¿Qué es la ciberesclavitud?

Irene Noboa

21 de marzo de 2025

Irene Noboa

Estudiante ecuatoriana en el último año de la carrera de Relaciones Internacionales, con una especialización en Servicios de Inteligencia. Comprometida con la protección de la seguridad y libertad a nivel

nacional e internacional, con un profundo interés en las dinámicas de organismos transnacionales que influyen en la volatilidad y liquidez de nuestro mundo, especialmente América Latina.

La globalización y los avances tecnológicos han transformado nuestra forma de vivir y conectar, pero también han dado pie a nuevos peligros. Las redes criminales transnacionales aprovechan la falta de regulación en territorios vulnerables, exponiendo a miles de personas a la explotación. Un caso reciente ilustra cómo la interconexión global ha facilitado la creación de un nuevo tipo de esclavitud: la ciberesclavitud.

El famoso actor chino Wang Xing recibió una oferta de trabajo para una audición en Tailandia y no dudó en coger el primer vuelo a Bangkok para aprovechar la oportunidad. Pensó que era una oferta normal, dijo el actor, como la que tuvo anteriormente en el 2018. Lo que no se imaginaba era su verdadero destino final, donde afeitaban su cabeza, confiscaban sus pertenencias y lo entrenaban para el fraude cibernético.

Vivimos en un mundo quebradizo, volátil e incierto. La interconexión que la globalización ha traído para el mundo es increíble, con flujos culturales y económicos nunca antes vistos. Con los avances tecnológicos hemos logrado llevarlo a otro nivel, creando una realidad virtual donde las fronteras y los kilómetros que nos separan desaparecen, aumentando la comunicación transnacional.

Aunque hemos demostrado a lo largo de los años que esta combinación ha beneficiado nuestro desarrollo, su novedad ha traído nuevos desafíos. Con la velocidad de la tecnología y la globalización, nuevos modos de criminalidad han aparecido, aprovechando la porosidad de las fronteras, especialmente en territorios donde no es eficiente el poder de un gobierno.

El domingo 23 de febrero, la policía tailandesa y de Camboya trabajaron juntos para rescatar a 215 extranjeros que se encontraban forzados en un centro de estafa cibernética en Poipet. En dichas oficinas, operan algunos por voluntad propia, pero la trata de personas ha incrementado con el crecimiento de estos centros, dando lugar para un nuevo tipo de esclavitud del siglo XXI, la esclavitud cibernética.

➞ Te puede interesar: ¿Cuáles son las tácticas más comunes de captación en la trata de personas?

Operado por organizaciones criminales transnacionales, su cobertura para «reclutar» trasciende las fronteras. En la última operación policial,

rescataron a 109 taiwaneses, 50 pakistaníes, 48 indios, 5 taiwaneses y 3 indonesios, demostrando la magnitud del sistema de redes criminales.

¿Qué es la ciberesclavitud?

Es la esclavitud moderna, en la cual se trafican humanos para explotarlos laboralmente y que participen en actividades criminales involuntariamente, contribuyendo económicamente a los explotadores y a los traficantes. En el caso de que las víctimas se resistan, sufrirán consecuencias de violencia física, psicológica o ataduras económicas a la red criminal.

Inicia con la trata de personas. Reclutan a los trabajadores de manera engañosa, por medio de falsas ofertas laborales, secuestros o comprando a las víctimas de otros operadores como mercancía. Es un trabajo donde la víctima es tanto el estafado como el estafador. Se han dado casos donde pueden irse si consiguen reclutar a otra persona que ocupe su lugar, convirtiéndonos en cómplices de la trata de personas y de la red criminal.

→ Te puede interesar: El plan de España para luchar contra la trata y explotación de seres humanos

Según el último informe publicado por UNODC, hay distintos métodos empleados para mantener a los trabajadores en el ciclo de trabajo forzado. Unos son más sutiles, como por supuestas «deudas» acumuladas por los costos que los operadores tuvieron al transportarlos de un lugar a otro. En otros casos, los obligan a trabajar 17 horas diarias sin descanso bajo la amenaza de no alimentarlos, abusarlos físicamente o venderlos a otro operador.

El crimen organizado

La imagen adjuntada incluye las ubicaciones de los centros de fraude en las zonas económicas especiales en Laos, Camboya, Myanmar y Tailandia, publicada por UNODC. Estas zonas fueron creadas para fomentar el comercio, pero han sido infiltradas por redes criminales transnacionales.

Por ejemplo, la zona económica especial del triángulo dorado en Laos ahora es liderada por Zhao Wei, un criminal chino que controla la zona desde el Kings Romans Casino. Son zonas donde la ausencia del poder gubernamental es notoria, y se han convertido en el refugio de sus

actividades, manifestando que el modelo de SEZs no solo atrae inversión, sino que ha beneficiado a redes criminales.

La falta de regulación en el sector digital facilita la impunidad, dado que aprovechan los exchanges de criptomonedas y plataformas de apuestas para lavar el dinero. Simultáneamente, estas lagunas con el crecimiento de las estafas en línea crean las condiciones para la esclavitud digital.

→ Te puede interesar: La hibridación del crimen organizado: tendencias y desafíos actuales

La presencia de sindicatos criminales chinos, como el 14K Triad, expande el modelo de negocios. Su líder principal, Wan Kuok Koi, es uno de los inversores principales de los casinos y granjas de fraudes. Sus empresas han sido acusadas previamente de complicidad con el tráfico de drogas, trata de personas y apuestas ilegales.

El crimen organizado es altamente dependiente del flujo de dinero. Tanto para operaciones actuales como futuras. La velocidad que hoy experimentan los avances tecnológicos facilita espacios para que dichas actividades se cometan antes del desarrollo de una legislación efectiva.

El momento en el que se integren técnicas impulsadas por IA aumentará el fraude cibernético en términos de volumen. La velocidad y escala del fraude cibernético serán mayores y más sofisticados, haciendo que el alcance, el contenido y los recursos de los grupos criminales sean más eficientes y convincentes.

Ciberesclavitud y las múltiples víctimas del fraude

Hay dos víctimas haciendo dinero involuntariamente para los centros de fraude. La primera víctima es el reclutado. Ha habido testimonios de víctimas aclamando que tenían una oferta laboral que parecía ser prometedora, por lo cual emprenden su viaje. Por ejemplo, Nantapat Yaemmanat, un tailandés que fue atraído por una oferta laboral en un casino de Myanmar por medio de Facebook. Fue golpeado a diario con una barra de hierro gruesa. Su deber era convencer a sus objetivos de invertir en criptomonedas.

Jalil Muyeke, otra víctima nacida en Uganda, tuvo una experiencia similar a la de Nantapat. Convencido de que viajaba a Bangkok para una

oferta laboral, terminó en un centro de estafas. Coercitivamente, tuvo que firmar documentos, y comenzar su trabajo por los siguientes 7 meses. *«Hay toda una ciudad en esas paredes»*, recuerda Muyeke sobre la granja de estafas. *«La mayoría de nosotros lo hacíamos porque queríamos sobrevivir allí. Nunca quisimos estafar a nadie.»*

Pero las víctimas no solo son los retenidos. Daniel, un sueco de 40 años, conoció a «Adele» en Tinder. «Ella» lo sedujo a invertir en criptomonedas, mientras desconocía que este sería el principio de su pesadilla. Invirtió casi todos sus ahorros una vez que confió en la aplicación, perdiéndolo todo. Él se había dejado convencer por un grupo de WhatsApp, donde estaba Manish Aurora, un gestor de fondos estadounidenses. Al ponerse en contacto con él, descubrió que solo era otra víctima a quien le robaron la identidad y arruinaron su reputación.

→ Te puede interesar: Las 10 empresas referentes en ciberseguridad en España

La estrategia utilizada para estafar es conocida como *sha zhu pan* o *matanza de cerdo*. Un tipo de fraude en el cual el estafador se encarga de ganarse la confianza del estafado, desarrollando una relación afectiva con él (engordan el cerdo), hasta llegar al momento correcto de estafar. Una vez que la víctima cae en el engaño, aprovechan la oportunidad (la matanza del cerdo).

Para llevarse su pedazo del pastel, los estafadores recurren a grandes exhanges de criptomonedas que afirman cumplir con las regulaciones AML/KYC y KYT, pero han servido como puntos de salida para un promedio de 27.800 millones de dólares estadounidenses anuales en flujos ilícitos, de los cuales 5.600 millones llegan de intercambios occidentales.

El impacto global de la cibereesclavitud y la necesidad de una cooperación internacional

El momento en que rescataban a Wang Xing fue crucial para las familias de las víctimas en China. Él se encontraba en Mae Sot, un punto clave para centros de actividad criminal. La amplia gama de centros fraudulentos representa la escala y el poder bajo los cuales estas organizaciones operan. China y el resto de los estados de ASEAN deben trabajar juntos para combatir a este enemigo en común.

Sin embargo, existen matices sobre quiénes deben rescatarse y quiénes son cómplices de las redes criminales. Los centros de fraude cibernético incluyen tanto ciber-esclavos como voluntarios. La limitada oferta laboral en la región ha llevado a muchos jóvenes a participar de estas actividades bajo la promesa de ganar grandes riquezas rápidamente. Similar a las organizaciones de narcotráfico en Latinoamérica, las condiciones socioeconómicas de los territorios pueden contribuir al reclutamiento.

Los esfuerzos por rescatar a las víctimas son principalmente voluntarios, pero la cooperación internacional en el asunto ha disminuido desde que USAid congeló su contribución bajo el mandato de Donald Trump. La congelación de fondos ha obligado a la sociedad civil y a los programas relacionados con la prevención de trata de personas a poner en pausa sus operaciones.

→ Te puede interesar: ¿Cómo afecta la trata de personas a la estabilidad geopolítica?

Por ejemplo, Caritas, una organización benéfica católica que acoge a refugiados que han escapado de los centros en Camboya, recientemente se vio obligada a dejar salir a algunas víctimas y es posible que no puedan aceptar a más por falta de fondos.

La ciberesclavitud en la región destaca múltiples desafíos globales que alimentan la eficiencia del crimen organizado, por lo tanto, es necesario un acercamiento multifacético e intersectorial. Que UNODC se involucre es un gran comienzo; no obstante, es necesario fortalecer las regulaciones y su aplicación para prevenir lagunas jurídicas.

Al ser un fenómeno global, la cooperación internacional es imprescindible, tanto como mejorar las infraestructuras digitales para prevenir el crecimiento de estas redes. Pero principalmente, es importante aprovechar la velocidad de las redes para crear conciencia en los usuarios que corren el riesgo del día de mañana ser una víctima más del fraude cibernético. Con importante atención a aquellos en las regiones más vulnerables.