MEMORIAS DEL VII CONGRESO EN INVESTIGACIÓN CRIMINAL. MÁS ALLÁ DE LO VISIBLE: REFLEXIONES EN TORNO A LA DEEP WEB EN UN MUNDO HIPERCONECTADO

27 OCT 2023

ISSN: 3028- 7553 (En línea)

MEMORIAS DEL VII CONGRESO EN INVESTIGACIÓN CRIMINAL. MÁS ALLÁ DE LO VISIBLE: REFLEXIONES EN TORNO A LA DEEP WEB EN UN MUNDO HIPERCONECTADO

Olga Patricia Parra Sarmiento
Rectora Fundación de Educación Superior Alberto Merani

Daniel Alejandro Rivera Marín
Coordinador de Programa
Tecnología en investigación criminal y ciencias forenses

María Isabel Otero Cubillos
Compiladora

Angie Lorena Palomino Pinto
Coordinadora de promoción institucional

Carlos Alberto Gómez García
Diseño gráfico y diagramación
Fundación de Educación Superior Alberto Merani
Editor

Teléfono: (57) 601 725 6492
Dirección: Calle 73 # 20 B - 19
Correo: gestioninvestigacion@umerani.edu.co
Bogotá, D.C. 2024

MERANI
Fundación de Educación Superior
Alberto Merani

INTRODUCCIÓN

La Fundación de Educación Superior Alberto Merani se destaca por su liderazgo en la formación de tecnólogos en investigación criminal y ciencias forenses, acumulando más de 20 años de experiencia.

En 2017, la Fundación organizó su primer Congreso Internacional en Investigación Criminal y Análisis Jurídico en colaboración con la empresa Vergara Padilla International Group. La segunda edición, realizada en 2018, se enfocó en la seguridad pública. Un año después, en 2019, tuvo lugar el tercer Congreso Internacional con el tema de Cibercriminalidad, contando con la participación de ponentes nacionales e internacionales. La cuarta edición, celebrada en 2020, se centró en la transformación digital. En 2021, la quinta edición abordó el uso de armas letales y no letales en el ámbito civil. La sexta edición, realizada en 2022, se dedicó al Cibercrimen.

La séptima edición del Congreso Internacional de Criminalística, que se celebra este año, explora la Deep Web, un tema de creciente relevancia en un mundo cada vez más hiperconectado.

Institución de educación superior avalada por el Ministerio de Educación Nacional con la resolución de aprobación vigente número 1327 de 2005.

Palabras de apertura: Rectora

Olga Patricia Parra Sarmiento

Muy buenos días a todos. La Fundación de Educación Superior Alberto Merani les da una cálida bienvenida a nuestro séptimo Congreso Internacional de Investigación Criminal, titulado "Más allá de lo visible: Reflexiones en torno a la Deep Web en un mundo interconectado". Es un honor y privilegio contar con su presencia hoy.

Expresamos un sincero agradecimiento a todos los asistentes, desde estudiantes de nuestra institución y otras casas de estudio, hasta destacados representantes de empresas públicas y privadas del sector. También agradecemos a nuestros respetados docentes del programa de investigación criminal y al personal administrativo por su compromiso y apoyo.

Este Congreso no sería posible sin la valiosa contribución de nuestros conferencistas nacionales e internacionales, cuyo amplio bagaje académico y experiencia profesional enriquecerán nuestras reflexiones sobre la Deep Web y su relevancia en un mundo interconectado.

La Deep Web, un mundo virtual más allá de la superficie de internet, plantea desafíos y oportunidades únicos para la investigación criminal.

Es un espacio donde se entrelazan el anonimato, los retos de ciberseguridad, la privacidad y la actividad delictiva.

Comprender qué es la Deep Web es un reto para quienes tratamos de hacer del mundo un lugar seguro para todos, pues ese conocimiento es esencial para abordar cuestiones que van desde la protección de datos hasta la seguridad nacional.

Estudiar y difundir estos conocimientos es fundamental no solo para investigadores y profesionales del ámbito criminal, sino también para la sociedad en su conjunto. A medida que nuestra vida diaria se vuelve más interconectada, es imperativo estar informados sobre los desafíos y riesgos que representa este entorno. Solo a través del conocimiento y la conciencia podemos desarrollar estrategias efectivas para abordar los problemas de este entorno en constante evolución.

Durante el día de hoy, profundizaremos en los aspectos éticos, legales y técnicos relacionados con la Deep Web. Exploraremos cómo la investigación criminal puede aprovechar las oportunidades que ofrece este espacio al mismo tiempo que enfrenta sus desafíos.

En nombre de nuestra institución, agradecemos a los miembros del equipo de la fundación que organizaron este evento, tanto desde el área académica como desde las áreas administrativa, de comunicaciones y logística. Su dedicación y esfuerzo incansables han hecho posible que estemos aquí hoy. Muchas gracias a todos.

Bienvenidos a este emocionante viaje de conocimiento. Este Congreso es para ustedes y por ustedes, y esperamos estar a la altura de sus expectativas.

Palabras de apertura: Coordinador

Daniel Alejandro Rivera Marín.

Estimados miembros de la comunidad meranista, distinguidos visitantes, directivos de la Fundación de Educación Superior Alberto Merani, estudiantes, docentes, comunidad académica en general y respetados investigadores criminales:

Es un placer darles la bienvenida a este importante evento. Hablar de la Deep Web es abordar un tema de gran actualidad y relevancia para la investigación criminal. Este campo nos desafía a adaptar nuestros métodos tradicionales al entorno digital, especialmente en lo que respecta al cibercrimen, con el objetivo de esclarecer la verdad y hacer justicia en nuevos contextos.

El propósito fundamental de este Congreso es fomentar el aprendizaje, el conocimiento y la creación de conexiones profesionales. Nos encontramos en un momento crucial, preparándonos para el futuro de la investigación criminal, un campo que demandará cada vez más excelencia de nuestra parte. Esta excelencia, sin duda, tendrá un impacto significativo en nuestra sociedad.

Los invito a participar activamente en este evento, que va más allá de ser un simple encuentro académico. Nuestro objetivo es que, al finalizar, todos nos vayamos con la satisfacción de haber ampliado nuestros conocimientos y perspectivas. Disfruten de las presentaciones, aprendan de ellas y establezcan nuevas relaciones profesionales Recuerden que un investigador eficaz no se limita a su oficina o grupo inmediato de trabajo, sino que forma parte de una comunidad con la que se relaciona.

Les doy nuevamente la bienvenida y les deseo una experiencia enriquecedora. Muchas gracias por su presencia y participación.

CONFERENCIAS

LA INVESTIGACIÓN CRIMINAL DIGITAL EN LA DEEP WEB COMO HERRAMIENTA DE CIBERPATRULLAJE

YEFRIN GARAVITO - Colombia

Ingeniero de Sistemas, con maestría en Criminología y Victimología, e Investigación Criminal de la Escuela de Posgrados de la Policía Nacional de Colombia. Perfilador criminal certificado por la ABPIAFC, criminalista con licencia del Consejo Superior de la Judicatura de Colombia. Cuenta con once años de experiencia como investigador y perito testigo en juzgados de circuito, especializados, tribunales superiores y ante la Corte Suprema de Justicia. Ha sido ponente internacional en el área de investigación criminal y ciencias forenses con instituci nes públicas, privadas y de policía judicial tanto en Colombia, Perú, Argentina, México y otros países, también se ha desempeñado como docente universitario.

La creciente relevancia del ciberespacio en las actividades delictivas ha llevado a la necesidad de desarrollar nuevas estrategias y herramientas de investigación criminal. En este contexto, el ciberpatrullaje y la investigación en la Deep Web emergen como elementos clave para la prevención y persecución de delitos informáticos.

El ciberpatrullaje se define como la actividad realizada por las fuerzas del orden para monitorear el ciberespacio en busca de actividades ilícitas. Esta práctica se ha vuelto fundamental debido a que gran parte de las amenazas identificadas por Interpol como prioritarias a nivel global tienen un componente cibernético. Entre estas amenazas destacan el lavado de dinero, el ransomware, el phishing, las estafas en línea, el fraude financiero, la explotación sexual de menores en línea y las intrusiones en sistemas informáticos.

La Deep Web, o internet profundo, juega un papel crucial en este escenario. A diferencia del internet superficial que conocemos cotidianamente, la Deep Web contiene información no indexada por los buscadores convencionales. Aunque no toda la información en la Deep Web es ilícita, su naturaleza no indexada la convierte en un espacio propicio para actividades delictivas. Más allá de la Deep Web se encuentra la Dark Web, que sí alberga en gran medida contenido ilegal y mercados negros digitales.

Para abordar estos desafíos, las autoridades han desarrollado marcos legales y técnicas especializadas. En Colombia, por ejemplo, el Centro Cibernético Policial tiene entre sus funciones realizar ciberpatrullajes las 24 horas del día, los 7 días de la semana. Esta actividad se fundamenta en diversas normativas, como el CONPES 3701 de 2011 que estableció los lineamientos de ciberseguridad y ciberdefensa para el país. La investigación criminal informática se basa en el análisis de fuentes de información tecnológica que pueden ser utilizadas en procesos judiciales.

Estas fuentes incluyen registros de llamadas, registros de conexión a internet, bases de datos y, de manera destacada, la inteligencia de fuentes abiertas (OSINT por sus siglas en inglés).

El OSINT se ha convertido en una herramienta fundamental para el ciberpatrullaje. Mediante el uso de software especializado, los investigadores pueden monitorear palabras clave en fuentes abiertas de internet para detectar posibles amenazas o actividades delictivas. Esta técnica permite, por ejemplo, prevenir riñas entre adolescentes al detectar convocatorias en redes sociales. Sin embargo, el uso de estas herramientas plantea desafíos éticos y legales. Es fundamental establecer límites claros para evitar vulnerar derechos fundamentales como la privacidad. El ciberpatrullaje debe entenderse como una actividad preventiva, similar a la presencia policial en las calles, y no como una recopilación indiscriminada de información personal.

Otro aspecto crucial es la distinción entre el agente encubierto virtual y el agente provocador. El agente encubierto tiene la tarea de infiltrarse en organizaciones criminales en línea, lo que puede implicar manejar material ilícito. Es esencial que estas operaciones se realicen dentro del marco legal y con los controles adecuados para evitar caer en prácticas de entrampamiento.

La eficacia del ciberpatrullaje es un tema de debate. Aunque se han reportado reducciones en los delitos informáticos, la magnitud del ciberespacio hace que los recursos actuales sean insuficientes. Se requiere una mayor inversión en personal especializado, capacitación y herramientas tecnológicas para hacer frente a la creciente sofisticación de los ciberdelincuentes.

Entre los retos que enfrenta el ciberpatrullaje se encuentra la necesidad mecanismos efectivos de colaboración entre diferentes países. Iniciativas como el Convenio de Budapest sobre Ciberdelincuencia proporcionan un marco para esta cooperación.

Además, los investigadores deben estar preparados para enfrentar los desafíos técnicos que presenta la Deep Web. Esto incluye el manejo de criptomonedas, el uso de redes anónimas como Tor, y la capacidad de navegar en foros y mercados ilegales en línea. También es fundamental desarrollar habilidades en análisis de metadatos y técnicas forenses digitales para extraer y validar evidencias.

La formación de los agentes de ciberpatrullaje debe ser integral. Además de conocimientos técnicos en informática y redes, es necesario que dominen idiomas extranjeros, ya que gran parte del contenido ilícito en la Deep Web no está en español. También deben tener una sólida formación legal para asegurar que sus actividades se mantengan dentro del marco jurídico.

En conclusión, el ciberpatrullaje y la investigación en la Deep Web se han convertido en herramientas indispensables para la lucha contra el cibercrimen. Sin embargo, su implementación efectiva requiere un delicado equilibrio entre la necesidad de seguridad y el respeto a los derechos fundamentales.

Es necesario continuar desarrollando marcos legales y éticos claros, invertir en formación y tecnología, y fomentar la cooperación internacional para hacer frente a los desafíos que plantea la delincuencia en el ciberespacio.

IDENTIFICACIÓN, OBTENCIÓN Y ANÁLISIS DE EVIDENCIAS EN LA DEEP WEB

SALVADOR SAMPER ALANA– España

Informático forense con amplia experiencia como analista para diferentes agencias a nivel internacional en el combate del ciber crimen. Miembro del *Center for Cybercrime Investigation and Cyber Security,* Center for Sciences CIC, Boston University of the United States of America. Fundador del *International Observatory of Computer Crime*, cofundador de "Escolta Digital" (primer protocolo europeo de protección digital dirigido a la defensa del Estado y activos relevantes). Actualmente se desempeña como presidente del Observatorio Español de Delitos Informáticos (OEDI), entidad referencial en el estudio, análisis y combate de los ciber delitos tanto a nivel nacional como internacional, contando, además, con la primera red de atención temprana a las víctimas en múltiples ciudades.

La ciberseguridad se enfrenta a desafíos cada vez más complejos en la era digital, especialmente en lo que respecta a la identificación, obtención y análisis de evidencias en la Deep Web. Las actividades ilícitas en internet representan un problema global que requiere un enfoque multidisciplinar y una cooperación internacional sin precedentes.

El panorama actual de la ciberdelincuencia se caracteriza por la persistencia y sofisticación de los mercados ilegales en línea. Estos operan las 24 horas del día, los siete días de la semana, utilizando criptomonedas para sus transacciones, lo que dificulta su rastreo y persecución. Los principales ámbitos de actividad criminal en el ciberespacio incluyen la venta de drogas, armas y datos robados; el fraude y robo de identidad; la pornografía infantil; los ciberataques y servicios de hacking; y la contratación de diversos servicios ilegales.

Para comprender la magnitud del problema, es crucial reconocer que internet no es un espacio homogéneo, sino que se compone de distintos estratos. Más allá del Internet superficial de uso cotidiano, existe la Deep Web, que alberga información no indexada que requiere accesos específicos, y la Dark Web, donde se concentra gran parte de la actividad ilícita a través de redes cifradas.

El crecimiento exponencial de la economía criminal en internet entre 2015 y 2020 ha sido alarmante. Plataformas como Hydra Market han demostrado la capacidad de las organizaciones criminales para desarrollar sofisticados sistemas de reputación y confianza, emulando modelos de negocio legítimos en entornos digitales opacos.

Las redes criminales han aprovechado las tecnologías de la información y comunicación para promocionar sus actividades, reclutar nuevos miembros y comunicarse con clientes potenciales. Esta adaptación les ha permitido consolidar su poder y aumentar sus ingresos ilícitos de manera significativa.

Frente a esta realidad, se hace evidente la necesidad de un enfoque integral y colaborativo en la lucha contra el cibercrimen. Una estrategia efectiva debe basarse en varios pilares fundamentales:

1. Investigación rigurosa de las estructuras y actividades criminales en el ciberespacio.

2. Coordinación efectiva entre agencias y organizaciones internacionales para compartir información y recursos.

3. Desarrollo y uso de tecnología avanzada para la recopilación y análisis de evidencias digitales.

4. Implementación de acciones estratégicas proactivas que se anticipen a las tácticas criminales.

5. Programas de prevención y sensibilización ciudadana sobre los riesgos en línea.

Los avances en herramientas forenses digitales, como sistemas capaces de obtener y analizar evidencias de diversas plataformas como Telegram, WhatsApp o TikTok, son cruciales en esta lucha. Sin embargo, también plantean desafíos en términos de privacidad y derechos digitales que deben ser cuidadosamente considerados.

La regulación efectiva de las redes sociales y la Deep Web enfrenta numerosos obstáculos legales y técnicos. La persecución de delitos transnacionales se complica debido a la volatilidad de las evidencias digitales, las dificultades de cooperación internacional y el rápido avance tecnológico que constantemente supera los marcos legales existentes.

Es imperativo fomentar la colaboración entre especialistas técnicos y jurídicos para desarrollar marcos regulatorios efectivos y adaptables. Asimismo, es necesario anticipar y abordar el impacto de tecnologías emergentes como la inteligencia artificial, no solo en el ámbito de la ciberseguridad, sino en diversos aspectos sociales y económicos.

El ecosistema digital contemporáneo difumina las fronteras entre lo legal y lo ilegal, planteando dilemas significativos en términos de privacidad y libertad de información.

La *Deep Web* y la *Dark Web*, si bien ofrecenoportunidades para actividades criminales, también suscitan debates importantes sobre el equilibrio entre seguridad y derechos individuales en la era digital.

La dimensión económica del cibercrimen merece especial atención. Las organizaciones criminales han demostrado una notable capacidad para adaptar modelos de negocio tradicionales al entorno digital. Este fenómeno subraya la necesidad de enfoques que trasciendan la mera persecución penal, abordando también los incentivos económicos que sustentan estas actividades ilícitas.

Los avances en capacidades forenses digitales son notables, pero también evidencian una constante carrera tecnológica entre las fuerzas del orden y los grupos criminales. Este escenario plantea el desafío de mantener un equilibrio entre la innovación en ciberseguridad y la protección de derechos fundamentales como la intimidad.

Los desafíos regulatorios y el impacto de tecnologías emergentes como la inteligencia artificial abren importantes líneas de debate en el campo de la ciberseguridad. Se hace patente la necesidad de desarrollar marcos normativos flexibles y adaptables, capaces de responder a un panorama tecnológico en rápida evolución. Asimismo, es crucial considerar las implicaciones éticas y sociales más amplias de estas tecnologías, más allá de su mera aplicación en el ámbito de la seguridad.

En conclusión, el panorama actual de la ciberseguridad presenta retos complejos que requieren un enfoque multidimensional. La lucha contra el cibercrimen debe abarcar aspectos técnicos, legales, económicos y sociales para ser efectiva. Al mismo tiempo, es fundamental mantener una reflexión continua sobre el papel de la tecnología en la sociedad contemporánea y la necesidad de enfoques éticos y responsables en su desarrollo y aplicación. Solo a través de una comprensión profunda de estos desafíos y una colaboración internacional sostenida podremos aspirar a un ciberespacio más seguro y equitativo para todos.

LA DEEP WEB Y LA DARK WEB: RIESGOS, CONTENIDOS Y ACCESO

JOHN ROBERT CORREA - Colombia

Profesional en electrónica. Master universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones. Doctor en Sistemas de Información y Doctor en Filosofía de la Universidad de las Américas y del Caribe en México. Con amplia experiencia en seguridad de la información y las comunicaciones e implementación de modelos estratégicos de cibers guridad de la información. Se ha desempeñado como perito ciberjudicial e investigador digital forense.

En el ámbito de la ciberseguridad, la comprensión de la *Deep Web* y de *Dark Web* es fundamental para profesionales y usuarios conscientes de la seguridad digital.

La *Dark Web*, un subconjunto de la *Deep Web,* es accesible únicamente mediante software especializado, siendo TOR (The Onion Router) el más conocido. TOR se define como una red de servidores que facilita el acceso a sitios ocultos dentro de la *Deep Web* y la *Dark Web*. Es importante destacar que, si bien TOR se asocia comúnmente con actividades ilícitas, también es una herramienta valiosa para periodistas, expertos en inteligencia civil y otros profesionales que requieren realizar investigaciones sensibles o acceder a información protegida.

Un concepto clave en la estructura de estas redes es el "nodo", definido como un punto de conexión que permite la interacción con otros espacios en el ciberespacio. En el contexto de TOR, los nodos forman una malla compleja que facilita la navegación anónima, característica esencial de estas redes ocultas.

La configuración de un entorno seguro para navegar en la *Deep Web* utilizando TOR implica varios pasos técnicos:

1. Actualización del sistema operativo (preferiblemente Linux).

2. Instalación de librerías y herramientas específicas (Terminator, TOR, NYX, CURL).

3. Configuración de Python y scripts necesarios.

4. Inicio y verificación de los servicios TOR.

Es crucial el uso de un proxy reverso (NYX) para ocultar la IP real del usuario y asignar una IP de la *Deep Web*. Adicionalmente, la herramienta Torsocks convierte la IP en una dirección oculta, dificultando su rastreo desde la internet superficial.

Un experimento de captura de tráfico en la *Deep Web*, realizado durante solo 20 minutos, reveló datos sorprendentes:

- Se capturaron 11,625 direcciones IP de la red oscura.

- Se identificaron nodos externos y nodos “full”.

- Se analizaron puertos, banderas activas y versiones de TOR utilizadas.

- Se detectaron direcciones IP tanto en formato IPv4 como IPv6.

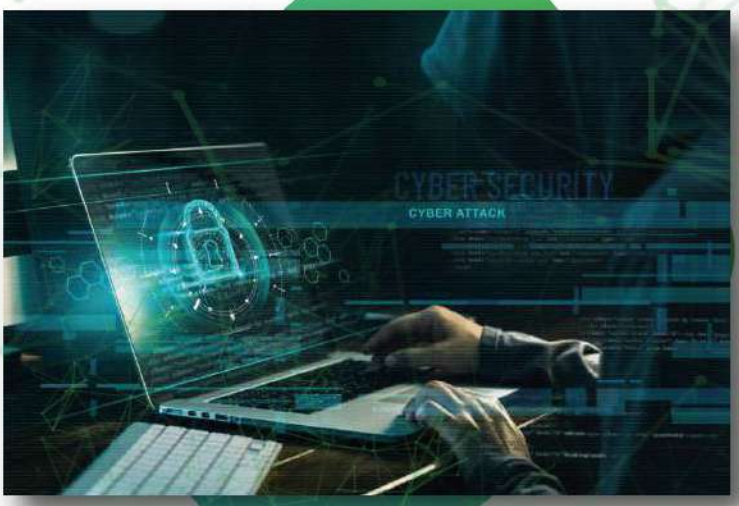
Este experimento demostró la inmensa cantidad de información que circula en estas redes, con una captura de aproximadamente 280 GB de datos en ese breve período.
Los riesgos asociados con la exposición de información personal en internet, tanto en la superficie como en las capas profundas, son numerosos y significativos:

1. El uso indiscriminado de redes sociales y la publicación excesiva de información personal.

2. Las vulnerabilidades inherentes a los dispositivos IoT (Internet of Things).

3. La captura y análisis de metadatos por parte de terceros.

4. La suplantación de identidad y diversas amenazas cibernéticas



La mayoría de los usuarios no son plenamente conscientes de cómo su información es recopilada y utilizada, lo que aumenta su vulnerabilidad tanto en la Internet superficial como en la Deep Web. En el contexto de la investigación en la Dark Web, las técnicas de OSINT (Open Source Intelligence) juegan un papel crucial. Se destaca una herramienta denominada “preforman OSINT”; como una de las más potentes disponibles en TOR para realizar búsquedas avanzadas y análisis de información. Sin embargo, para evitar vulnerar la privacidad de las personas y mantener la integridad profesional es importante utilizar las metodologías adecuadas y respetar los marcos legales al

realizar investigaciones en fuentes abiertas y cerradas .

Las métricas presentadas sobre el uso de la Deep Web son alarmantes:

- Más de 100,000 conexiones a nivel de navegador en 20 minutos

- 20 GB de tráfico para descargar datos en el mismo período

- 8,000 servidores activos entregando información constantemente

- Más de 7,500,000 usuarios conectados

Estas cifras ilustran la magnitud y el alcance de las actividades en la Deep Web, resaltando la necesidad imperiosa de una mayor conciencia y seguridad en el uso de internet.
Ante estos desafíos, se proponen varias recomendaciones:

1. Ejercer cautela al publicar información en redes sociales.

2. Utilizar filtros y configuraciones de seguridad robustas al navegar en la Deep Web.

3. Emplear máquinas virtuales y capas adicionales de seguridad para investigaciones en la Dark Web.

4. Desarrollar y fomentar una cultura de protección de datos personales.

5. Verificar meticulosamente los términos y condiciones de las plataformas en línea antes de utilizarlas.

Es fundamental reconocer que, si bien la Deep Web y la Dark Web presentan riesgos significativos, también son herramientas valiosas para la investigación y el periodismo cuando se utilizan de manera responsable y ética. La comunidad de ciberseguridad debe mantenerse en constante actualización y desarrollar estrategias cada vez más efectivas para proteger la información en un panorama digital en constante evolución.

En conclusión, la comprensión y el manejo adecuado de la Deep Web y la Dark Web son cruciales en la era digital actual. Estos espacios ocultos de internet representan tanto oportunidades como amenazas, y su navegación requiere conocimientos técnicos avanzados y una aguda conciencia de los riesgos involucrados. La educación continua, la implementación de medidas de seguridad robustas y el uso ético de estas tecnologías son fundamentales para aprovechar su potencial mientras se mitigan los peligros asociados. A medida que la tecnología evoluciona, también lo hacen las técnicas de los ciberdelincuentes, por lo que la vigilancia y la adaptación constantes son imperativas en el campo de la ciberseguridad.

VALIDEZ PROBATORIA DE LA EVIDENCIA DIGITAL Y APLICABILIDAD DEL CONVENIO DE BUDAPEST CONTRA LA CIBERCRIMINALIDAD

DAVID CARDONA – Colombia

Presidente en *The International Asociation Identification IAI* división Colombia, en el subcomité de informática forense. Se ha desempeñado como conferencista internacional en temas de derecho de la ciberseguridad y entornos digitales, y en derecho internacional humanitario.

Docente universitario en pregrado y posgrado en la Universidad Autónoma de México, Universidad Vizcaya de las Américas de México, Ministerio del Interior del Perú, Universidad Los Libertadores, Universidad de Manizales, entre otras. Exdetective de la República, exfuncionario de la Fiscalía General de la Nación de Colombia y el Departamento Administrativo de Seguridad, donde elaboró por más de 16 años.

El avance acelerado de la era digital, impulsado por la pandemia, ha planteado nuevos desafíos en el ámbito de la ciberseguridad y el derecho digital. En este contexto, la validez probatoria de la evidencia digital, la aplicabilidad del Convenio de Budapest contra la cibercriminalidad y las implicaciones legales de las nuevas tecnologías son temas cruciales.

En primer lugar, es importante distinguir entre evidencia digital y dispositivos electrónicos. La evidencia digital se define como la información y los datos almacenados en medios digitales, no los dispositivos en sí mismos. Esta distinción es fundamental para la correcta valoración de la evidencia en procesos judiciales.

El Convenio de Budapest, al cual Colombia adhirió en 2020, ha ampliado la definición de

delitos informáticos, incluyendo no solo aquellos que atentan contra la tecnología, sino también los que utilizan la tecnología como medio para cometer otros delitos. Esto ha permitido abordar de manera más efectiva problemas como la pornografía infantil y ha establecido la responsabilidad penal de las personas jurídicas en delitos informáticos.

Es muy difícil garantizar la autoría en la evidencia digital; es prácticamente imposible establecer más allá de toda duda razonable que una persona específica envió un mensaje o realizó una acción en línea, debido a la facilidad de suplantación y manipulación de datos digitales. Esto plantea desafíos significativos para la investigación y el procesamiento de delitos cibernéticos.

La extraterritorialidad plantea retos para la recolección de evidencia digital. Con la información almacenada en servidores ubicados en diferentes países, surge la necesidad de cooperación internacional y la aplicación de tratados como el Convenio de Budapest para acceder y utilizar legalmente esta evidencia en procesos judiciales.

La informática forense y el papel de los peritos en este campo son cruciales para validar la evidencia digital ante los tribunales. Los principios fundamentales de la evidencia digital son: autenticidad, integridad y disponibilidad futura. La autenticidad se refiere a garantizar que la evidencia proviene del lugar que se afirma, la integridad asegura que no ha sido alterada, y la disponibilidad futura permite su acceso posterior.

La Ley 527 de 1999 en Colombia, que regula el comercio electrónico y la admisibilidad de la evidencia digital, ha tenido aplicaciones inadecuadas y es obsoleta porque no aborda adecuadamente las realidades tecnológicas actuales; por lo tanto, puede llevar a decisiones judiciales problemáticas.

Es necesario tener una legislación más prospectiva en lugar de reactiva en el ámbito del derecho digital. Por ejemplo, el artículo 18.4 de la Constitución Española de 1978, preveía la necesidad de regular el uso de la informática para proteger derechos fundamentales, mucho antes de la era de Internet.

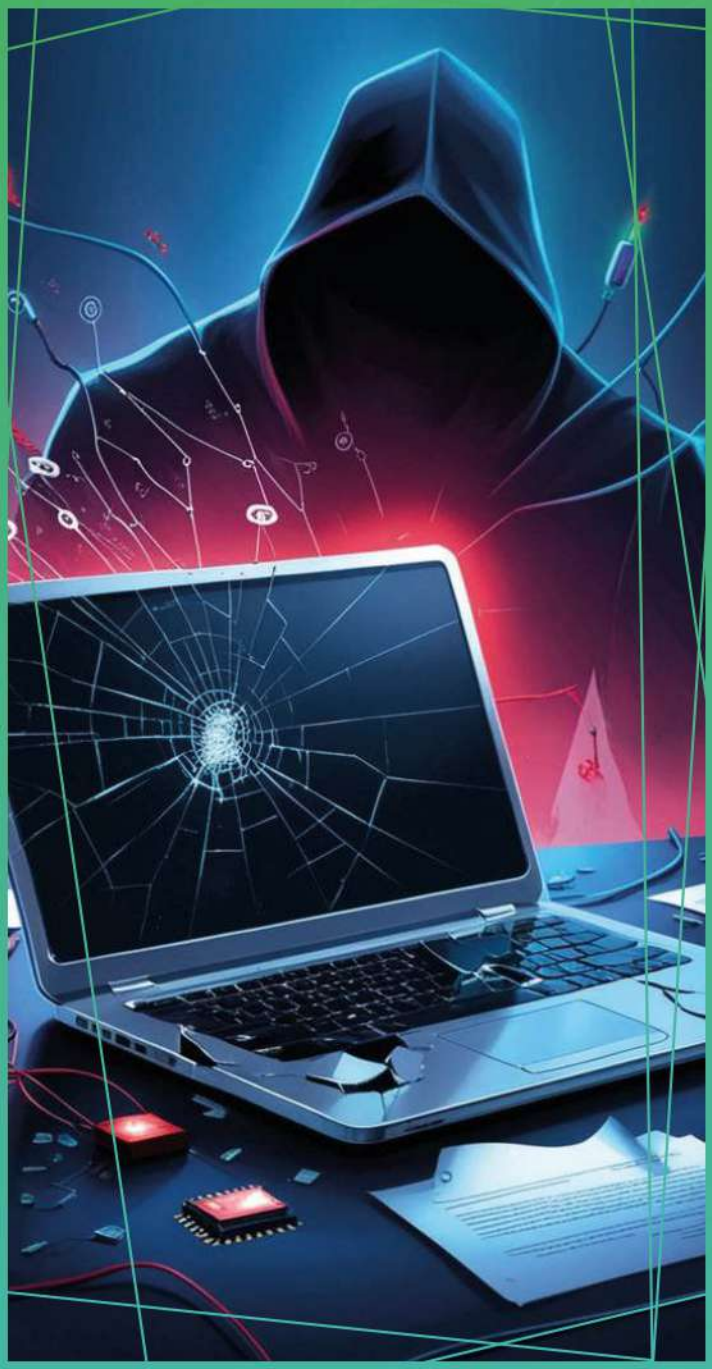
En cuanto a las implicaciones legales de la inteligencia artificial, se requiere una regulación para establecer la responsabilidad penal de los sistemas de IA. El Libro Blanco de la Inteligencia Artificial de la Unión Europea es un punto de referencia ético, aunque no vinculante para países fuera de la UE.

Los derechos fundamentales digitales (como el derecho a la desconexión digital y el derecho a la protección de datos personales) deben ser garantizados y protegidos, pues su violación puede tener consecuencias graves, incluso afectando derechos fundamentales como la salud y la vida.

El derecho digital es de naturaleza digital y, por lo tanto, se requiere una regulación internacional coherente. En esta vía, el Convenio de Budapest, que está en su tercer protocolo adicional, busca establecer procedimientos a nivel mundial para abordar los desafíos del cibercrimen y la evidencia digital.

En resumen, ante los desafíos actuales en el campo de la ciberseguridad y el derecho digital, es necesario actualizar la legislación, mejorar la cooperación internacional y desarrollar nuevas habilidades en el sistema judicial para abordar eficazmente los delitos cibernéticos. Para todo ello es importante y necesario desarrollar la informática forense y lograr una comprensión más profunda de las tecnologías digitales en el ámbito legal. El derecho en la era digital debe incluir la regulación de la inteligencia artificial, la protección de derechos fundamentales digitales, y la adaptación del sistema judicial a las nuevas realidades tecnológicas. El futuro ya está aquí y el derecho debe evolucionar rápidamente para mantenerse al día con los avances tecnológicos.

Los profesionales del derecho, los legisladores y los expertos en tecnología tienen el reto de trabajar conjuntamente para desarrollar marcos legales y procedimientos que puedan abordar eficazmente los desafíos de la era digital. El derecho digital es un campo en rápida evolución que requiere una atención continua y una adaptación constante para garantizar la justicia y la seguridad en el mundo digital.



DESAFÍOS Y EVOLUCIÓN DE LA INFORMÁTICA FORENSE EN LA ERA DE LA WEB PROFUNDA

RICARDO RODRÍGUEZ - México

Licenciado en Informática por el Instituto Nacional de México, campus Tepic, posgrado en Criminología con énfasis en delitos informáticos, especialidad en Grafoscopía y Documentoscopía Forense, diplomados en Ciudad Segura, Ciberseguridad, Ciber criminología, Informática Forense, (ISC)2, *Autopsy, Ethical Hacking Foundation*, Ciberinteligencia con herramientas OSINT, Certificación CSFPC (*Cibersecurity Foundation*) y Certificación en *Protection Level Expert Cybercriminologist*. Formación en docente, en evaluación y desempeño basado en modelos de educación por competencias, en procesos de formación de auditor en riesgo de Ciberseguridad Empresarial, por CIC de la Universidad de Boston. Cuenta con experiencia profesional en el sector público de los tres órdenes de gobierno de su país, ha sido testigo experto en el poder judicial de la federación de la materia pericial de informática forense, cibercriminalidad y cibercriminología desde el año 2017, director general de la Consultoría THEOSMX.

La informática forense es una disciplina crucial en la investigación y análisis de datos almacenados en medios electrónicos y digitales. Su objetivo principal es identificar, preservar, recuperar, analizar y presentar datos válidos en procesos legales. Este campo enfrenta constantes desafíos debido a la rápida evolución tecnológica y la creciente complejidad de los delitos cibernéticos.

Un aspecto fundamental de la informática forense es la preservación de la evidencia digital. Este proceso implica asegurar los elementos digitales desde su punto de origen, manteniendo una cadena de custodia rigurosa hasta su análisis. La metodología empleada debe ser sistemática y reproducible, garantizando que diferentes herramientas aplicadas al mismo conjunto de datos produzcan resultados idénticos.

El perito en informática forense se enfrenta a retos cada vez más complejos. La evolución tecnológica ha llevado a la creación de dispositivos más sofisticados y formas de almacenamiento más diversas, desde equipos físicos hasta servicios en la nube. Además, la aparición de tecnologías como

la inteligencia artificial y el Internet de las Cosas presenta nuevos desafíos para la recopilación y análisis de evidencia digital.

La estructura de Internet también plantea desafíos significativos. Más allá de la web superficial, accesible a través de motores de búsqueda convencionales, existen la *Deep Web* y la *Dark Web*. *La Deep Web* contiene información no indexada que requiere autenticación para su acceso, como bases de datos académicas, gubernamentales y corporativas. Por otro lado, la *Dark Web* es un espacio más restringido, accesible solo mediante navegadores específicos y frecuentemente asociado con actividades ilícitas.

En el contexto de la *Dark Web*, los investigadores forenses deben enfrentarse a una serie de herramientas y técnicas diseñadas para garantizar el anonimato y dificultar el rastreo. Estas incluyen sistemas operativos especializados, navegadores cifrados, servicios de VPN, correos electrónicos desechables y generadores de identidades falsas. Estas herramientas, aunque pueden tener usos legítimos, también facilitan actividades ilegales como la venta de drogas, armas y datos personales robados.

Los retos de la informática forense en la *Deep Web* y la *Dark Web* son múltiples. En primer lugar, las herramientas disponibles para la investigación forense pueden ser costosas y requerir licencias específicas. Además, el volumen de datos para analizar es a menudo abrumador, lo que demanda software y hardware capaces de procesar grandes cantidades de información en tiempos limitados.

La ética juega un papel crucial en la informática forense. Los profesionales en este campo deben mantener altos estándares éticos para garantizar la imparcialidad y confiabilidad de sus análisis. Esto es particularmente importante dado el carácter sensible de la información manejada y las posibles consecuencias legales de sus hallazgos.

Un aspecto importante para considerar es la naturaleza cambiante de la *Dark Web*. Los sitios en este espacio son efímeros, aparecen y desaparecen rápidamente. Esto dificulta la tarea de los investigadores, que deben adaptarse constantemente a un entorno en evolución. Además, la *Dark Web* ofrece ventajas como la libre expresión y el activismo político en regiones con restricciones de libertad de expresión, lo que añade complejidad ética a la labor de los investigadores forenses.

Para enfrentar estos desafíos, se han desarrollado herramientas especializadas. Una de ellas es *ONION SCAN*, una herramienta de código abierto diseñada para analizar la red *TOR (The Onion Router*). Esta herramienta ha permitido investigar la estructura y funcionamiento de la red *TOR,* proporcionando información valiosa sobre la duración de los servidores, los enlaces entre nodos y otros aspectos técnicos.

Otra técnica relevante es el *Ataque Entry Guard*, que busca identificar y analizar los nodos de entrada en la red *TOR*. Este método intenta superar las capas de cifrado que caracterizan a la red *TOR*, aunque su efectividad está limitada por la naturaleza dinámica y aleatoria de las conexiones en esta red.

El futuro de la informática forense apunta hacia la integración de tecnologías cognitivas y predictivas. Estas tecnologías permitirán desarrollar sistemas de inteligencia avanzada capaces de tomar decisiones y establecer controles más efectivos. La implementación de *firewalls* inteligentes y sistemas de detección de amenazas basados en inteligencia artificial será crucial para mejorar la capacidad de respuesta ante nuevas formas de ciberdelincuencia.

Finalmente, las herramientas de Inteligencia de Fuentes Abiertas (OSINT) están ganando relevancia en la informática forense. Estas herramientas permiten recopilar y analizar información disponible públicamente en internet, lo que puede ser valioso para investigaciones en la *Deep Web* y la *Dark Web*.

En conclusión, la informática forense se enfrenta a desafíos significativos en un entorno digital en constante evolución. La combinación de herramientas avanzadas, metodologías rigurosas y un fuerte compromiso ético es esencial para que los profesionales en este campo puedan enfrentar eficazmente las amenazas cibernéticas actuales y futuras. La continua investigación y desarrollo de nuevas técnicas y tecnologías será crucial para mantener la eficacia de la informática forense en la lucha contra el cibercrimen.

HERRAMIENTAS FORENSES EN INVESTIGACIONES EN DEEP WEB

SANTIAGO VILLAMIL ODDONE - Argentina

Abogado con MBA en Administración y Gestión de Empresas. Se ha desempeñado como abogado y asesor jurídico en diferentes estudios jurídicos de su país. Fue docente del curso de Especialización en Cibercrimen y Ciberseguridad en la Policía Nacional del Ecuador, director de Escritorio Español en China, encargado de Derecho Corporativo, Derecho Laboral, Propiedad Intelectual, Arbitraje e Impuestos. Se desempeña como *CEO MOBILedit Forensic Express* donde se ofrecen herramientas forenses todo en uno, (extracción de información de celular y cloud, análisis de datos y generador de reportes en una sola solución, adquisición lógica y física de datos, análisis avanzado de aplicaciones, recuperación de datos eliminados, actualizaciones en línea, compatibilidad con la mayoría de los dispositivos y extracciones concurrentes e interfaz sencilla de utilizar). Lo más relevante de la compañía es que desarrolla softwares especializados en investigación del contenido de teléfonos móviles.

Los relojes inteligentes son dispositivos que tienen una creciente importancia como fuente de evidencia digital en investigaciones criminales.

Los relojes inteligentes se han convertido en los dispositivos portátiles más populares, con un mercado en rápido crecimiento. Se proyecta que las ventas alcanzarán los 130.000 millones de dólares para 2030. Estos dispositivos contienen información única y valiosa, incluyendo datos biométricos, patrones de sueño, ubicaciones detalladas y actividad física del usuario. Su naturaleza personal y el uso constante los convierten en fuentes potenciales de evidencia que pueden no estar disponibles en otros dispositivos.

La herramienta *MOBILedit Forensic*, desarrollada por la empresa *Compelson* para la extracción y análisis de datos de relojes inteligentes, es utilizada por organismos de seguridad y defensa a nivel internacional, incluyendo el FBI, Interpol y Europol. Su capacidad de extracción de datos varía según las marcas de los relojes inteligentes:

1. Samsung Galaxy Watch: permite extraer contactos, llamadas, imágenes, audios, documentos, aplicaciones y notificaciones, incluyendo algunos datos borrados.

2. Garmin: ofrece extracción sin necesidad de código de acceso, incluyendo perfiles de usuario, actividades físicas detalladas, rutas GPS y datos biométricos.

3. Apple Watch: permite extraer información del dispositivo, lista de aplicaciones, fotos con ubicaciones, grabaciones de voz y notas.

4. Otros modelos como Alcatel, TCL, Huawei, Amazfit y Suunto también son compatibles con la herramienta.

La importancia de considerar los relojes inteligentes como fuentes potenciales de evidencia en investigaciones criminales radica en que estos dispositivos pueden contener información crucial que no se encuentra en teléfonos móviles, especialmente en casos donde el teléfono ha sido destruido o no está disponible.

Los siguientes son ejemplos de casos de estudio que ilustran la relevancia de los datos extraídos de relojes inteligentes en investigaciones criminales:

1. Un asesino a sueldo utilizaba una aplicación encriptada en su teléfono, pero las notificaciones quedaron registradas en su reloj inteligente, proporcionando evidencia crucial.

2. En un caso de homicidio, los datos de ubicación de un reloj inteligente ayudaron a exonerar a una sospechosa.

3. En un caso de robo donde los ladrones utilizaron un Apple Watch como dispositivo de rastreo GPS para localizar a su objetivo.

4. Un caso de pornografía infantil descubierto a través de imágenes almacenadas en un Apple Watch.

5. Un homicidio donde los mensajes recuperados del reloj inteligente de la víctima proporcionaron evidencia crucial para la condena del perpetrador.

Es importante tener presente los aspectos legales y procedimentales de la recolección de evidencia digital. Un código de práctica criminal de Inglaterra establece que los investigadores deben seguir imparcialmente todas las líneas de indagación razonables, tanto a favor como en contra del sospechoso. Esto implica la necesidad de recolectar y analizar toda la evidencia disponible, incluyendo la proveniente de relojes inteligentes.

Para abordar eficazmente los delitos cibernéticos que a menudo trascienden fronteras, se requiere cooperación entre diferentes organismos de seguridad, tanto a nivel nacional como internacional.

Es necesario que los investigadores forenses estén preparados para analizar datos de relojes inteligentes. Para ello es recomendable adquirir herramientas especializadas como *MOBILedit Forensic* y kits de conexión para diferentes modelos de relojes inteligentes.

En resumen, los relojes inteligentes tienen un papel cada vez más significativo en las investigaciones forenses digitales, especialmente en las relacionadas con delitos vinculados a la *Deep Web* y *Dark Web*. Es importante estar al día con las nuevas tecnologías y herramientas forenses para enfrentar los desafíos de la ciberdelincuencia moderna. La creciente adopción de relojes inteligentes y su capacidad para almacenar datos personales detallados los convierten en fuentes de evidencia cada vez más relevantes en investigaciones criminales.

Las investigaciones digitales deben tener un enfoque holístico, considerando todos los dispositivos electrónicos potencialmente relevantes.

Los relojes inteligentes, a menudo pasados por alto, pueden proporcionar información crucial que complemente o incluso supere la evidencia obtenida de teléfonos móviles y computadoras.

Por todo esto, para los profesionales de la seguridad cibernética y la informática forense es de suma importancia la formación continua y la actualización de conocimientos. A medida que la tecnología evoluciona rápidamente, es crucial que los investigadores se mantengan al tanto de las nuevas fuentes de evidencia digital y las herramientas disponibles para su análisis.

HERRAMIENTAS DE PREVENCIÓN Y MITIGACIÓN DE LOS CIBERDELITOS Y AMENAZAS AL ESTADO EN LA WEB

WALTER ALEJANDRO LINARES GUERRA - Colombia

Mayor de la Policía Nacional de Colombia con once años de experiencia en tecnologías de la información en la Administración Policial. Especialista en Gerencia en Telemática, Magister en Ciberseguridad e Informática Forense. Docente universitario en temas relacionados con ciberseguridad y seguridad de la información. Actualmente se desempeña como jefe del centro de respuesta a incidentes informáticos de la Presidencia de la República.

El cibercrimen y la ciberseguridad son temas de creciente relevancia en la actualidad. Con el aumento del uso de tecnologías digitales, los ciberdelitos se han incrementado significativamente, representando una amenaza para individuos, organizaciones y gobiernos. Se examinarán las principales modalidades de ciberataques, así como las herramientas y buenas prácticas para prevenirlos y mitigarlos.

Entre los ciberdelitos más comunes se encuentran el phishing, el smishing, el vishing y el ransomware. El phishing consiste en el envío de correos electrónicos fraudulentos que suplantan la identidad de entidades legítimas para obtener información confidencial. El smishing utiliza mensajes de texto SMS con el mismo propósito. El vishing implica llamadas telefónicas fraudulentas para engañar a las víctimas. El ransomware es un tipo de malware que cifra los archivos del usuario y exige un rescate para recuperarlos.

La ingeniería social juega un papel crucial en estos ataques. Los ciberdelincuentes estudian a sus objetivos a través de la información que comparten en redes sociales y otros medios digitales. Con estos datos, elaboran mensajes y llamadas personalizados que resultan más convincentes. Por ello, es fundamental ser cauteloso con la información que se publica en línea y verificar la autenticidad de cualquier comunicación sospechosa. Para protegerse de estos ataques, existen diversas herramientas y prácticas recomendadas:

1. Uso de contraseñas robustas: se aconseja utilizar contraseñas largas (mínimo 8 caracteres), alfanuméricas y únicas para cada servicio. Evitar contraseñas obvias basadas en información personal.

2. Autenticación de doble factor: activar esta función en todas las cuentas que lo permitan, especialmente en correo electrónico y redes sociales. Añade una capa extra de seguridad.
3. Actualizaciones de software: mantener el sistema operativo y todas las aplicaciones actualizadas para corregir vulnerabilidades conocidas.
4. Copias de seguridad: realizar periódicamente copias de seguridad de la información importante en dispositivos externos o en la nube.
5. Cifrado de dispositivos: utilizar herramientas como *BitLocker* para cifrar discos duros y memorias USB con información sensible.
6. Precaución en redes públicas: evitar acceder a cuentas bancarias o información confidencial cuando se utilizan redes Wi-Fi públicas.
7. Educación y concienciación: mantenerse informado sobre las últimas amenazas y técnicas de ingeniería social.

Es importante destacar que los ciberataques no solo afectan a individuos, sino que pueden tener consecuencias graves para organizaciones y gobiernos. Un ejemplo reciente es el ataque ransomware a la empresa IFX en Colombia, que afectó a 22 entidades estatales, incluyendo el Ministerio de Salud y la rama judicial. Este incidente resalta la importancia de implementar medidas de ciberseguridad robustas en infraestructuras críticas.

Otro aspecto preocupante es el aumento de delitos relacionados con la explotación sexual de menores en línea. El *grooming*, donde adultos se hacen pasar por menores para ganar la confianza de niños y adolescentes con fines sexuales, es una práctica cada vez más común. Es crucial que padres y educadores estén atentos a estas amenazas y eduquen a los menores sobre los riesgos en línea.

Para combatir estos delitos, existen canales oficiales de denuncia como el CAI virtual de la Policía Nacional, la página web de la Fiscalía para denuncias de delitos informáticos, y la línea 141 del Instituto Colombiano de Bienestar Familiar para casos de explotación sexual de menores.

En conclusión, la ciberseguridad es una responsabilidad compartida entre individuos, organizaciones y gobiernos. La implementación de buenas prácticas y el uso de herramientas de seguridad pueden reducir significativamente el riesgo de ser víctima de ciberataques. Sin embargo, es igualmente importante mantenerse informado y alerta, ya que las técnicas de los ciberdelincuentes evolucionan constantemente.

La educación y la concienciación son fundamentales para crear una cultura de ciberseguridad. Esto implica no solo conocer las amenazas y cómo protegerse, sino también entender el valor de la información personal y ser responsable en su manejo. Las organizaciones deben invertir en la formación de sus empleados y en la implementación de políticas de seguridad robustas.
Asimismo, es necesario un enfoque proactivo en la protección de infraestructuras críticas y servicios esenciales. Los gobiernos deben trabajar en estrecha colaboración con el sector privado para desarrollar estrategias de ciberseguridad nacionales y fortalecer la resiliencia ante ataques cibernéticos a gran escala.

A medida que avanzamos hacia un mundo cada vez más digitalizado, la importancia de la ciberseguridad seguirá creciendo. Es esencial que tanto individuos como organizaciones se adapten a este nuevo panorama de amenazas y adopten una mentalidad de seguridad en todas sus interacciones digitales. Solo a través de un esfuerzo colectivo y continuo podremos crear un ciberespacio más seguro para todos.

DELITOS CIBERNÉTICOS Y CIBERDELINCUENCIA EN LA DEEP WEB, UN ESCENARIO DE RETOS LÓGICOS EN MATERIA DE INVESTIGACIÓN

ALDAIR JOSÉ BUENO - Colombia

Abogado especialista en derecho penal, crimen organizado, corrupción y terrorismo de la universidad de Salamanca España, Magister en Derechos Humanos y Derecho Internacional de los Conflictos Armados de la Escuela Superior de Guerra. Cuenta con experiencia en el estudio, análisis, defensa y asesoría en los delitos informáticos; es asesor empresarial en planes de cumplimiento para la exoneración de la responsabilidad de la persona jurídica en materia de cibercriminalidad. Profesor universitario en el ámbito nacional e internacional, investigador en ciberconflictos armados, conductas que afectan a la comunidad respecto de sus derechos fundamentales digitales. Analista de conductas ciberterroristas, neuroderechos e inteligencias artificiales. Exasesor jurídico del Ejercito Nacional de Colombia, asesor de la Alta Consejería para la Paz y el Postconflicto, actual CEO del Instituto Iberoamericano de Derecho Digital y de la Ciberseguridad, desarrollador de movimientos académicos de cibercultura.

El ciberespacio se ha convertido en un escenario complejo que plantea numerosos desafíos en materia de seguridad y regulación. La sociedad actual se caracteriza por una hiperdigitalización creciente, donde las interacciones y transacciones en línea son cada vez más frecuentes y sofisticadas. En este contexto, es fundamental comprender la estructura y dinámica de Internet, así como las amenazas y riesgos asociados.

Internet puede dividirse en tres niveles principales: la *surface web* o web superficial, la deep web o web profunda, y la *dark web* o web oscura. La *surface web* es la parte visible y accesible a través de motores de búsqueda convencionales, donde se desarrollan la mayoría de las actividades cotidianas en línea. La *deep web*, por su parte, contiene información no indexada y requiere autenticación para acceder, siendo utilizada por universidades, gobiernos y otras instituciones para almacenar datos sensibles. Finalmente, la *dark web* es un espacio altamente encriptado y anónimo donde proliferan actividades ilícitas.

La ciberdelincuencia aprovecha las características de anonimato y encriptación de la *deep web* y la *dark web* para llevar a cabo sus operaciones. Esto plantea serios retos para la investigación y persecución de delitos cibernéticos, ya que resulta difícil rastrear el origen de los ataques e identificar a los responsables. Además, la naturaleza transnacional de Internet complica aún más la labor de las autoridades, al involucrar múltiples jurisdicciones.

Entre los casos más notorios de ciberdelincuencia destacan *Silk Road*, un mercado negro en línea desmantelado en 2013, y las operaciones *Pacifier* y *AlphaBay-Hansa*, enfocadas en combatir redes de pornografía infantil y narcotráfico respectivamente. Estos ejemplos ilustran la complejidad y alcance global de las actividades delictivas en el ciberespacio, así como la necesidad de cooperación internacional para hacerles frente. Un fenómeno emergente que genera preocupación es el uso malicioso de la inteligencia artificial (IA) con fines delictivos. Se han documentado casos de manipulación de imágenes mediante IA para crear contenido sexual no consentido, lo que plantea nuevos dilemas éticos y legales. La legislación actual en muchos países no contempla adecuadamente estos escenarios, dejando vacíos jurídicos que los ciberdelincuentes pueden explotar.

Para enfrentar estos desafíos, es necesario adoptar un enfoque integral que combine avances tecnológicos, marcos regulatorios actualizados y cooperación internacional.

Algunas medidas propuestas incluyen:

1. Implementar de tecnologías avanzadas de monitoreo y análisis en tiempo real de actividades sospechosas en la red.

2. Desarrollar de herramientas de inteligencia artificial y aprendizaje automático para detectar y prevenir ciberataques.

Entre los casos más notorios de ciberdelincuencia destacan *Silk Road*, un mercado negro en línea desmantelado en 2013, y las operaciones *Pacifier* y *AlphaBay-Hansa*, enfocadas en combatir redes de pornografía infantil y narcotráfico respectivamente. Estos ejemplos ilustran la complejidad y alcance global de las actividades delictivas en el ciberespacio, así como la necesidad de cooperación internacional para hacerles frente. Un fenómeno emergente que genera preocupación es el uso malicioso de la inteligencia artificial (IA) con fines delictivos. Se han documentado casos de manipulación de imágenes mediante IA para crear contenido sexual no consentido, lo que plantea nuevos dilemas éticos y legales. La legislación actual en muchos países no contempla adecuadamente estos escenarios, dejando vacíos jurídicos que los ciberdelincuentes pueden explotar.

Para enfrentar estos desafíos, es necesario adoptar un enfoque integral que combine avances tecnológicos, marcos regulatorios actualizados y cooperación internacional.

Algunas medidas propuestas incluyen:

1. Implementar de tecnologías avanzadas de monitoreo y análisis en tiempo real de actividades sospechosas en la red.

2. Desarrollar de herramientas de inteligencia artificial y aprendizaje automático para detectar y prevenir ciberataques.

3. Fortalecer de las capacidades de investigación forense digital, incluyendo técnicas especializadas para la *dark web*.

4. Actualizar y armonizar marcos legales a nivel nacional e internacional para abordar nuevas formas de ciberdelincuencia.

5. Fomentar la colaboración entre sectores público y privado, así como entre diferentes países, para compartir información y recursos.

6. Promoción de una cultura de ciberseguridad mediante programas de educación y concientización para usuarios y organizaciones.

Es importante destacar que la regulación del ciberespacio presenta desafíos únicos debido a su naturaleza virtual y en constante evolución. Los enfoques tradicionales de legislación pueden resultar inadecuados o rápidamente obsoletos frente al ritmo acelerado de innovación tecnológica. Por ello, se requiere un proceso continuo de adaptación y actualización de las políticas y estrategias de ciberseguridad.

La aparición de nuevas tecnologías como el metaverso, la computación cuántica y los neurodispositivos plantea interrogantes adicionales sobre privacidad, seguridad y ética digital. Estos avances ofrecen oportunidades sin precedentes, pero también conllevan riesgos potenciales que deben ser anticipados y gestionados de manera proactiva.

En el ámbito de la investigación criminal, resulta crucial adoptar un enfoque multidisciplinario que combine experiencia técnica, legal y forense.

Los investigadores deben mantenerse constantemente actualizados sobre las últimas tendencias y herramientas en ciberseguridad, así como desarrollar habilidades para analizar y presentar evidencia digital de manera efectiva en contextos judiciales.

La protección de datos personales emerge como un tema central en la era digital. El uso generalizado de aplicaciones y servicios en línea implica la cesión constante de información personal, a menudo sin plena conciencia por parte de los usuarios. Es fundamental promover una mayor transparencia en las políticas de tratamiento de datos y educar a la población sobre los riesgos asociados al compartir información en línea.

En conclusión, el panorama actual de la ciberseguridad se caracteriza por su complejidad y dinamismo. Los retos planteados por la ciberdelincuencia requieren un abordaje holístico que combine innovación tecnológica, marcos regulatorios flexibles y colaboración internacional. Es imperativo mantener un equilibrio entre el aprovechamiento de las oportunidades ofrecidas por las nuevas tecnologías y la mitigación de los riesgos asociados.

La construcción de un ciberespacio más seguro y confiable demanda el compromiso y participación activa de todos los actores involucrados: gobiernos, sector privado, academia y sociedad civil. Solo mediante un esfuerzo coordinado y sostenido será posible hacer frente a las amenazas cibernéticas actuales y futuras, salvaguardando los derechos y libertades fundamentales en el entorno digital.

ALIADOS Y PATROCINADORES

HOCFORENSIC INTERNACIONAL SAS

Hocforensic Internacional SAS, subsidiaria de Hocforensic Inc., es una empresa líder en ciencias forenses e investigación criminal fundada en 2010 en Bogotá.

Con 13 años de experiencia, la compañía se dedica a la promoción de estudios, implementación y fabricación de insumos forenses, cumpliendo con estándares internacionales.

La empresa cuenta con un equipo de expertos altamente calificados y certificados en diversas áreas de las ciencias forenses, brindando servicios tanto a entidades públicas como privadas. Hocforensic Internacional se destaca por:

1. Fabricación y diseño de reactivos de lofoscopia y equipos de luces forenses.

2. Consultoría internacional en medicina legal, especialmente en temas de fuentes de luz alterna.

3. Suministro de insumos a instituciones como la Fiscalía General de la Nación, la Escuela de Investigación Criminal y el Comité Internacional de la Cruz Roja.

4. Formación y capacitación de profesionales, tecnólogos y técnicos en ciencias forenses

y criminalística.

5. Consultoría pericial para la Secretaría de Movilidad de Bogotá y CESVI Colombia en atención de siniestros de tránsito.

Su coordinadora nacional e internacional de proyectos de investigación criminal y ciencias forenses es Luisa Fernanda Herrera Ramírez. El director fundador, perito certificado por el Instituto Nacional de Medicina Legal y Ciencias Forenses, se capacita regularmente en instituciones internacionales de Ciencias Forenses en Estados Unidos.

DIAF

DIAF, Tienda Forense Colombia, es una empresa fundada en 2012 que ofrece servicios de investigación privada, capacitación forense y venta de equipos especializados. La compañía cuenta con un equipo de peritos e investigadores expertos en lofoscopia, grafoscopia, documentología y perfilación criminal.

La DIAF ofrece los siguientes servicios:

1. Investigaciones empresariales y privadas

2. Estudios de seguridad para multinacionales y procesos de selección de personal.

3. Análisis de firmas y documentos cuestionados en casos penales, civiles y

empresariales.

4. Fabricación, venta, exportación e importación de insumos y equipos forenses.

La empresa ha expandido sus operaciones a nivel nacional e internacional, realizando capacitaciones en Panamá y Bolivia. También ha colaborado con el Ejército colombiano y participado en proyectos mediáticos, como el análisis del caso de Luis Alfredo Garavito para el canal Testigo Directo.

DIAF organiza regularmente conferencias gratuitas sobre temas forenses, con la participación de expertos en diversas áreas. Estas actividades buscan promover la actualización constante de los profesionales en el campo de la criminalística.

DIAF reconoce la importancia de la formación continua y la especialización para los estudiantes y profesionales del área forense; recomienda buscar un enfoque específico dentro del campo, ya sea en el sector público o privado, y complementar la educación formal con cursos, diplomados y seminarios especializados.

La empresa mantiene alianzas estratégicas con diversas instituciones y planea expandir sus actividades en colaboración con *Criticalpath Forensics*, una marca mexicana reconocida en el ámbito forense. Esta colaboración incluirá una gira nacional en Colombia y México, ofreciendo oportunidades de capacitación internacional para los profesionales del sector.

RedExpertos

RedExpertos es una empresa certificada en ISO 27001, especializada en gestión de servicios de ciberseguridad. La compañía aborda los incidentes de ciberseguridad desde una perspectiva innovadora, adaptada a los cambios tecnológicos recientes.

El enfoque tradicional de ciberseguridad basado en el perímetro se ha vuelto obsoleto debido a la adopción de tecnologías en la nube y el auge del teletrabajo. En respuesta, RedExpertos promueve un modelo de “cero confianza”;, que implica dudar de todos los eventos que ocurren en el entorno digital.

Este cambio de paradigma se debe, en gran parte, a la evolución de las tácticas de los ciberdelincuentes, quienes cuentan con muchos recursos y una alta capacidad de innovación. Para enfrentar estos desafíos, las organizaciones requieren personal más comprometido y motivado.

RedExpertos utiliza el marco de trabajo del Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, que consta de cinco capas:

1. Identificación de activos

2. Prevención de incidentes

3. Detección de amenazas

4. Respuesta a incidentes

5. Restauración tras incidentes

Adicionalmente, la empresa incorpora una sexta capa enfocada en aspectos legales, para ayudar a las organizaciones a enfrentar los desafíos jurídicos relacionados con la ciberseguridad.
La capa de detección es particularmente relevante para el análisis forense, ya que implica la recopilación y consolidación de información de sistemas, así como el uso de inteligencia artificial para la detección temprana de incidentes.

En resumen, RedExpertos se enfoca en un modelo de prevención de incidentes informáticos, adaptando sus estrategias a las nuevas realidades del panorama de ciberseguridad y priorizando un enfoque proactivo y de confianza cero.

UID

La Unidad de Investigación Criminal de la Defensa colabora con la administración de justicia apoyando a las víctimas de delitos junto con la Policía Judicial y la Fiscalía General de la Nación. Su objetivo es la judicialización de los responsables respaldando los programas metodológicos con pruebas y análisis forense.

También presta servicios de investigación criminal y ciencias forenses a personas acusadas por diferentes tipos de delitos sin importar su condición social, estrato socioeconómico, vínculo político o creencia religiosa.

Ha brindado capacitación a funcionarios públicos en Centro y Sur América en coordinación con diferentes agencias internacionales y destacadas universidades del país.

MEMORIAS DEL VII CONGRESO EN INVESTIGACIÓN CRIMINAL. MÁS ALLÁ DE LO VISIBLE: REFLEXIONES EN TORNO A LA DEEP WEB EN UN MUNDO HIPERCONECTADO

27 OCT 2023

ISSN: 3028- 7553 (En línea)