CIBERDELITOS, EL FENÓMENO DELICTIVO Y LA INTELIGENCIA ARTIFICIAL

Abg. Juan Fernando Calderón
Abogado Asociado - Fexlaw Abogados

FEXLAW ABOGADOS



El fenómeno delictivo, por su naturaleza, siempre ha estado un paso adelante de las instituciones punitivas del Estado. Esto no debería sorprender a nadie, ya que responde a una lógica de causa y efecto: primero ocurre el delito, y luego la reacción estatal. Por ejemplo, si se produce un asalto a un banco, los agentes del orden llegarán al lugar de los hechos minutos después, dependiendo de factores como la eficiencia y la logística. Si las labores de investigación son eficaces, es probable que logren dar con el paradero de los criminales; de lo contrario, se iniciará una investigación que dependerá de la calidad de las técnicas utilizadas para tener éxito.

En ambos escenarios —uno claramente más eficaz que el otro— el fenómeno criminal parte con ventaja: debe primero ser descubierto, lo que plantea a las fuerzas del orden el reto de detectar y neutralizar la amenaza. Esta ventaja no es nueva ni sorprendente, ha sido una constante. Sin embargo, el problema actual es mucho más complejo. Desde hace un par de décadas, la tecnología ha sido clave para derribar obstáculos, superar límites y facilitarnos, literalmente, estar a un solo clic de un delincuente o de una estafa masiva. ¿Es entonces la tecnología la culpable del avance del crimen? La respuesta es rotundamente no; pensar eso es un error.

Lo que sí ha cambiado es la forma en que los delincuentes cometen sus crímenes. Con la llegada de la inteligencia artificial (IA), esa ventaja histórica que mencionábamos se ha triplicado. ¿Cómo? Veamos el caso revelado por la Policía de Hong Kong el año pasado: un trabajador financiero de una multinacional fue engañado para transferir 25 millones de dólares. Durante una videollamada, creyó estar hablando

Abg. Juan Fernando Calderón
Abogado Asociado - Fexlaw Abogados

con el director financiero de la empresa y con colegas que conocía bien. Sin embargo, todos los participantes habían sido recreados con tecnología de deepfake, utilizando inteligencia artificial. ¿En qué consiste esto? En la creación de imágenes, videos e incluso voces que simulan a personas reales, cuando en realidad todo es un montaje digital.

Esta tecnología ya está siendo utilizada también por grupos criminales en la frontera entre México y Estados Unidos. Supuestas fundaciones, con la fachada de ayudar a localizar familiares desaparecidos, reciben fotos de las víctimas y las manipulan con IA para crear videos falsos en los que los desaparecidos aparentan estar secuestrados. Luego, exigen dinero por su "liberación".

Cuando hablamos de que la ventaja del crimen se ha triplicado, nos referimos a dos aspectos: primero, la eficacia de la IA como herramienta para delinquir; segundo, el engaño tan sofisticado que muchas víctimas ni siquiera se enteran de que han sido estafadas, como en el caso de Hong Kong, donde el trabajador no tuvo posibilidad de alertar a tiempo, y cuando su empresa se percató, ya era demasiado tarde.

Muchos se preguntarán: ¿debemos detener el avance de la inteligencia artificial? La respuesta es un no rotundo. No se trata de parar el desarrollo, sino de preguntarnos si nuestras instituciones estatales, fuerzas del orden, unidades especializadas del Ministerio Público, empresas y demás actores estamos preparados para usar la IA como herramienta en la lucha contra el crimen. Aquí los delincuentes llevan otra ventaja: ellos simplemente la usan, sin regulaciones. En cambio, las instituciones públicas requieren reformas legales, formación y recursos para incorporar estas tecnologías. Por eso, debemos empezar cuanto antes, para que el futuro no nos tome desprevenidos.