huellas dactilares o incluso la forma de caminar, ofrece un nivel de seguridad que reduce significativamente el riesgo de accesos no autorizados.

Además de la vigilancia y el control de accesos, la IA ha demostrado ser una herramienta eficaz para proteger activos en sectores como la banca, las telecomunicaciones y la industria. Con la capacidad de analizar patrones en grandes volúmenes de datos, la IA puede identificar comportamientos anómalos en transacciones financieras, protegiendo contra fraudes y ciberataques. Empresas tecnológicas y financieras ya

están utilizando sistemas de IA para detectar amenazas en tiempo real, minimizando las pérdidas y aumentando la seguridad de los activos digitales.

Sin embargo, a pesar de los avances que ya hemos presenciado, la implementación de la IA en seguridad no está exenta de desafíos. Uno de los mayores retos es la preocupación por la privacidad. El uso extendido de cámaras y sistemas de reconocimiento facial ha suscitado debates sobre los límites éticos de la vigilancia. ¿Hasta qué punto es legítimo monitorizar a los individuos en aras de la seguridad? Esta es una cuestión clave que las empresas y los gobiernos deberán abordar mientras la IA sigue evolucionando.

Otro desafío importante es la dependencia excesiva en estos sistemas. Aunque la IA es eficiente, no es infalible. Los sistemas de seguridad basados en IA pueden ser vulnerables a errores o manipulaciones, como el uso de técnicas de falsificación de imágenes (deepfakes) para engañar a los sistemas de reconocimiento facial. La seguridad debe seguir evolucionando, no solo para hacer frente a las amenazas actuales, sino también para garantizar que la IA no se convierta en una herramienta que pueda ser usada en contra de quienes intenta proteger. La tentación puede ser muy grande y la línea que separa protección de invasión es cada vez más delgada.



Mirando hacia el futuro

El potencial de la IA en el mundo de la seguridad es inmenso. Como hemos visto, a día de hoy ya tenemos muchas aplicaciones en marcha, pero no podemos olvidar que la IA que tenemos hoy es lo que se conoce como "Narrow AI", es decir, que una IA sólo sirve para un campo en concreto cada vez. La gran diferencia con la Inteligencia Humana es que ésta es capaz de aprender y gestionar múltiples campos a la vez. Cuando esto suceda con la Inteligencia Artificial, habremos alcanzado lo que se conoce como IAG (Inteligencia Artificial General). Será en ese momento en el que podremos equipararla con nuestros cerebros. Con eso y con los avances en el procesamiento de datos en tiempo real, los sistemas de seguridad podrán responder aún más rápido y con mayor precisión a incidentes. En un futuro cercano, podríamos ver una mayor integración de la IA con el Internet de las Cosas (IoT), permitiendo que sistemas de seguridad interconectados actúen de manera autónoma, adaptándose a las amenazas emergentes. Además, es probable que la IA continúe mejorando las capacidades de predicción, anticipando crímenes o incidentes antes de que ocurran, lo que abriría un nuevo paradigma en la protección de personas y activos.

En resumen, la IA ya está revolucionando la seguridad, y aunque enfrenta retos importantes, su futuro promete un mundo más seguro, eficiente y conectado, siempre que lo sepamos gestionar ...¿Será la humanidad capaz de hacerlo?. ■