EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Excélsior
Sección: Portada, dinero
2025-09-24 01:55:10 1234 cm^2 Página: 1, 6 - 7 1/5

RECONFIGURAN OPERACIONES

Redes criminales amplifican poder con uso de la IA

EMPLEANDO INTELIGENCIA ARTIFICIAL para rastrear a personas vulnerables o suplantar identidades, obtienen ganancias que pueden superar las que dejan las drogas

POR PAUL LARA

La inteligencia artificial generativa (IA Gen) está detonando la potencia de los grupos del crimen organizado, que la emplean para hacer los llamados *deepfakes* y delinquir.

Los equipos tecnológicos del crimen organizado han usado chatbots y agentes de IA para rastrear en redes sociales, servicios de mensajería y sitios web, los perfiles de gente que puede ser fácilmente engañada. Los casos de éxito de fraude son altos, al punto que los cárteles están ganando millones de pesos, a veces más de lo que obtienen por la venta de drogas.

"El uso de la IA por parte del crimen organizado ha dejado de ser un concepto de ciencia ficción para convertirse en una cruda realidad que está reconfigurando las operaciones delictivas en América Latina. Lejos de la imagen de mafias obsoletas, organizaciones criminales de alto riesgo (...) han integrado la IA en su *modus operandi*, trasladando una parte crucial de sus actividades al ámbito digital", explica Juan Manuel Aguilar, autor del estudio presentado hace unos días a escala mundial llamado: *Uso de inteligencia artificial por redes criminales de alto riesgo*, que trabajó en conjunto con el Paccto 2.0, un brazo de investigación de la Unión Europea.

Mediante estas tecnologías, los cárteles han logrado replicar voces de familiares o figuras de autoridad con alto nivel de fidelidad acústica, lo que ha permitido montar escenarios de secuestro, emergencia médica o coerción judicial.

DINERO

EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Excélsior
Sección: Portada, dinero
2025-09-24 01:55:10 1234 cm^2 Página: 1, 6 - 7 2/5

FRAUDES, ESPIONAJE, TRÁFICO Y LAVADO

LA IA POTENCIA A LOS CÁRTELES MEXICANOS

EL CJNG Y EL CÁRTEL DE SINALOA cuentan con equipos especializados en uso de inteligencia artificial generativa para cazar, engañar y estafar a sus víctimas, así como vulnerar equipos federales y servicios de mensajería ›6 Y 7

> Los cárteles han integrado la IA en su *modus operandi*, trasladando una parte crucial de sus actividades al ámbito digital. Esta modernización tecnológica les permite optimizar la eficiencia, reducir la exposición de sus miembros y amplificar su capacidad de daño a una escala sin precedentes.

JUAN MANUEL AGUILAR
PROFESOR DE LA UNAM Y AUTOR DEL ESTUDIO USO DE INTELIGENCIA ARTIFICIAL POR REDES CRIMINALES DE ALTO RIESGO

EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Excélsior
Sección: Portada, dinero
2025-09-24 01:55:10 1234 cm^2 Página: 1, 6 - 7 3/5

CÁRTELES USAN IA

LA SOMBRA ALGORÍTMICA DEL CRIMEN ORGANIZADO

Las nuevas herramientas tecnológicas transforman los negocios ilícitos, según un reporte del Pacto 2.0 de la Unión Europea y un investigador de la UNAM

POR PAUL LARA
paul.lara@gimm.com.mx

Tu esposa, tu hermana, tu pareja o tu madre, un familiar directo, ha recibido una llamada con tu voz, o inclusive una videollamada con tu imagen. En ella, le solicitas dinero, pues has sido secuestrado, o tal vez tuviste un accidente, te quedaste sin dinero para pagar la renta o la despensa en el centro comercial. Los casos pueden ser muchos, pero el objetivo es el mismo: recibir una cantidad específica.

Todo esto es falso. Grupos del crimen organizado en México, como el Cártel Jalisco Nueva Generación (CJNG) o el Cártel de Sinaloa, han utilizado inteligencia artificial generativa (IA Gen) para usar los llamados *deepfakes* y delinquir. Lamentablemente, un gran porcentaje de los contactados son defraudados.

Pero no son elegidos al azar. Los equipos tecnológicos del crimen organizado han usado chatbots y agentes de IA para rastrear en redes sociales, servicios de mensajería y sitios web, los perfiles de gente que puede ser fácilmente engañada. Los casos de éxito de fraude son altos, al punto que los cárteles están ganando millones de pesos, a veces más que vender drogas.

"El uso de la inteligencia artificial (IA) por parte del crimen organizado ha dejado de ser un concepto de ciencia ficción para convertirse en una cruda realidad que está reconfigurando las operaciones delictivas en América Latina. Lejos de la imagen de mafias obsoletas, organizaciones criminales de alto riesgo como el Cártel de Sinaloa y el Cártel Jalisco Nueva Generación (CJNG) han integrado la IA en su modus operandi, trasladando una parte crucial de sus actividades al ámbito digital. Esta modernización tecnológica les permite optimizar la eficiencia, reducir la exposición de sus miembros y amplificar su capacidad de daño a una escala sin precedentes", explica Juan Manuel Aguilar, profesor de la Universidad Nacional Autónoma de México (UNAM) y autor del estudio presentado hace unos días a escala mundial llamado: *Uso de inteligencia artificial por redes criminales de alto riesgo*, que trabajó en con-

junto con el Paccto 2.0, un brazo de investigación de la Unión Europea.

Desde su punto de vista, la IA no funciona como gadget, sino como sistema: desde los bots conversacionales que inducen al pago bajo amenaza, hasta los algoritmos que seleccionan víctimas por perfil psicológico, y lo que se observa es una integración sistémica que convierte a la verticalidad en ventaja táctica. La orden no sólo baja en la cadena de mando: se programa.

La tecnología, según el estudio, ha permitido la producción automatizada de mensajes persuasivos, redactados en distintos registros emocionales y adaptados culturalmente. "La capacidad de simular interacciones conversacionales verosímiles –a través de modelos de lenguaje entrenados para sostener diálogos prolongados– ha sido esencial para el desarrollo de esquemas de fraude afectivo y emocional, como el conocido *pig butchering*".

Un elemento complementario y particularmente perturbador ha sido la incorporación de sistemas de clonación de voz. Mediante estas tecnologías, los cárteles han logrado replicar voces de familiares o figuras de autoridad con alto nivel de fidelidad acústica, lo que ha permitido montar escenarios de secuestro, emergencia médica o coerción judicial que resultan emocionalmente devastadores para las víctimas.

En el plano visual, la utilización de *deepfakes* ha comenzado a consolidarse como recurso de alto impacto simbólico. Se han identificado casos en los que se emplean tecnologías de reconstrucción facial y *lip-sync* automatizado para simular videos de supuestas agresiones, capturas o amenazas.

Los bots conversacionales programados con IA permiten escalar la extorsión sin requerir interlocución humana directa. "Estos bots están diseñados para detectar patrones emocionales en las respuestas de la víctima y ajustar su tono o contenido en tiempo real, maximizando la presión psicológica mediante una lógica de retroalimentación algorítmica", explica Aguilar.

LAS VÍCTIMAS

Algunos casos son brutalmente perturbadores. Los cárteles se infiltran a través de la tecnología en colectivos como madres buscadoras, a quienes con videos o voces falsas les solicitan fotos y videos de sus desaparecidos, para luego con el uso de la IA generativa clonar las imágenes y sus voces, y hacerles creer que aún están vivos, pedirles dinero y defraudarlos. Los algoritmos de los cárteles permiten localizar fácilmente a individuos en situación de vulnerabilidad digital, afectiva o económica: adultos mayores, mujeres solas, migrantes y personas con escasa alfabetización tecnológica. Estos sectores constituyen el blanco principal de campañas de fraude afectivo o extorsión familiar, construidas con información personalizada obtenida a través de scraping o bases de datos filtradas.

En segundo lugar, las microempresas, comerciantes locales y trabajadores por cuenta propia enfrentan amenazas automatizadas que simulan procesos judiciales, sanciones fiscales o denuncias falsas. Estos mensajes, enviados desde cuentas cifradas o números rotativos, reproducen identidades visuales oficiales e incluyen deepfakes de funcionarios para inducir miedo y pagos inmediatos. La desprotección institucional y la saturación de canales de denuncia amplifican la efectividad de esta coerción.

"También son víctimas las comunidades locales, especialmente en regiones con débil presencia estatal o alta conflictividad. Allí, los cárteles implementan campañas de ocupación simbólica, difundiendo amenazas, comunicados falsos o rumores digitales que minan la confianza, paralizan la denuncia y normalizan la sumisión. Este tipo de coerción algorítmica no requiere control territorial directo: controla la narrativa del espacio mediante automatización del miedo", agrega el especialista de la UNAM.

El uso de IA por parte del CJNG y el Cártel de Sinaloa ha transformado la relación entre estructura criminal y espacio social. La violencia ya no opera únicamente desde la presencia armada, sino desde la simulación digital, la automatización del daño y la ocupación cognitiva.

El riesgo no reside sólo en las armas, sino en los modelos algorítmicos que personalizan la amenaza, replican el discurso del miedo y desplazan la responsabilidad del perpetrador.

ESTRUCTURAS

Las organizaciones criminales han integrado la IA como "infraestructura operativa" en otras dimensiones críticas de su funcionamiento: la optimización de cadenas logísticas delictivas, el perfeccionamiento de esquemas de lavado financiero multijurisdiccional y la automatización de procesos operativos internos, lo que les permite reducir tiempos, costos y exposición humana en sus actividades de tráfico, extorsión y blanqueo de activos.

El CJNG, ha centralizado el desarrollo de esquemas de extorsión automatizada con IA generativa. Esta organización ha sido pionera en el uso de clonación de voz y bots conversacionales para realizar fraudes emocionales, como el conocido pig butchering, en el que se construyen vínculos afectivos falsos con víctimas a lo largo del tiempo, hasta inducirlas a transferir grandes cantidades de dinero.

En paralelo, el Cártel de Sinaloa ha adoptado una lógica de replicación descentralizada. Diversas células operan de manera autónoma en la ejecución de campañas de smishing (suplantación de funcionarios y manipulación de identidades digitales). Este modelo facilita una rápida adopción de herramientas como deepfakes, traducción algorítmica o geolocalización automatizada, muchas veces sin necesidad de una estructura.

"Una de las prácticas más extendidas es el uso de software de scraping y minería de datos, aplicado a redes sociales, directorios públicos y bases de datos filtradas. Esta información es procesada por sistemas clasificatorios que construyen perfiles de vulnerabilidad individual, seleccionando víctimas por edad, localización, nivel educativo o tipo de empleo. El cruce de estas bases con motores de IA ha elevado la precisión de campañas criminales a niveles inéditos", explica Aguilar.

Ambos cárteles han integrado el uso de mensajería automatizada y distribución algorítmica de amenazas. Las campañas de smishing y vishing, enviadas desde cuentas temporales o mediante redes cifradas, son alimentadas con datos personales obtenidos por scraping o por compra directa en foros clandestinos.

La automatización permite mantener decenas de miles de contactos activos, con mensajes que se ajustan al perfil de la víctima: nombre completo, ubicación, nombres de familiares, lugar de trabajo o historial digital. Esta personalización opera como verificador de autenticidad, generando miedo y urgencia sin requerir contacto directo.

Otro factor que se explica, es que los cárteles han colocado cámaras de vigilancia para temas de reconocimiento facial en decenas de estados en los que operan, y han vulnerado las del gobierno, desde donde vigilan a personas, autoridades y negocios para tener más conocimiento de a quién van a estafar, o tomar datos para sus ilícitos.

LA INFRAESTRUCTURA

Logística Inteligente:
Han incorporado algoritmos de smart routing para optimizar las rutas de tráfico de drogas y personas, haciendo más eficiente el transporte de sus ilícitos.

Extorsión y Fraude:
El CJNG, en particular, ha centralizado el desarrollo de esquemas de extorsión automatizada. Utilizan la clonación de voz y bots conversacionales para llevar a cabo "fraudes emocionales" y estafas como el pig butchering en el que construyen vínculos afectivos falsos para engañar a sus víctimas y despojarlas de grandes sumas de dinero. Por su parte, el Cártel de Sinaloa ha adoptado una lógica descentralizada para ejecutar campañas de smishing (suplantación de funcionarios) y manipular identidades digitales a gran escala.

Vigilancia y Control:
La IA también se articula con estrategias de propaganda, extorsión, reconocimiento facial y vigilancia territorial, reforzando su poder sobre los territorios que controlan, tanto físicos como digitales.

RECOMENDACIONES

Creación de Unidades Especializadas:
Es imperativo establecer unidades híbridas con capacidades técnico-jurídicas avanzadas. Estas células deben integrar a peritos digitales, fiscales, policías cibernéticos, ingenieros de datos y analistas de inteligencia para investigar el crimen algorítmico.

Protocolos Forenses:
Se necesita diseñar protocolos forenses específicos para el análisis de evidencia generada por IA, garantizando su autenticidad e integridad en procedimientos judiciales.

Cooperación Multijurisdiccional:
En países con estructuras federales como México, es vital articular respuestas coherentes entre los distintos niveles de gobierno, estableciendo mesas técnicas permanentes y armonizando los protocolos de investigación.

Puntos de Contacto Nacionales:
Cada país debe designar puntos de contacto especializados en IA criminal (SPOC-IA) para facilitar la comunicación y coordinación con redes policiales internacionales como la Interpol.