



Sistemas de videovigilancia inteligentes: privacidad de los datos y seguridad ciudadana

por Luis Ernesto Alemán-Madrigal y Lenin Sebastián Barreto-Pastora

La videovigilancia con inteligencia artificial se ha convertido en una herramienta empleada para fortalecer la seguridad privada y pública; no obstante, su implementación plantea desafíos en cuanto la privacidad, protección de datos y aceptación social¹. En Nicaragua, su uso se encuentra en una etapa inicial, coexistiendo con un marco normativo poco desarrollado, situación que plantea interrogantes en cuanto a sus implicaciones técnicas y éticas de implementación.

En este contexto y como proyecto de culminación extracurricular para la Universidad Americana (UAM) se desarrolló un protocolo de investigación titulado “Integración de medidas de videovigilancia con IA de reconocimiento inteligente en Nicaragua” en el que se propone la implementación de un Sistema de Vigilancia Inteligente (SVI) para el reconocimiento de placas vehiculares y la identificación de peatones como medidas destinadas a fortalecer la seguridad del recinto. Su propósito inicial parecía, por tanto, claramente definido: aprovechar las posibilidades que ofrece la inteligencia artificial para contribuir a la creación de un entorno más seguro para la comunidad universitaria.

Sin embargo, el desarrollo de la investigación permitió advertir que la viabilidad de una solución tecnológica de esta naturaleza no depende exclusivamente de su capacidad para responder a una necesidad de seguridad. Mediante la aplicación de entrevistas estructuradas a autoridades y estudiantes de la Universidad se identificaron, junto con las expectativas generadas por la utilización de estos sistemas, interrogantes vinculadas con la confianza institucional y el riesgo de afectación a la privacidad. De este modo, una investigación concebida desde una perspectiva tecnológica condujo a una cuestión previa y de mayor alcance ¿hasta dónde puede utilizarse la inteligencia artificial para incrementar la seguridad sin afectar desproporcionadamente la privacidad y la protección de los datos personales de los miembros de la comunidad?

La interrogante resulta particularmente relevante cuando se pretende trasladar la propuesta fuera del ámbito universitario. Un sistema inicialmente diseñado como experiencia académica podría encontrar aplicaciones en empresas privadas, instituciones públicas e incluso en organismos encargados de garantizar la seguridad ciudadana. El reconocimiento automatizado de placas vehiculares, la identificación de personas o el análisis inteligente de imágenes pueden incrementar las capacidades de prevención y control; sin embargo, también permiten recopilar, relacionar y conservar cantidades significativas de información sobre las personas. El mismo desarrollo

¹ Vid. VIZCAÍNO ZAMORA, Á. “Videovigilancia e inteligencia artificial: entre la utopía y la distopía”, *Revista Mexicana de Ciencias Penales*, vol. 4, núm. 14, 2021.

tecnológico que incrementa la capacidad de vigilancia amplía, por consiguiente, los riesgos derivados de un tratamiento inadecuado de los datos obtenidos.

Es precisamente en este punto donde la idea original encuentra sus principales límites. La posibilidad técnica de desarrollar un sistema no determina, por sí sola, la legitimidad de su utilización. Entre ambas cuestiones aparece el Derecho, al que corresponde establecer quién puede recopilar información, con qué finalidad, durante cuánto tiempo puede conservarla, quién puede acceder a ella y qué garantías deben reconocerse a las personas sometidas a vigilancia. El problema deja entonces de consistir únicamente en determinar si Nicaragua dispone de la tecnología necesaria para implementar un SVI y pasa a preguntarse bajo qué condiciones jurídicas podría hacerlo.

Habría que señalar de que no se parte de una ausencia absoluta de regulación pues la Ley 787/2012², reconoce garantías frente al tratamiento de información personal y tutela la autodeterminación informativa, mientras que la Ley 1042/2020³, incorpora mecanismos de protección frente a determinadas conductas ilícitas ejecutadas mediante tecnologías de la información y comunicación; sin embargo, estas normas no fueron concebidas específicamente para responder a las particularidades que plantea la utilización de SVI. La capacidad de estos instrumentos para recopilar información de manera permanente, automatizar su análisis y extraer patrones a partir de los datos obliga a reconsiderar la suficiencia de las garantías tradicionales.

Esta circunstancia llevó a observar experiencias regulatorias desarrolladas fuera del país, concretamente, el llamado Reglamento de Inteligencia Artificial de la Unión Europea⁴, el que ofrece un referente relevante por adoptar un modelo basado en el riesgo: la intensidad de las obligaciones jurídicas aumenta en función del potencial que presenta cada sistema para afectar la seguridad, los derechos fundamentales y otros bienes jurídicamente protegidos. Desde esta perspectiva, no toda utilización de inteligencia artificial recibe el mismo tratamiento ni toda tecnología de vigilancia puede ser jurídicamente equiparada.

Es de nuestra consideración que un sistema de reconocimiento automatizado de placas vehiculares no puede confundirse sin más con sistemas de identificación biométrica remota de personas, reconocimiento de emociones, puntuación social o mecanismos de actuación policial predictiva. Cada tecnología utiliza información diferente, persigue finalidades distintas y genera riesgos particulares; por ello, trasladar el modelo europeo al contexto nicaragüense no significa reproducir mecánicamente sus prohibiciones o categorías⁵, sino aprovechar los principios que lo sustentan para preguntarse qué nivel de riesgo genera el sistema que se pretende implementar y qué garantías deberían acompañar su utilización.

La protección de datos constituye otro componente indispensable de esta discusión, pues la incorporación de inteligencia artificial a los sistemas de videovigilancia transforma progresivamente la cámara tradicional, que se limita a registrar imágenes, en una herramienta capaz de procesarlas, clasificarlas y relacionarlas con información previamente almacenada. Cuando el sistema vincula,

² Ley 787, de 21 de marzo de 2012, Ley de Protección de Datos Personales, La Gaceta Diario Oficial núm. 61 de 29 de marzo de 2012.

³ Ley 1042, de 27 de octubre de 2020, Ley Especial de Ciberdelitos, La Gaceta Diario Oficial núm. 201 de 30 de octubre de 2020.

⁴ Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 Y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2017/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), Diario Oficial de la Unión Europea núm. 1689, de 12 de julio de 2024.

⁵ Vid. Alemán-Madrigal, L. E. y López Esquivel, S. E., “La Inteligencia Artificial y el Derecho del Trabajo: retos en la protección de los trabajadores nicaragüenses”, *Revista Jurídica del Trabajo*, vol. 7, núm. 18, 2026, pp. 113-116.

por ejemplo, una placa vehicular con el nombre de una persona, su condición de estudiante o trabajador, su autorización de ingreso y los registros de acceso a determinadas instalaciones, la cuestión deja de ser exclusivamente tecnológica para convertirse también en un problema de tratamiento de datos personales.

Ello exige que la utilización de estos sistemas se encuentre acompañada de garantías relacionadas con la finalidad del tratamiento, transparencia, proporcionalidad, seguridad de la información y limitación del acceso y conservación de los datos. La búsqueda de mayor seguridad no puede convertirse en una habilitación general para recopilar y utilizar cualquier información disponible; por el contrario, cuanto mayor sea la capacidad tecnológica para observar y procesar información sobre las personas, mayor deberá ser también la exigencia de justificar la necesidad de su utilización y establecer controles frente a eventuales abusos.

La incorporación progresiva de tecnologías inteligentes puede contribuir a modernizar los mecanismos utilizados por empresas e instituciones para proteger instalaciones, controlar accesos y prevenir determinadas conductas; sin embargo, su desarrollo no debería producirse al margen de una discusión paralela sobre los límites jurídicos de la vigilancia. Seguridad y privacidad no deben plantearse como objetivos necesariamente incompatibles, sino como intereses cuya convivencia requiere reglas previamente definidas.

Lo que comenzó como una propuesta dirigida a comprobar las posibilidades técnicas de un SVI terminó evidenciando que su implementación no puede evaluarse únicamente desde la eficiencia tecnológica. La verdadera dificultad aparece cuando el sistema abandona el laboratorio y comienza a interactuar con personas cuyos movimientos, vehículos, imágenes o datos pueden ser registrados y procesados. La implementación de sistemas inteligentes de videovigilancia en Nicaragua requiere avanzar simultáneamente en dos direcciones: por una parte, aprovechar las posibilidades que estas tecnologías ofrecen para mejorar la seguridad; por otra, desarrollar criterios jurídicos capaces de establecer límites claros respecto de la recopilación, utilización, conservación y protección de la información obtenida. La innovación tecnológica puede contribuir significativamente a la seguridad ciudadana, pero su legitimidad dependerá de que el incremento de las capacidades de vigilancia vaya acompañado de un fortalecimiento equivalente de las garantías de quienes son vigilados.

Luis Ernesto Alemán-Madrigal

<https://orcid.org/0000-0003-3318-6967>

Profesor Asociado Facultad de Derecho, Humanidades y Relaciones Internacionales, Universidad Americana (UAM)

luis_e_aleman@usal.es / <https://luisalemanderecho.blogspot.com/>

Lenin Sebastián Barreto-Pastora

<https://orcid.org/0009-0003-6331-9625>

Estudiante de Ingeniería en Sistema de Comunicación, Universidad Americana (UAM)

Estudiante de Licenciatura en Contabilidad y Finanzas, Universidad Americana (UAM)

lsbarreto@uamv.edu.ni

Lista de Referencias

Alemán-Madrigal, L. E. y López Esquivel, S. E., “La Inteligencia Artificial y el Derecho del Trabajo: retos en la protección de los trabajadores nicaragüenses”, *Revista Jurídica del Trabajo*, vol. 7, núm. 18, 2026. Disponible en: <https://revistajuridicadeltrabajo.com/index.php/rjt/article/view/284>

Ley 787, de 21 de marzo de 2012, Ley de Protección de Datos Personales, La Gaceta Diario Oficial núm. 61, de 29 de marzo de 2012. Disponible en <http://digesto.asamblea.gob.ni/consultas/utl/pdf.php?type=rdd&rdd=HOyUfBOpy6c%3D>

- Ley 1042, de 27 de octubre de 2020, Ley Especial de Ciberdelitos, La Gaceta Diario Oficial núm. 201, de 30 de octubre de 2020. Disponible en <https://digesto.asamblea.gob.ni/consultas/util/pdf.php?type=rdd&rdd=SN1tt24fk8U%3D>
- Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 Y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2017/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), Diario Oficial de la Unión Europea núm. 1689, de 12 de julio de 2024. Disponible en <https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079>
- Vizcaíno Zamora, Á. “Videovigilancia e inteligencia artificial: entre la utopía y la distopía”, *Revista Mexicana de Ciencias Penales*, vol. 4, núm. 14, 2021. DOI: <https://doi.org/10.57042/rmcp.v4i14.432>