Revista Iberoamericana de Derecho, Cultura y Ambiente

Edición Nº 9 – Julio de 2026

Capítulo de Derecho Ambiental

www.aidca.org/revista

EL PAPEL DE LOS CIBERDELITOS EN EL DERECHO Y GESTION AMBIENTAL

Por Alejandro Horacio Braga[1]

INTRODUCCION

La intersección entre los ciberdelitos y el derecho ambiental representa una nueva frontera en la persecución de ilícitos, donde las tecnologías digitales se utilizan tanto para cometer delitos contra el entorno como para protegerlo. El derecho ambiental busca regular, prevenir y sancionar conductas que degraden el ecosistema, mientras que el ciberdelito abarca actividades ilegales que utilizan medios informáticos.

En ese orden, el Derecho cibernético y el Derecho ambiental abordan cuestiones diferentes y requieren enfoques distintos. Esta diferencia se puede observar en la naturaleza de los temas abordados. El Derecho de los delitos cibernéticos se centra en los delitos cometidos por medios digitales, como el

[1] Abogado UBA. Posgrado Derecho Ambiental Universidad Austral. Máster Derecho Ambiental Facultad de Derecho País Vasco España. Profesor universitario y nivel superior. Fiscal Ministerio Publico Fiscal Poder Judicial Provincia de Buenos Aires

pirateo informático, el fraude en línea, el robo de identidad y el ciberacoso. Su objetivo es garantizar la seguridad e integridad del ciberespacio. En cambio el Derecho Ambiental se ocupa principalmente de la preservación y protección del medio ambiente natural incluyendo cuestiones como la calidad del aire, los recursos hídricos, la conservación de la fauna silvestre, la gestión de residuos y el desarrollo sostenible; valiéndose también para ese fin del Derecho Penal y particularmente aquel incipiente Derecho Penal ambiental.

Para abordar eficazmente la ciberdelincuencia y las preocupaciones medioambientales se requieren conocimiento y experiencias especializados. Combatir la ciberamenazas exige comprender la informática forense, la protección de datos, las pruebas electrónicas y cooperación internacional. La protección del medio ambiente por otro lado implica el conocimiento de sistemas ecológicos, las ciencias ambientales y las practicas sostenibles.

Así, la legislación sobre delitos informáticos incluye disposiciones relativas a la evidencia electrónica, la protección de datos y la cooperación internacional para abordar eficazmente la complejidad de los delitos digitales. En la actualidad, los ciberdelincuentes ya no sólo buscan dinero, sino que información confidencial de las organizaciones e incluso hay intereses políticos de dañar en áreas tan complejas como la ecología a gobiernos opositores.

Valga el ejemplo en el rubro que se ha visto comprometido con la acción de estos criminales digitales es la acuicultura, en que una falla podría traer consecuencias catastróficas al medio ambiente. Allí han puesto sus ojos los ciberdelincuentes quienes lograron entrar a sus sistemas para dejarlos inactivos. Pidieron dinero por devolver el control y se podría temer la liberación de millones de peces, afectando al ecosistema cercano al lugar de su crianza. embarcaderos, reglamentos, permisos, supervisión y mecanismos de aplicación específicos para la protección y conservación del medio ambiente.

En esta línea existe también otra forma de contaminar como el cryptojacking que es una acción criminal que aumenta la huella de carbono. Se trata de una técnica en que intervienen miles de equipos de personas comunes,

para ponerlos bajo su control, en la labor de minar criptomonedas para beneficiarse. De esta forma, se adueñan de dispositivos de terceros, aumentan sus ganancias y hacen crecer el impacto medioambiental a raíz de la enorme cantidad de aparatos conectados que requieren energía constante para el proceso de minado. El uso de energía para la delincuencia atenta contra el desarrollo sostenible.

Es así, que la ciberdelincuencia genera problemas al medio ambiente: La demanda de dispositivos electrónicos como computadoras, teléfonos móviles y servidores para apoyar al cibercrimen puede aumentar la producción y el uso de recursos naturales, como metales, plásticos y energía, lo que puede provocar una huella de carbono significativa.

Si bien el Derecho cibernético y el Derecho ambiental pueden parecer incompatibles, es fundamental abordarlos por separado –debido al incipiente desarrollo de ambos- y centrarnos en cómo afrontar eficazmente los desafíos únicos que presentan. A pesar de sus diferencias es crucial reconocer la importancia tanto de la tecnología como de la ecología en nuestra sociedad. Al estudiar y comprender estos temas individualmente, podemos desarrollar conocimientos y estrategias para combatir el cibercrimen y proteger el medio ambiente.

PLANTEO DEL PROBLEMA

Hemos señalado hasta aquí, que tanto el Derecho cibernético como el Derecho ambiental, particularmente el Derecho Penal ambiental transitan por carriles separados.

Uno de los fundamentos de ello, es su relativa reciente formulación: tal es así que no podemos decir –hasta ahora- que nos encontremos ante una rama del Derecho como puede ser Derecho Penal, Derecho Civil, Derecho laboral aunque ambos tengan institutos propios que lo caracterizan y conformen una rama autónoma como ocurre, por ejemplo, con el Derecho de los Recursos Naturales particularmente el Derecho minero.

El primer desafío de estas disciplinas es encontrar puntos en común para poder avanzar en las investigaciones criminales sin que estas se frustren.

Al principio del trabajo ya algo hemos señalado al sostener que es de interés de los ciberdelincuentes acceder a información de datos que se logren a través de una gestión ambiental; ejemplo tratamiento de aguas, calidad, cantidad, origen, monitoreo y distribución; de recursos mineros estratégicos como así también de información agroalimentaria. Esa información se encuentra almacenada y es allí donde los ciberdelincuentes podrían actuar.

Podemos encontrar así vínculos principales entre Ciberdelitos y Daño Ambiental

Ataques a Infraestructura Crítica: Ciberdelincuentes pueden hackear sistemas de gestión de recursos (agua, energía, residuos) para inhabilitarlos, lo que puede resultar en la liberación de contaminantes o peces (en criaderos), afectando el ecosistema cercano.

Cryptojacking y Huella de Carbono: La minería ilícita de criptomonedas (cryptojacking) secuestra la capacidad de cómputo de múltiples dispositivos, aumentando drásticamente el consumo de energía y, por ende, la huella de carbono.

Fraude en Normativa Ambiental y Comercio Ilegal: La tecnología se utiliza para falsificar permisos de tala, transporte de madera o comercio ilegal de especies silvestres, dificultando la trazabilidad y la acción de las autoridades.

Lavado de Activos: Los beneficios económicos obtenidos de delitos ambientales (deforestación, pesca ilegal, minería) a menudo se lavan a través de complejos sistemas financieros digitales.

Es así que nos encontramos ante una situación problemática que este trabajo pretende abordar en una primera y somera presentación.

Se pretende individualizar puntos en común entre el Derecho cibernético y el Derecho Ambiental, particularmente el Derecho Penal ambiental; que sirvan como insumo para las investigaciones criminales y evitar que estas naufraguen.

ANALISIS PROPIO DE LA PROBLEMÁTICA

La falta de Legislación Específica: En Argentina, por ejemplo, no existe una tipificación penal específica para el "ecocidio" o los delitos ambientales de manera autónoma en el Código Penal, recurriéndose a figuras dispersas.

Trasnacionalidad: Los ciberdelitos suelen ser transnacionales, lo que complica la jurisdicción y requiere cooperación internacional (cartas rogatorias) para investigar.

Nuevas Modalidades de Investigación: La evidencia digital es clave. Se requieren protocolos de actuación para el allanamiento remoto y la preservación de pruebas en entornos virtuales.

Ciberataques con consecuencias reales: **¿cómo la ciberdelincuencia afecta al medio ambiente?**

Cuando hablamos de ciberataques, nos imaginamos el robo informático de datos confidenciales o secuestro de equipos y extorsión, sin embargo, la ciberdelincuencia también tiene consecuencias en el mundo físico, no solo en digital, impactando hasta el medio ambiente.

Vivimos en tiempos en que todos los procesos industriales, de seguridad y control se ejecutan a través de dispositivos electrónicos e Internet. Las bandas lo saben y han agudizado sus habilidades para violar empresas sensibles que, ante un mínimo descuido, pondrían en jaque a la seguridad medioambiental de un país.

Se trata de ataques a infraestructura estratégica que ocurren generalmente a través de un error humano, acceden a servidores y equipos para controlar centrales eléctricas, oleoductos, plantas de tratamiento de agua, y generar un impacto directo a través de la contaminación del aire y del agua.

Vale citar como ejemplo que en mayo de 2021, una banda extranjera logró tomar control de la red de oleoductos más grande de Estados Unidos y se temió el derrame de millones de litros de petróleo si no pagaban el rescate. De haber logrado su objetivo, el desastre ecológico habría sido enorme, sumado al desabastecimiento.

MEDIR EL IMPACTO AMBIENTAL DE UN ATAQUE

En los últimos años, se ha planteado la opción de medir las consecuencias medioambientales de un ataque para dimensionar el impacto que tienen los ciberataques. Como no solo hay implicancias económicas, se piensa auditar el daño que puedan llegar a tener en el entorno y las comunidades.

El impacto ambiental que puedan alcanzar ataques cibernéticos específicos puede ser superior al daño económico que genere, y como consecuencia impactar también al prestigio de la organización, por lo que destaca que empresas del área de distribución de agua o combustibles, empresas químicas o generadoras de electricidad, además de centrales nucleares deben estar muy atentas a eventuales ataques, sus consecuencias y daños colaterales.

En ese contexto los ciberataques pueden provocar daño a los recursos naturales y por ende al ambiente.

En la búsqueda de los puntos en común entre ambas disciplinas podemos decir que el Derecho Ambiental nace en la década de los 70 a partir de los movimientos new age, el mayo francés de 1968 fue un hito fundamental pero aquello que resulta principal para el trabajo es que el espíritu de este nacimiento fue la concientización de la protección del ambiente ante el avance de la industrialización y la destrucción de los recursos naturales que esta provocaba.

El Derecho Penal ambiental ya tenía algunas normas que plasmaban ello especialmente a través de los arts. 200 a 205 del Código Penal argentino donde pretendía evitar particularmente la contaminación de aguas, suelo y aire; la ley de fauna -22421- estableciendo allí los requisitos para la caza, protegiendo así a las especies si no se daban esos requisitos administrativos; la ley de suelos 22428 al establecer existencias en pro de su conservación y evitar su erosión y más recientemente la ley de residuos peligrosos 24051 y su posterior residuos industriales donde establece los requisitos para la eliminación de sustancias peligrosas y de aquellas derivadas de las actividades industriales.

Hay que tener presente en este punto que evitar la comisión de estos delitos conforma así la gestión ambiental y esta actividad causa la recolección de

datos acerca de la calidad, cantidad, trazabilidad como así también entrecruzamiento de estos componentes.

Esta información es almacenada por las empresas locales pero ya podemos encontrar un punto en común con el ciberdelito toda vez que en ocasiones cuando esta actividad se encuentra en manos de empresas trasnacionales esta información se encuentra alojada fronteras afuera de nuestro territorio nacional.

Los recursos naturales en muchos supuestos son compartidos entre distintos Estados; por ejemplo el agua donde compartimos el Rio de la Plata con Uruguay.

Lo que se pretende señalar aquí es que le evolución del Derecho ambiental –al igual que el Derecho cibernético- ya cuenta con una base que es el Derecho Penal y para ambos allí nace una subespecialidad.

Ambos evolucionan.

El Derecho Penal ambiental avanza ante la necesidad de regular la calidad de los recursos naturales, protege un bien jurídico –ambiente aunque nuestro Código Penal lo tenga camuflado como salud- y el Derecho de los ciberdelitos protege la privacidad, entre otros.

Para empezar a comprender la incidencia de los ciberdelitos en el campo del Derecho y la gestión medio ambiental esta área del Derecho deberá comenzar a familiarizarse y comprender conceptos tales como como:

Cibercrimen

-Identifica los delitos principales que pueden incluir: (1) acceso ilegal, (2) interferencia con datos, (3) interferencia con sistemas informáticos, (4) interceptación ilegal de datos y (5) dispositivos ilegales que considera dentro de su alcance.

-Definido como delitos cometidos contra datos informáticos, medios de almacenamiento de datos informáticos, sistemas informáticos, proveedores de servicios.

-Ataques sofisticados, o delitos de alta tecnología.

-Delitos cometidos contra datos informáticos, medios de almacenamiento de datos informáticos, sistemas informáticos, proveedores de servicios. El concepto generalmente abarca categorías de delitos tales como acceso ilegal, interferencia con datos y sistemas informáticos, fraude y falsificación, interceptación ilegal de datos, dispositivos ilegalese infracciones de propiedad intelectual.

Ciberseguridad

-Típicamente definida como la protección de la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos con el fin de mejorar la seguridad, la resiliencia, la fiabilidad y la confianza en las TIC. El concepto generalmente abarca dimensiones políticas (intereses nacionales y seguridad), técnicas y administrativas.

-Se refiere al conjunto de herramientas, políticas, enfoques de gestión de riesgos, acciones, formación, mejores prácticas, garantías y tecnologías que pueden utilizarse para proteger el entorno cibernético, y los activos de la organización y del usuario.

-Una postura sólida de ciberseguridad protege los sistemas informáticos contra el acceso no autorizado o los daños o la inutilización. Su objetivo es reducir el riesgo de ciberataques y proteger contra la explotación no autorizada de sistemas, redes y tecnologías mediante el uso de tecnologías, procesos y controles a nivel técnico, procedimental e institucional.

-La ciberseguridad se centra en la política y el procedimiento para proteger los sistemas y activos.

-Las regulaciones de ciberseguridad generalmente trabajan para prevenir ataques antes de que ocurran. La seguridad es un ciclo continuo que incluye la respuesta a incidentes y la revisión de procesos que ocurren después de la detección de una brecha.

Informática forense - es el proceso de examinar metódicamente medios informáticos (discos duros, disquetes, cintas, etc.) en busca de evidencias. En

otras palabras, la informática forense es la recopilación, preservación, análisis y presentación de evidencia relacionada con computadoras.

Informática forense - también conocida como análisis forense informático, descubrimiento electrónico, descubrimiento de evidencia electrónica, descubrimiento digital, recuperación de datos, descubrimiento de datos, análisis informático y examen informático.

Delitos ambientales. Abarcan una amplia lista de actividades ilícitas, incluido el comercio ilegal de vida silvestre; el contrabando de sustancias que agotan la capa de ozono (SAO); el comercio ilícito de residuos peligrosos; la pesca ilegal, no declarada y no reglamentada; y la tala ilegal y el comercio de madera.

Sistema de Derecho Ambiental - es una forma organizada de utilizar todas las leyes de nuestro sistema jurídico para minimizar, prevenir, sancionar o remediar las consecuencias de acciones que dañan o amenazan el medio ambiente, la salud pública y la seguridad.

Derecho ambiental - es un área donde existe un "sistema" de estatutos, reglamentos, directrices, conclusiones fácticas e interpretaciones específicas de casos que se relacionan entre sí en el contexto de principios generalmente aceptados establecidos durante la breve historia del derecho ambiental.

Acceso. Se refiere a la instrucción, comunicación, almacenamiento de datos, recuperación de datos o cualquier otro uso de los recursos de un sistema informático o red de comunicación.

Controles de acceso. Medidas que establecen privilegios, determinan el acceso autorizado y previenen el acceso no autorizado.

Huella digital activa. Creada por datos proporcionados por el usuario.

Fraude de tarifa anticipada. Un fraude informático que implica una solicitud de tarifa anticipada para completar una transferencia, depósito u otra transacción a cambio de una suma mayor de dinero.

Amenazas persistentes avanzadas. Individuos y/o grupos que persisten en atacar a una entidad. También conocidos como APT.

Alteración. Se refiere a la modificación o cambio, en forma o sustancia, de datos o programas informáticos existentes.

Denominaciones de origen. Símbolos de la calidad de los productos y de la reputación del lugar de creación, que no pueden utilizarse a menos que el producto haya sido desarrollado en esa región según las normas de práctica. También conocidas como indicaciones geográficas.

Anonimato. El ocultamiento de la identidad de uno para permitir que las personas participen en actividades sin revelarse a sí mismas y/o sus acciones a otros.

Servidores proxy anónimos. Estos servidores proxy permiten a los usuarios ocultar datos de identidad enmascarando su dirección IP y sustituyéndola por una diferente. También conocidos como anonimizadores.

Antiforense digital. Herramientas y técnicas utilizadas para obstaculizar la investigación del cibercrimen y los esfuerzos de forensia digital. También conocida como antiforense.

Antimalware o Antivirus. Estos sistemas utilizan firmas o análisis de comportamiento de aplicaciones para identificar y bloquear la ejecución de código malicioso.

Análisis de aplicaciones y archivos. Tipo de análisis que se realiza para examinar aplicaciones y archivos en un sistema informático con el fin de determinar el conocimiento, la intención y las capacidades del perpetrador para cometer cibercrímenes.

Activo. Algo que se considera importante y/o valioso.

Atribución. La determinación de quién y/o qué es responsable de un cibercrimen.

Disponibilidad. Los datos, servicios y sistemas son accesibles a demanda.

Big data. Grandes volúmenes de datos estructurados y no estructurados que pueden consolidarse y analizarse para revelar información sobre asociaciones, patrones y tendencias.

Ataque de fuerza bruta. El uso de un script o bot para adivinar las credenciales de usuario.

Rastreo inverso. El proceso de rastrear actos ilícitos hasta el origen del cibercrimen. También conocido como trazabilidad.

Botcode. Un tipo de software malicioso que permite el control remoto de dispositivos y los usa para cometer cibercrímenes, robar información y/o llevar a cabo ciberataques.

Botherder. Controlador de dispositivos digitales infectados por bots.

Alojamiento a prueba de balas. Un servicio que permite a los delincuentes utilizar servidores para cometer cibercrímenes, almacenar contenido ilícito y proteger el contenido ilícito para que no sea accedido por las autoridades policiales y/o eliminado.

Plan de continuidad del negocio. Describe las instrucciones a seguir y las acciones a tomar en caso de un incidente de ciberseguridad. También conocido como plan de gestión de emergencias.

Censura. La prohibición de información, representaciones visuales y comunicaciones escritas u orales prohibidas por la ley y/o su supresión por un gobierno, comunidad o grupo porque son ilegales y/o se consideran dañinas, impopulares, indeseables o políticamente incorrectas.

Cadena de custodia. Un registro detallado sobre la evidencia, el estado de la evidencia, su recopilación, almacenamiento, acceso y transferencia y los motivos de su acceso y transferencia, es esencial para garantizar la admisibilidad de la evidencia digital en la mayoría de los tribunales.

Recopilación. Se refiere a la obtención y recepción de información.

Comunicación. Se refiere a la transmisión de información a través de medios de tecnología de la información y comunicación (TIC), incluidos voz, video y otras formas de datos.

Autoridad Competente. Se refiere al Centro de Investigación y Coordinación de Cibercrimen o al DOJ – Oficina de Cibercrimen, según corresponda.

Código de ética. Directrices que cubren la conducta correcta e incorrecta para orientar la toma de decisiones.

Datos informáticos. Cualquier forma de representación de información procesada por un sistema de dispositivo digital. También conocidos como información informática. Significa cualquier representación de hechos, información o conceptos en una forma adecuada para el procesamiento en un sistema informático, incluido un programa adecuado para hacer que un sistema informático realice una función.

Medio de almacenamiento de datos informáticos. Cualquier artículo o material (por ejemplo, un disco) del que sea posible reproducir información, con o sin la ayuda de cualquier otro artículo o dispositivo.

Equipo de Respuesta a Emergencias Informáticas. Un equipo que brinda apoyo en incidentes de ciberseguridad. También conocido como Equipo de Respuesta a Incidentes de Seguridad Informática.

Información informática. Cualquier forma de representación de información procesada por un sistema de dispositivo digital. También conocida como datos informáticos o datos.

Programa informático se refiere a un conjunto de instrucciones ejecutadas por la computadora para lograr los resultados deseados.

Confidencialidad. Los sistemas, redes y datos están protegidos, y sólo los usuarios autorizados pueden acceder a ellos.

Divulgación coordinada de vulnerabilidades. La práctica de compartir y divulgar información de forma armonizada sobre vulnerabilidades a las partes interesadas pertinentes junto con las tácticas utilizadas para su mitigación.

Derechos de autor. Productos creativos, como obras artísticas y literarias, protegidos por la ley.

Desplazamiento del crimen. Cuando un crimen destinado a un objetivo se comete en otro objetivo debido a las medidas de seguridad implementadas.

Reconstrucción del crimen. Este proceso busca determinar quién fue responsable del crimen, qué sucedió, dónde ocurrió el crimen, cuándo tuvo lugar y

cómo se desarrolló, mediante la identificación, compilación y vinculación de datos. También conocido como reconstrucción de eventos.

Criptomoneda. Una forma de moneda digital asegurada mediante cifrado avanzado. Es dinero digital que puede usarse para comprar bienes y servicios, utilizando técnicas de cifrado sólidas para proteger estas transacciones en línea.

Crimen organizado cibernético. Término utilizado para describir una empresa criminal continua que trabaja racionalmente para obtener beneficios de actividades ilícitas que tienen demanda en línea.

Delincuentes organizados cibernéticos. Un grupo estructurado de tres o más personas, existente durante un período de tiempo y actuando de concierto con el objetivo de cometer uno o más delitos graves u ofensas establecidas de acuerdo con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 2000, que operan total o parcialmente en línea, con el fin de obtener, directa o indirectamente, un beneficio económico u otro beneficio material.

Proxies cibernéticos. El uso de intermediarios para contribuir directa o indirectamente a un delito ciber-dependiente que intencional y deliberadamente tiene como objetivo a un estado.

Ciberespionaje. El uso de tecnología de la información y comunicación por parte de actores gubernamentales, grupos patrocinados o dirigidos por el estado, u otros que actúan en nombre de un gobierno, para obtener acceso no autorizado a sistemas y datos en un esfuerzo por recopilar inteligencia sobre sus objetivos con el fin de mejorar la seguridad nacional, la competitividad económica y/o la fortaleza militar de su país.

Ciberacoso (Cyberharassment). El uso de tecnología de la información y comunicación para humillar, molestar, atacar, amenazar, alarmar, ofender y/o abusar verbalmente de manera intencional a un individuo (o individuos).

Cryptoransomware. Malware que infecta el dispositivo digital de un usuario, cifra los documentos del usuario y amenaza con eliminar archivos y datos si la víctima no paga el rescate.

Ciberdifamación. Publicación o distribución de información falsa o rumores sobre un adulto o un niño para dañar la posición social, las relaciones interpersonales y/o la reputación de la víctima.

Ciberacecho. El uso de tecnología de la información y comunicación para cometer una serie de actos durante un período de tiempo diseñados para acosar, molestar, atacar, amenazar, asustar y/o abusar verbalmente de un individuo (o individuos).

Postura de ciberseguridad. Término utilizado para describir las capacidades de ciberseguridad de un país, organización o empresa.

Ciberterrorismo. Los delitos ciber-dependientes perpetrados contra infraestructuras críticas para causar alguna forma de daño y provocar miedo en la población objetivo.

Ciberguerra. Actos cibernéticos que comprometen y alteran los sistemas de infraestructura crítica, que equivalen a un ataque armado. También es el uso de tecnología para penetrar y atacar los sistemas informáticos y redes de otra nación con el fin de causar daño o interrumpir servicios, como apagar una red eléctrica.

Base de datos se refiere a una representación de información, conocimiento, hechos, conceptos o instrucciones que están siendo preparados, procesados o almacenados, o que han sido preparados, procesados o almacenados de manera formalizada, y que están destinados para su uso en un sistema informático.

Evidencia digital se refiere a información digital que puede usarse como evidencia en un caso. La recopilación de la información digital puede llevarse a cabo mediante la incautación del medio de almacenamiento (portador de datos), la interceptación o monitoreo del tráfico de red, o la realización de copias digitales (p. ej., imágenes forenses, copias de archivos, etc.) de los datos almacenados.

Dark Web. La parte de la World Wide Web conocida por sus sitios web oscuros y ocultos que albergan actividades, bienes y servicios ilícitos, y que sólo puede accederse utilizando software especializado. También conocida como darknet.

Datos. Cualquier forma de representación de información procesada por un sistema de dispositivo digital. También conocidos como datos informáticos o información informática.

Preservación de datos. Las solicitudes son realizadas por las fuerzas del orden a los proveedores de servicios para retener datos antes de que sean eliminados o alterados de cualquier manera.

Minería de datos. La recuperación de información de conjuntos de datos.

Protección de datos. La salvaguarda de la información personal y la regulación de su recopilación, almacenamiento, análisis, uso y compartición.

Ataque DDoS. El uso de múltiples computadoras y otras tecnologías digitales para llevar a cabo ataques coordinados con la intención de abrumar servidores para impedir el acceso de usuarios legítimos. También conocido como ataque de denegación de servicio distribuido.

Deep Web. La parte de la World Wide Web que no está indexada por los motores de búsqueda y no es fácilmente accesible y/o disponible para el público.

Ataque de denegación de servicio. Un cibercrimen que interfiere con los sistemas al abrumar los servidores con solicitudes para impedir que el tráfico legítimo acceda a un sitio y/o use un sistema. También conocido como ataque DoS.

Patentes de diseño. Una forma de propiedad intelectual que incluye diseños creados con el propósito específico de ser estéticamente agradables para los consumidores e influir en su elección entre productos. También conocidas como diseños industriales.

Evidencia digital. Datos obtenidos de tecnología de la información y comunicación. También conocida como evidencia electrónica.

Huella digital. Datos dejados por los usuarios de TIC que pueden revelar información sobre ellos, incluyendo edad, género, raza, etnia, nacionalidad, orientación sexual, pensamientos, preferencias, hábitos, aficiones, historial médico y preocupaciones, trastornos psicológicos, situación laboral, afiliaciones, relaciones, geolocalización, rutinas y otras actividades.

Proceso forense digital. La búsqueda, recuperación, preservación y mantenimiento de evidencia digital; la descripción, explicación y establecimiento del origen de la evidencia digital y su importancia; el análisis de la evidencia y su validez, fiabilidad y relevancia para el caso; y la presentación de la evidencia pertinente al caso.

Forense digital. Una rama de la ciencia forense que aplica cuestiones legales a la tecnología de la información y comunicación y a la evidencia digital.

Nombre de dominio. Una representación de una dirección IP en un navegador de Internet (o web).

Sistema de Nombres de Dominio. Permite el acceso a Internet traduciendo los nombres de dominio a direcciones IP.

Ataque DoS. Un cibercrimen que interfiere con los sistemas al abrumar los servidores con solicitudes para impedir que el tráfico legítimo acceda a un sitio y/o use un sistema. También conocido como ataque de denegación de servicio.

Doxing. Información personal sobre individuos publicada en línea para causar algún tipo de daño al individuo.

Doxware. Una forma de cryptoransomware que los perpetradores usan contra las víctimas que libera los datos del usuario si no se paga el rescate para descifrar los archivos y datos.

EDiscovery. El proceso de búsqueda, identificación y preservación de datos digitales para su uso como evidencia en un procedimiento legal.

Evidencia electrónica. Datos obtenidos de tecnología de la información y comunicación. También conocida como evidencia digital.

-La evidencia electrónica se refiere a la evidencia cuyo uso está sancionado por las reglas de evidencia existentes, para determinar en un procedimiento judicial la verdad respecto a un hecho, que se recibe, registra, transmite, almacena, procesa, recupera o produce electrónicamente.

Plan de gestión de emergencias. Describe las instrucciones a seguir y las acciones a tomar en caso de un incidente de ciberseguridad. También conocido como plan de continuidad del negocio.

Cifrado. Medida que bloquea el acceso de terceros a la información y comunicaciones de los usuarios.

Reconstrucción de eventos. Este proceso busca determinar quién fue responsable del evento, qué sucedió, dónde ocurrió el evento, cuándo tuvo lugar y cómo se desarrolló, mediante la identificación, compilación y vinculación de datos. También conocida como reconstrucción del crimen.

Teoría de la utilidad esperada. Una teoría que sostiene que las personas participan en acciones cuando la utilidad esperada de esas acciones es mayor que la utilidad esperada de participar en otras acciones.

Noticias falsas. Propaganda y desinformación que se hace pasar por noticias reales.

Quinto dominio. Término utilizado para describir el ciberespacio como otro dominio de guerra.

Cortafuegos (Firewall). Una medida de seguridad que restringe el libre flujo de información bloqueando el tráfico de datos no autorizado.

Forense se refiere a la aplicación de técnicas de investigación y análisis que se ajustan a los estándares de evidencia y se utilizan en, o son apropiadas para, un tribunal de justicia u otro contexto legal.

Imagen forense, también conocida como copia forense, se refiere a una copia exacta bit a bit de un portador de datos, incluido el espacio no asignado y no utilizado. Existen herramientas forenses disponibles para hacer estas imágenes. La mayoría de las herramientas producen información, como un valor hash, para garantizar la integridad de la imagen.

Relevancia forense. La relevancia de los datos forenses se determina por si la evidencia digital: vincula o descarta una conexión entre el perpetrador y el objetivo y/o la escena del crimen; respalda o refuta el testimonio del perpetrador, la víctima y/o los testigos; identifica al(los) perpetrador(es) del cibercrimen; proporciona pistas de investigación; proporciona información sobre el método de operación del perpetrador; y demuestra que se ha cometido un crimen.

Tallado de archivos. Búsqueda basada en identificadores de contenido.

Primeros respondedores. Individuos que responden primero en la escena y son responsables de asegurar la evidencia en el lugar.

Divulgación completa de vulnerabilidades. Publicar públicamente la vulnerabilidad de software o hardware a través de foros y sitios web en línea antes de que haya disponible una corrección.

Análisis funcional. La evaluación del rendimiento y las capacidades de los sistemas y dispositivos involucrados en los eventos.

Disuasión general. El castigo diseñado para enviar el mensaje a otros de que un comportamiento ilícito similar recibirá un castigo severo similar.

Dogpiling. Una táctica mediante la cual los usuarios dentro de un espacio en línea bombardean a las víctimas con mensajes ofensivos, insultantes y amenazantes para silenciar al objetivo, obligarlo a retractarse de lo dicho y/o pedir disculpas, o forzarlo a abandonar la plataforma.

Nombre de dominio. Una representación de una dirección IP en un navegador de Internet (o web).

Sistema de Nombres de Dominio. Permite el acceso a Internet traduciendo los nombres de dominio a direcciones IP.

Ataque DoS. Un cibercrimen que interfiere con los sistemas al abrumar los servidores con solicitudes para impedir que el tráfico legítimo acceda a un sitio y/o use un sistema. También conocido como ataque de denegación de servicio.

Doxing. Información personal sobre individuos publicada en línea para causar algún tipo de daño al individuo.

Doxware. Una forma de cryptoransomware que los perpetradores usan contra las víctimas que libera los datos del usuario si no se paga el rescate para descifrar los archivos y datos.

Doble incriminación. Una cláusula en los tratados que requiere que los actos se consideren ilegales en los países cooperantes.

EDiscovery. El proceso de búsqueda, identificación y preservación de datos digitales para su uso como evidencia en un procedimiento legal.

Fraude electoral. El uso de tácticas ilegales para influir en las elecciones.

Evidencia electrónica. Datos obtenidos de tecnología de la información y comunicación. También conocida como evidencia digital.

Plan de gestión de emergencias. Describe las instrucciones a seguir y las acciones a tomar en caso de un incidente de ciberseguridad. También conocido como plan de continuidad del negocio.

Cifrado. Medida que bloquea el acceso de terceros a la información y comunicaciones de los usuarios.

Reconstrucción de eventos. Este proceso busca determinar quién fue responsable del evento, qué sucedió, dónde ocurrió el evento, cuándo tuvo lugar y cómo se desarrolló, mediante la identificación, compilación y vinculación de datos. También conocida como reconstrucción del crimen.

Cortafuegos (Firewall). Una medida de seguridad que restringe el libre flujo de información bloqueando el tráfico de datos no autorizado.

Imagen forense, también conocida como copia forense, se refiere a una copia exacta bit a bit de un portador de datos, incluido el espacio no asignado y no utilizado. Existen herramientas forenses disponibles para hacer estas imágenes. La mayoría de las herramientas producen información, como un valor hash, para garantizar la integridad de la imagen.

Relevancia forense. La relevancia de los datos forenses se determina por si la evidencia digital: vincula o descarta una conexión entre el perpetrador y el objetivo y/o la escena del crimen; respalda o refuta el testimonio del perpetrador, la víctima y/o los testigos; identifica al(los) perpetrador(es) del cibercrimen; proporciona pistas de investigación; proporciona información sobre el método de operación del perpetrador; y demuestra que se ha cometido un crimen.

Tallado de archivos. Búsqueda basada en identificadores de contenido.

Primeros respondedores. Individuos que responden primero en la escena y son responsables de asegurar la evidencia en el lugar.

Divulgación completa de vulnerabilidades. Publicar públicamente la vulnerabilidad de software o hardware a través de foros y sitios web en línea antes de que haya disponible una corrección.

Análisis funcional. La evaluación del rendimiento y las capacidades de los sistemas y dispositivos involucrados en los eventos.

Dirección IP. Un identificador único asignado por un proveedor de servicios de Internet a un dispositivo digital conectado a Internet para conectarse a Internet. También conocida como dirección de Protocolo de Internet.

Cibercrimen interpersonal. Cibercrímenes cometidos por individuos contra otros individuos con quienes están interactuando, comunicándose y/o teniendo algún tipo de relación real o imaginaria.

Sistemas de detección de intrusiones. Una medida de ciberseguridad que permite la detección de ciberataques y el acceso y uso no autorizados de sistemas, redes, datos, servicios y recursos relacionados.

Jurisdicción. El poder y autoridad de un estado para hacer cumplir las leyes y sancionar el incumplimiento de las mismas.

Cartas rogatorias. Solicitudes escritas de los tribunales nacionales para obtener evidencia de un país extranjero.

Extracción lógica. La búsqueda y adquisición de evidencia desde la ubicación del sistema de archivos.

Búsquedas por palabras clave. Búsqueda basada en términos proporcionados por el investigador.

Malware. También conocido como software malicioso. Se refiere a cualquier código que puede usarse para robar datos, eludir controles de acceso o causar daño o comprometer un sistema.

Metadatos. Datos sobre el contenido. También conocidos como datos no relacionados con el contenido.

Muleros de dinero. Individuos que, ya sea a sabiendas o sin saberlo, cometen crímenes y/o cibercrímenes al obtener y transferir bienes ilícitos, participar en servicios ilícitos y/o recibir o transferir ilegalmente dinero para otros a cambio de una remuneración.

Tratado de asistencia legal mutua. Un acuerdo entre países para cooperar en investigaciones y enjuiciamientos de ciertos y/o todos los delitos proscriptos por ambas partes bajo la ley nacional.

Neutralidad de la red. Requiere que todos los datos, independientemente de su origen, sean tratados por igual.

Técnicas de neutralización. Técnicas utilizadas para superar o minimizar las emociones negativas asociadas con la participación en actividades ilícitas.

Suplantación de identidad en línea. La suplantación de las víctimas mediante la creación de cuentas con nombres similares y haciendo uso de imágenes existentes de las víctimas.

Autor original se refiere a la persona que creó o es el origen de la declaración o publicación electrónica cuestionada utilizando un sistema informático.

Crimen organizado. Una empresa criminal continua que trabaja racionalmente para obtener beneficios de actividades ilícitas que a menudo tienen gran demanda pública.

Análisis de propiedad y posesión. Tipo de análisis utilizado para determinar la persona que creó, accedió y/o modificó archivos en un sistema informático.

Teoría de la actividad rutinaria. Una teoría que sostiene que el crimen ocurre cuando dos elementos están presentes - un delincuente motivado y un objetivo adecuado, y un elemento está ausente - un guardián capaz.

Huella digital pasiva. Datos obtenidos y dejados involuntariamente por los usuarios de Internet y la tecnología digital.

Patente. "Derecho exclusivo otorgado por una invención (innovación o creación), que es un producto o un proceso que proporciona, en general, una nueva forma de hacer algo, u ofrece una nueva solución técnica a un problema" (OMPI, s.f.).

Autonomía personal. La capacidad de tomar decisiones y actuar según su propio criterio, libre de coerción.

Pharming. La creación de un sitio web falso y duplicado diseñado para engañar a los usuarios para que ingresen sus credenciales de inicio de sesión.

Phishing. El envío de un correo electrónico a objetivos con un enlace de sitio web para que los usuarios hagan clic, lo que podría descargar malware en los dispositivos digitales de los usuarios o enviar a los usuarios a un sitio web malicioso diseñado para robar las credenciales de los usuarios.

Extracción física. La búsqueda y adquisición de evidencia desde la ubicación dentro de un dispositivo digital donde reside la evidencia.

Privacidad. El derecho a ser dejado solo y estar libre de observación; la capacidad de mantener secretos los pensamientos, creencias, identidad y comportamiento de uno; y el derecho a elegir y controlar cuándo, qué, por qué, dónde, cómo y a quién se revela información sobre uno mismo y en qué medida se revela la información.

Privacidad por diseño. Medidas de privacidad integradas en el diseño de sistemas y tecnologías. También conocida como protección de datos por diseño.

Derecho preventivo. Normas legales que se centran en la regulación del riesgo y buscan prevenir el crimen o al menos mitigar el daño que podría causarse en caso de un crimen.

Derecho procesal. Normas legales que cubren los procesos y procedimientos a seguir para aplicar el derecho sustantivo, las reglas para hacer cumplir el derecho sustantivo, y las reglas y estándares en los procedimientos de justicia penal.

Preservación se refiere al mantenimiento de datos que ya existen en forma almacenada, protegidos de cualquier cosa que pueda causar un cambio o deterioro en su calidad o condición actual.

Servidor proxy. Un servidor intermediario que se utiliza para conectar a un cliente con un servidor del que el cliente está solicitando recursos.

Seudonimización. El proceso por el cual los datos de identificación en un registro son reemplazados por identificadores artificiales.

Ransomware. Malware diseñado para tomar como rehén el sistema, archivos y/o datos de los usuarios y devolver el control al usuario solo después de que se pague el rescate.

Recuperación. La identificación, creación e implementación final de medidas para la resiliencia y la restauración de sistemas, redes, servicios y datos que no estaban disponibles, fueron dañados o comprometidos durante el incidente.

Análisis relacional. La determinación de los individuos involucrados y lo que hicieron, y la asociación y relaciones entre estos individuos.

Resiliencia. La capacidad de resistir interrupciones, adaptarse a las condiciones cambiantes y recuperarse de incidentes de TIC y proteger la confidencialidad, integridad y disponibilidad de sistemas, redes, servicios y datos.

Divulgación responsable de vulnerabilidades. La práctica de no divulgar la vulnerabilidad hasta que la organización responsable proporcione una corrección.

Prevención situacional del crimen. Medidas utilizadas para prevenir y reducir el crimen.

Smishing. Phishing a través de mensajes de texto. También conocido como phishing SMS.

Phishing SMS. Phishing a través de mensajes de texto. También conocido como smishing.

Fraude de ingeniería social. Engañar a la víctima para que revele o de otro modo proporcione información personal y/o fondos al perpetrador.

Dilema social. Cuando las decisiones de los individuos se basan en el interés propio en lugar del interés del grupo o colectivo, incluso cuando la utilidad de participar en el interés colectivo es mayor que la utilidad de participar en el interés propio.

Introyección solipsista. La imagen ficticia de los demás creada por las percepciones de los usuarios sobre los demás y sus rasgos en ausencia de datos contextuales, incluidas las relaciones que tienen con ellos basadas en información imaginada en lugar de real.

Ingeniería social. Una táctica mediante la cual un perpetrador engaña al objetivo para que revele información o realice otra acción.

Spearphishing. El envío de correos electrónicos con archivos adjuntos infectados o enlaces diseñados para engañar al receptor para que haga clic en los archivos adjuntos o enlaces.

Spyware. Malware diseñado para monitorear subrepticiamente los sistemas infectados, y recopilar y transmitir información de vuelta al creador y/o usuario del spyware.

Stalkerware. Una forma de spyware que puede ejecutarse en la computadora, teléfono inteligente u otro dispositivo digital habilitado para Internet de una víctima y recopilar y transmitir todas las acciones del usuario en estos dispositivos, desde correos electrónicos y mensajes de texto enviados y recibidos, hasta fotografías tomadas y teclas presionadas.

Procedimientos operativos estándar. Documentos que incluyen las políticas y actos secuenciales que deben seguirse para investigar cibercrímenes y manejar la evidencia digital en tecnología de la información y comunicación.

Esteganografía. La ocultación sigilosa de datos ocultando el contenido y haciéndolo invisible.

Información de suscriptores se refiere a cualquier información contenida en forma de datos informáticos o cualquier otra forma que sea mantenida por un proveedor de servicios, relacionada con los suscriptores de sus servicios, que no sean datos de tráfico o de contenido, y mediante la cual se pueda establecer cualquiera de los siguientes: El tipo de servicio de comunicación utilizado, las disposiciones técnicas tomadas al respecto y el período de servicio; La identidad del suscriptor, la dirección postal o geográfica, el teléfono y otros números de acceso, cualquier dirección de red asignada, información de facturación y pago disponible en base al acuerdo o arreglo de servicio; o Cualquier otra información disponible en el sitio de instalación de equipos de comunicación disponible en base al acuerdo o arreglo de servicio.

Análisis temporal. La determinación del momento en que ocurrieron los eventos y la secuencia de estos eventos.

Trazabilidad. El proceso de rastrear actos ilícitos hasta el origen del cibercrimen. También conocido como rastreo inverso.

Secretos comerciales. Información valiosa sobre procesos y prácticas de negocio que son secretos y protegen la ventaja competitiva de la empresa.

Robo de secretos comerciales. El robo de un secreto comercial fuera de línea y/o en línea para obtener una ventaja competitiva injusta.

Falsificación de marcas comerciales. Uso no autorizado intencional de una marca comercial para etiquetar un bien o servicio que no proviene del propietario de la marca.

Marcas comerciales. Identificadores que distinguen la fuente de un bien o servicio.

Datos de tráfico. Datos transmitidos a través de una red informática (o red). También significa cualquier dato informático relacionado con una comunicación por medio de un sistema informático, generado por un sistema informático que formó parte en la cadena de comunicación, indicando el origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente de la comunicación.

-Los Datos de Tráfico o Datos No Relacionados con el Contenido se refieren a cualquier dato informático que no sea el contenido de la comunicación, incluyendo, entre otros, el origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente de la comunicación.

Caballo de Troya. Malware diseñado para parecer software legítimo con el fin de engañar al usuario para que descargue el programa, que infecta el sistema de los usuarios para espiar, robar y/o causar daño.

Vulnerabilidad. Exposición al daño.

Virus. Malware que requiere actividad del usuario para propagarse.

Vishing. Phishing a través de telecomunicaciones.

Ataque de abrevadero. Colocación de malware en los sitios web más frecuentados por los objetivos para infectar finalmente sus sistemas y obtener acceso no autorizado a ellos.

Rastreadores web. Aplicaciones diseñadas para recorrer la World Wide Web con el fin de lograr objetivos específicos.

Whaling. Hacer pasar por ejecutivos de alto nivel de una empresa, abogados, contadores y otros en posiciones de autoridad y confianza, con el fin de engañar a los empleados para que les envíen fondos.

Gusano (Worm). Software malicioso independiente que se propaga sin necesidad de actividad del usuario.

Bloqueador de escritura. Diseñado para prevenir la alteración de datos durante el proceso de copiado.

Día cero. Vulnerabilidad previamente desconocida que se explota una vez identificada.

Estos términos resultan insumos para programas de gestión ambiental que no revisten mayor implicancia que su conocimiento para prevenir ataques a una gestión ambiental eficaz.

Ahora bien, existen dos conceptos que me parecen si complicados de superar dado el diferente abordaje que realiza el Derecho de los ciber delitos y el Derecho Ambiental; estos serían el acceso a la información y la competencia que corresponde ante determinados delitos.

Ello es así porque el Derecho de acceso a la información ambiental se encuentra garantizado en el artículo 43 de la Constitución Nacional y es tan amplio que no puede ser negado a ninguna persona ya sea de existencia visible o de existencia ideal incluye ONGs y tal es así que el propio Derecho ambiental lo ha establecido como una ley de presupuestos mínimos –ley 27275- esto es conforma en núcleo máximo constitucional para las leyes ambientales obligando a toda empresa y organismo público a entregar toda documentación de relevancia para el cuidado del ambiente y aquella que el Estado no posea lo obliga a generarla.

Este es un punto dicotómico entre el Derecho Ambiental y el Derecho de los ciberdelitos, pues podemos imaginarnos hacer uso de este Derecho para que una empresa nos facilite su información y cuálsería el límite que esta trabaje con datos en sus sistemas informáticos alegando secreto profesional u otro Derecho de confidencialidad; así el punto a dilucidar en entender si una información alojada en un sistema es propia de este Derecho o del Derecho Ambiental entiendo es un tema conflictivo que se avecina.

En otro orden la Convención de Budapest en su artículo 14 y concordantes establece los principios de la competencia atribuible a cada Estado y de la cooperación mutua pretendiendo establecer las bases para determinarla y ello puede entrar en confrontación con distintos Convenios internacionales que forman el Derecho Ambiental tales como la Convención de Basilea que regula el tránsito de residuos peligrosos donde los residuos originados en un país tienen disposición final en otro y es en este "otro" donde los ciberdelincuentes puede actuar afectando el ambiente cuando es responsable el Estado generador aunque sea dispuesto finalmente en otro Estado. En este punto vale aclarar que muchas veces ingresan al país productos que son utilizados como cosas y una vez cumplido su fin adquiere la calidad de residuos –ejemplo los neumáticos- entrando en discusión si la información que vale es aquella que es generada en el propio país o aquella que tiene disposición final cuando los ciberdelincuentes ataquen un sistema informático.

CONCLUSIONES

El Derecho de los ciberdelitos y el Derecho Ambiental son dos ramas autónomas no independientes del Derecho de reciente formulación.

Hasta la fecha han transcurrido en carriles distintos y ello lleva a que sea necesario individualizar puntos en común para proteger el ambiente y en los supuestos necesarios abordar investigaciones penales evitando que estas naufraguen.

Estos primeros puntos en común son los que someramente fueron citados precedentemente sirviendo como insumo para los operadores y gestores ambientales.

Para ello es necesario que los gestores ambientales empiecen a familiarizarse con conceptos del Derecho Informático y particularmente con los ciberataques –como los citados supra-; ello es así pues los sistemas informáticos albergan información acerca del uso producción comercialización y disposición final de productos originados en recursos naturales y que regresan al ambiente.

Estos sistemas informáticos deben preveer estos ataques que pueden llegar a ser de verdadera gravedad; valga el ejemplo citado en el acceso informático al tránsito por oleoductos en Estados Unidos citado supra, donde se exigía una suma de dinero para evitar su adulteración y potencial derrame en aguas con su consecuente contaminación.

Para ello es fundamental reconocer los marcos legales y mecanismos de aplicación diferenciados que requieren el Derecho de los delitos cibernéticos y el Derecho Ambiental. Al mantener una legislación específica para cada materia, podemos desarrollas sistemas jurídicos solidos adaptados a sus respectivos ámbitos; y ambas disciplinas, particularmente la ambiental deberá comenzar a familiarizarse con estos conceptos dada la información que maneja en sus sistemas informáticos para proteger y gestionar el ambiente. Este enfoque permite una implementación y aplicación más efectiva de las leyes garantizando la protección tanto de los espacios digitales como del medio ambiente.

La cuestión adquiere mayor complejidad cuando entra en juego el Derecho Ambiental Internacional con la Convención de Budapest.

En esta área, las convenciones internacionales regulan el tránsito de residuos y sustancias peligrosas como asítambién de recursos naturales como los minerales, fauna y bosques, estableciendo como responsable al generador; es decir aquel que los genera desligando de responsabilidad a quien los recibe –con excepciones- no individualizando a la fecha una solución común para ambas disciplinas cuando exista un ciberataque en los sistemas informáticos del Estado

receptor y fuera aquel quien ocasiona el daño ambiental … empieza aquí una pregunte pendiente …Que Derecho aplicamos, Que Convención prevalece …. La falta de jurisprudencia empieza a responder esta pregunta. Entiendo que sería necesario un Protocolo a modo de Prevención para esta circunstancia.

BIBLIOGRAFIA CONSULTADA

Convención Internacional sobre el control de los movimientos transfronterizos de los desechos peligrosos y su eliminación, firmada en Basilea, 1989-1992.

Convención sobre la ciberdelincuencia, Budapest, 23-XI-2001.

KROM Silvia Beatriz, *La nueva minería sustentable,* Estudio, Buenos Aires, 2009, pp 11-31

MOYANO Lucas*, Ciberdelitos, como investigar en entornos digitales*, Hammurabi, 2024, pp 213-302.

MARTINEZ Víctor, *Ambiente y responsabilidad penal,* Depalma, 1994, pp 129-144