

El uso de la inteligencia artificial en la lucha contra la ciberdelincuencia

Estamos en los albores de una era que impondrá aún más presión sobre las organizaciones para que mejoren sus procesos. Para enfrentar el ciberdelito debemos cambiar la forma en que operan las organizaciones en materia de lucha contra la ciberdelincuencia. Estos delitos aumentan vertiginosamente; se han convertido en una amenaza para la seguridad y la economía mundial, y el factor humano no es capaz de detectarlos y rastrearlos a tiempo, por lo cual, debemos hacer uso de la inteligencia artificial para detectar y responder a este delito.

La pregunta es ¿cómo lo hacemos?

Primero

Es necesario promulgar leyes que exijan el uso de inteligencia artificial en el rastreo y la detección del ciberdelito.

Esto se puede lograr adaptando la ley procesal penal a fin de que el personal judicial pueda detectar y rastrear el ciberdelito de forma rápida sin tener que atravesar procedimientos judiciales complejos y largos. Cuando la ley confiera las facultades legales a estos funcionarios, podrán detectar y rastrear el ciberdelito en el momento justo.

Segundo

Contar con personal judicial que tenga facultades para responder a estos delitos con rapidez.

Debe haber personal judicial autorizado para realizar todas las diligencias judiciales con la misma rapidez con la que se cometen dichos delitos.

Deben contar con una sólida formación académica y entrenamiento; una combinación de formación en leyes y capacitación técnica, como el uso de Internet para encontrar prueba y dar con la persona que cometió el delito. Todo esto supone desarrollar un programa de capacitación para el personal judicial a fin de que puedan responder a estos delitos, técnica y procedimentalmente, con el mayor nivel de profesionalismo.

Tercero

Se debe contar con un sector de seguridad especializado en estos delitos que esté a cargo de la investigación.

Es necesario crear un sector de seguridad especializado en ciberdelincuencia con facultades para abordar e investigar la comisión de dichos delitos, encontrar pruebas y someter a los infractores a la justicia.

Cuarto

Fiscales especializados en ciberdelincuencia.

Es necesario contar con fiscales especializados en estos delitos porque se trata de delitos rápidos y muy peligrosos que requieren la intervención de un fiscal experto en la materia.

Quinto

Tribunales especializados en ciberdelincuencia.

Tribunales especializados en ciberdelincuencia con jueces que dispongan de conocimiento y experiencia sobre las características de estos delitos a fin de que se haga justicia y que la condena sea adecuada.

Sexto

Debe haber acuerdos internacionales que prevean el uso de inteligencia artificial en la lucha contra la ciberdelincuencia y la provisión y el pedido de asistencia en materia de inteligencia artificial a fin de llevar a juicio a los responsables de la comisión de estos delitos.

Debe haber acuerdos internacionales que prevean la forma de solicitar y brindar información mediante inteligencia artificial y que establezcan dónde y quién procesará al o a los responsables del delito, puesto que en muchos casos la persona que cometió el delito se encuentra en una jurisdicción distinta de aquella donde se cometió y, a menudo, los delitos se cometen con la ayuda de una persona en una tercera jurisdicción. El delito, además, puede impactar en más de un país aunque se haya cometido en otro. Estos delitos adoptan distintas formas: robo, lavado de dinero o financiamiento del narcotráfico.

Séptimo

Sensibilizar y generar conciencia jurídica entre los ciudadanos de a pie acerca del peligro que supone cometer, participar en la comisión o asistir a quienes cometen estos delitos.

Esto se puede lograr a través de medios de difusión en la comunidad, a través de periódicos, la televisión o las redes sociales.

Octavo

Imponer penas graves a quienes cometan estos delitos.

Se trata de un delito sumamente peligroso y las consecuencias son aún más graves, por lo cual el castigo debe ser el máximo aplicable.

Estadísticas

Ministerio de comunicaciones y tecnología de la información

<https://www.mcit.gov.sa/ar/media-center/news/93609>

El costo de la ciberdelincuencia en Arabia Saudita	Ataques contra empresas saudíes
\$ 2600 millones	69%

Este sitio web de Kaspersky publica las estadísticas diarias de ciberdelitos y ciberataques.

<https://cyberstat.kaspersky.com>

Las estadísticas muestran que se comete un gran número de ciberdelitos por día

Asesor legal Muteab

ALotabi

