Fraude "agéntico", la gran oportunidad

José de la Peña Muñoz
Director
jpm@codasic.com

Entretenidos como estamos en la vorágine de las IA, y sin que todavía hayamos superado algunas limitaciones de persistencia en la conexión a Internet y de acceso a las redes de telefonía celular (cualquier tiempo pasado fue peor, todo hay que decirlo), los CISOs cuyas ocupaciones del día a día les permiten dedicar un tiempo a los análisis prospectivos, ya tiemblan ante una posible amenaza nunca antes vista: la explosión del comercio "agéntico" asistido y autónomo, que vendrá acompañado de la correspondiente explosión de fraude "agéntico" asistido y autónomo.

> En el tiempo que le quede tras el día a día, el CISO que tenga ganas y fuerzas puede relajarse criando un agente IA deseoso de quedar bien con su dueño y preguntarle si alguna vez se traspondrá a la legislación española la NIS2. Aunque no la necesitemos.

La industria de la ciberseguridad no está madura –al menos a efectos públicos– para ofrecer plataformas orientadas a las ciberseguridades en comercio "agéntico". Y tampoco sabemos cómo se va a ir desarrollando, porque es el propio comercio el que se va a ver sacudido por la IA, y con él, las legislaciones, regulaciones, contratos y prácticas. Es una buena oportunidad para emprendedores en ambos frentes, el de la ciberseguridad y el del derecho.

Lo que los expertos sospechan es que el comercio "agéntico" tiene todas las papeletas para provocar el siguiente apretón en ciberseguridad, en privacidad y, en general, en la forma de gestionar los riesgos y el aseguramiento en las empresas a efectos globales.

Imaginemos a los hoy sujetos de derecho (personas físicas y jurídicas) haciendo operaciones de comercio electrónico y digital, conviviendo con órdenes automáticas de compra, sistemas de *trading* algorítmico (valores, divisas, futuros, opciones, criptomonedas…), adhesión a servicios de renovación automática, intermediaciones y delegaciones "agénticas"… ¡Reclamaciones "agénticas", devoluciones "agénticas", *call centers* "agénticos" en las nubes, sanciones "agénticas"! Y todo a toda velocidad y en todas partes.

La cosa puede (debe) funcionar. Pero hay que diseñar bien el modelo, y, sobre todo, hay que saber gestionar un delicado multiconstructo que operará a efectos globales a la velocidad de la luz en el medio que toque, generando derechos y obligaciones a personas (por ahora) de una forma muy diferente a aquellos *bitubí* y *bitusí* que se abrieron camino allá por el año 2000.

Inmadurez "agéntica"

En líneas generales sabemos los frentes por los que es más factible que den la cara los chorizos sueltos y en manada (manipulación de agentes, suplantación, datos falsos, secuestro de credenciales y robo de permisos, fraude conversacional, colusión entre agentes, generación de agentes fraudulentos, desinformación y autorizaciones falsas, fraude de agente contra agente, escalado masivo de ataques, personalización de engaños, ataques a la cadena de herramientas propias y de terceros, orquestación de explotación de vulnerabilidades muy complejas...), y, por tanto, con asistencia "agéntica" de calidad podremos amplificar la observabilidad, la verificación de identidades, la detección de anomalías, la consulta automática a inteligencia multifuente accionable, la ponderación de intenciones, el reajuste de políticas, …

Al fin y al cabo, lector, este es el desarrollo de las TIC en esta fase de la sociedad algorítmica, en la que hasta el matemático y actual Papa, León XIV, ha considerado oportuno escribir su Carta Encíclica Magnífica Humanitas sobre la custodia de la persona humana en el tiempo de la IA, cuya lectura recomiendo.

Eso sí, mientras se va desenrollando esta revolución, vamos a tener que seguir gestionando la ciberseguridad en el día a día –que todavía no es tan "agéntico" como parece el futuro– y, si acaso, pensar en el plan criptográfico poscuántico y criptoágil, el impacto de las carteras de identidad europeas en la empresa, el impacto en el acortamiento de los tiempos de descubrimiento, detección y explotación de vulnerabilidades de día cero y sin día cero, la supresión de brechas, la mejora del sistema de ciberseguridad para que las pólizas de ciberseguros cuesten menos y tengan más coberturas y… ¡la obtención del presupuesto!

Y en el tiempo que quede, criar un agente inteligente deseoso de quedar bien con su dueño y preguntarle si alguna vez tendremos una ley mediante la que, al menos, se trasponga a la legislación española la NIS2. Aunque no la necesitemos. ●