..\BUENOS.AIRES\ARGENTINA\MARZO\2021_

UNIVERSIDAD DE BELGRANO

FACULTAD de DERECHO Y CIENCIAS SOCIALES

- ABOGACÍA -

TESINA para la Obtención del Título de Grado

"INTELIGENCIA ARTIFICIAL E IMPACTO EN EL CIBERCRIMEN"

GEORGINA GAIMARI

MATRÍCULA: 10133775

ID: 000 14 8806

TUTOR:
DR. RICARDO BASILICO

“INTELIGENCIA ARTIFICIAL
E IMPACTO EN EL CIBERCRIMEN”

IMPACTO

 # CIBERCRIMEN # CIBERESPACIO

 # IA #ALGORTIMO #CONDUCTA NO HUMNA

 # DELITOS # PLURIOFENSIVOS

AMBITO # VALIDEZ ESPACIAL

 # EL NO LUGAR

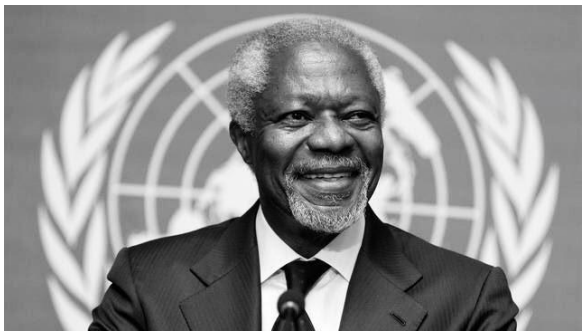
SURFACE # DEEPWEB # DARKWEB

#UB #DERECHO

C:\Users\GAIMARI.GEORGINA_

"No disfrutaremos la seguridad sin desarrollo, no disfrutaremos el desarrollo sin seguridad, y no disfrutaremos ninguna sin el respeto por los derechos humanos"

KOFI ATTA ANNAN



(08 04 38 – 18 08 18)

PREMIO NOBEL DE LA PAZ 2001

AGRADECIMIENTOS

Es importante para mí, agradecer a todos los que me han estimulado y apoyado en este recorrido, que concluyo con esta primera etapa de formación.

A mis padres Aldo y Melania, principales destinatarios de este mérito, quienes siempre me han aconsejado y estimulado en el camino del conocimiento y superación en diferentes áreas; a Juan Manuel, quien no dudó en acompañarme en este desafío, tolerando mis impaciencias y mis noches de estudio y compartiéndome su intelecto. A mis amigos en especial a Joi quien siempre supo celebrar a distancia cada una de mis conquistas, a mi hermano Ulises quien escuchó mis monólogos en mi ejercicio de aplicación de conceptos (pero me suplicó que luego de esta entrega me abstenga de hablarle de derecho, por lo menos 72 horas), a Paola quien colaboró y me acompañó madrugadas para cerrar este capítulo universitario. Tampoco puedo dejar de nombrar a Jack, presente en esta aventura con su incondicional afecto. A Javier quien sin resistencia, atendió a mis (que no fueron pocas) consultas técnicas de programación, donde la entrevista se volvió un interrogatorio.

Académicamente, a quienes supieron potenciar mi interés y compromiso, quienes desde primer año me alertaron de la importancia del modo de incorporación de conceptos. A mi tutor, quien me alentó y se mostró enteramente a disposición desde mi propuesta de elegirlo.

A la universidad y sus autoridades, por el despliegue realizado en un contexto de pandemia, cuando parecía verse frustrada la posibilidad que durante el 2020, pueda concluir con mi formación.

Y por supuesto a mis compañeros de cursada que han tolerado en cada una de las materias a esta alumna que constantemente insistió en evacuar inquietudes. A Nina, que llenó de color y post it el inaudito 2020 que compartimos y supimos transitar.

A todos ellos es a quienes le dedico esta primera experiencia investigativa.

Sin conexión a Internet

Prueba a:

- Comprobar los cables de red, el módem y el router
- Volver a conectarte a una red Wi-Fi
- Ejecutar Diagnósticos de red de Windows

ERR_INTERNET_DISCONNECTED

INDICE

TÍTULO 1

INTRODUCCIÓN

TÍTULO 2

DESARROLLO

CAPÍTULO 1

CIBERCRIMEN

CAPÍTULO 2

CIBERESPACIO

¿UN NUEVO LUGAR?

CAPÍTULO 4

DELITOS PLURIOFENSIVOS
"INGRESO" DE BIENES JURÍDICOS AL ESPACIO FÍSICO VS. VIRTUAL

CAPÍTULO 5

CIBERESPACIO Y ÁMBITO DE VALIDEZ ESPACIAL

TÍTULO 3

CONCLUSIÓN

ANEXOS

TÍTULO 1

INTRODUCCIÓN

1. PALABRAS PRELIMINARES

Desde el comienzo de mi carrera en el año 2017, siempre ha sido de mi interés el ámbito del Derecho Penal y una "nueva" modalidad delictiva –CIBERCRIMEN–. Conductas Humanas, y en algunos casos a priori no humanas de la mano de la Inteligencia Artificial, las cuales se despliegan en un nuevo escenario –CIBERESPACIO–.

La evolución en el campo digital de la tecnología, exige apartarse de dogmas sostenidos hasta el momento, y requieren su comprensión técnica para una mejor tutela, provocando nuevos análisis y alianzas.

Intento con este trabajo, no aferrarme a teorías ya conocidas desde el universo jurídico, sino lograr entrelazar lo que se desprende de ese universo virtual paralelo en el que habitamos todos los días, que trae aparejado eventualidades delictivas que le son propias.

El proceso ha sido largo, inquietante, y he pasado por diferentes procesos, replanteos, selecciones y decisiones buscando no apartarme de la intención de brindar una perspectiva personal y el planteo de interrogantes en busca de soluciones.

Como método he utilizado el deductivo cuantitativo, ya que a lo largo de la investigación recorro diferentes enfoques que plantea la doctrina en general, buscando concluir en soluciones que sean transversales a los diferentes puntos de vista planteados. También ha sido de gran aporte entrevistar que he tenido con diversos programadores que se desarrollan en diferentes ámbitos de aplicación de su conocimiento.

2. OBJETIVO

A través de mi investigación, busco recorrer primordialmente, el nuevo escenario objeto de comisión delitos, a consecuencia del avance de la tecnología –CIBERCRIMEN–. La finalidad, advertida como la necesidad de mejor comprensión de algunos términos, a fin de dar herramientas para que no se transforme en algo de comprensión inalcanzable, y desde allí como operadores de derecho, comenzar a transversalizar las herramientas hoy existentes, y vislumbrar las necesarias a los fines de mitigar esta clase de delitos, que inesperadamente u oportunamente en el contexto de pandemia junto con la violencia de género han estado a la orden del día.

El derecho penal como ultima ratio, necesita que anticipemos y minimicemos el impacto que termina recayendo en la jurisdicción como última oportunidad de reparación.

La Era del Conocimiento, y su homónima economía, donde las tecnologías de la información y de las comunicaciones (TIC) han producido una mutación social, con innumerables ventajas de comunicación social transnacional, universal y en permanente evolución tecnológica que a su vez apareja nuevos problemas e interrogantes que requieren una respuesta jurídica.

Asimismo, analizar el ciberespacio, quien se perfila como un nuevo ámbito de oportunidad criminal, obliga a su comprensión, apartándose de ciertos dogmas, y explorándolo como un nuevo "territorio virtual", hoy conocido por pocos, el cual parece ser infinito e "inmortal".

La Inteligencia Artificial, tendrá su merecido lugar en esta investigación en sus aspectos positivos y negativos.

Es mi intención, explorar desde la orientación profesional, acortar la distancia en el manejo de ciertos tecnicismos, para aplicarle a ellos mejores defensas y propuestas desde un horizonte jurídico. El derecho regula conductas, que van alterándose y modificando.

3. HIPÓTESIS

El cibercrimen, irrumpe en la sociedad internacional como una nueva modalidad delictiva, que requiere un recorrido de investigación impensado para una futura operadora de derecho. El derecho penal como *ultima ratio*, no parece ser suficiente.

Comprender las conductas delictivas mutantes desplegadas en este escenario emanada de la evolución tecnológica, plantea examinar el ámbito de oportunidad para la delincuencia.

Resolver sobre la existencia o no de un territorio, la suficiencia normativa en la materia. Un nuevo escenario, acaso un nuevo territorio? Aspectos que indudablemente se vinculan a políticas criminales que no lo contemplaban, parece ser el banquete de los delincuentes para operar desde cualquier punto geográfico del planeta estando en el a priori –no lugar–, manipulando la tecnología para conseguir una reservada y hasta anónima autoría.

En este sentido, capitulare algunos preceptos que abrirán un conglomerado de interrogantes, siendo que muchas veces, vale una mejor pregunta, a una conocida respuesta. La existencias de dogmas en derecho vs. la evolución tecnológica.

Recorrer selectivamente la modalidad delictiva, el escenario nutrido en elementos que hasta este trabajo conocía intuitivamente, la inteligencia artificial como conducta o inconducta

humana, las normas y el "ingreso" de los bienes jurídicos al espacio físico y virtual, y el ámbito de validez espacial del derecho penal, buscando aciertos y diferencias.

El recorrido sin duda será una experiencia para en un futuro profundizar y mejorar desde mi óptica actual.

TÍTULO 2

DESARROLLO

CAPÍTULO 1

CIBERCRIMEN

1. INTRODUCCIÓN

Con el avance de la tecnología, la informática y en especial con internet, implicó la aparición de nuevos paradigmas en materia de procesos de comunicación masiva. Internet se transformó en una fuente de información mundial, mutando nuestras relaciones sociales, como nuestro vínculo con el trabajo y nuevas formas de ejecución como el Teletrabajo o también llamado Home Office; nuestras relaciones de consumo; nuestras formas de comercio; salud; educación y seguridad entre otros.

Por tanto, el avance significativo respecto de la capacidad de procesamiento de toda información disponible y en -real time- que se origina de manos de internet causando una "*hiperconexión*", y también de la inteligencia artificial– A.I., del inglés "*artificial intelligence"*- (a la cual destinaré un capítulo de mi trabajo), importan ser los elementos fundantes de un nuevo universo que día a día evoluciona más rápidamente de lo que el ser humano es capaz de advertir desde su universo físico. Involucrando escuetos jugadores como proveedores de servicios, distribución, y gestión, sumado el contenido y por supuesto usuarios.

Una hiperconexión acelerada, que provoca una adaptación constante y mutante que escapa a la capacidad humana –más aún en ciertas franjas etarias– y por tanto requiere, anticipar y contener los límites, que inclusive desde una mirada legal significa una evolución final de la capacidad o incapacidad de la humanidad. ¿Estaremos entonces en situación de revertir o invertir procesos en curso?

No es la primera vez que el mundo ha pasado por diversos avances científicos que se han convertido en instrumentos tecnológicos, y cuya transferencia a todos los sectores sociales ha producido significativos cambios sociales, económicos y políticos, entre otros. Claras manifestaciones de estas transformaciones a lo largo de la historia de la humanidad son la rueda (4000 a.C.), la vela cuadrada (1300 a.C.), la imprenta (1450 d.C.), los computadores (1941 d.C.) y el internet (1969 d.C), con méritos muy significativos en los distintos procesos de desarrollo y avances en los procesos de globalización y de regionalización como reflejo este último de la actualidad. Cuestiones que plantearé en pocas líneas en el acápite de vinculación entre el derecho y la informática.

El derecho, desde una mirada trialista[1] no ajeno a la captación de lo que ocurre en la dimensión sociológica tuvo que aggiornar sus instituciones a los fines de describir, prever y regular las conductas sociales materializadas en los mencionados procesos, por medio de herramientas que permitan reglamentar aquellas conductas que puedan resultar penalmente reprochables, en el ejercicio del poder punitivo estatal.

Por lo tanto, considerando que el derecho es un regulador de las conductas sociales a los fines de establecer un orden, no le es ajeno a nuestro conocimiento, la aparición de nuevas conductas que requieren ser captadas para así alcanzar su tipificación en el ámbito normológico (legal) y su ulterior sometimiento a la dimensión dikelógica (valoración) en caso se vean quebrantadas las normas.

Paradigmas que involucran el estudio de nuevos tipos penales, llamados "informáticos"; a la vez que analizan el cibercrimen y la necesidad de crear herramientas para la efectiva investigación en entornos digitales.

Es por ello, que nuestro derecho positivo, se ve forzado a examinar características y problemáticas que representan las normas que regulan los delitos cometidos en nuestro país a través de medios digitales.

Este fenómeno, que se puede denominar "digital" en oposición hasta su aparición, entendidas como "analógicas" provocó la sanción de diferentes leyes, a mi criterio a modo de "parches" o enmiendas como ser, la ley 26.388, sancionada en el año 2008, conocida como la ley de delitos informáticos, introduce nuevos tipos penales al Código Penal de la Nación vinculados al uso de la tecnología. Desatando una ulterior sanción en protección de los menores, para resguardos del conocido *grooming*, mediante la sanción de la ley 26.904, ampliándose luego a la ley 27.436, para perseguir la tenencia de pornografía infantil, que implico una modificación al artículo 128 del CP.

Asimismo, es dable destacar, que aún hoy existe la necesidad de rápidamente implementar no sólo nuevas leyes de persecución de estos nuevos delitos, sino también de formación en este tipo de conocimientos técnicos por parte tanto de los legisladores, operadores de derechos y porque no de la creación de nuevas Teorías Jurídicas, parafraseando a Luis Jiménez de Asua (1969) quien decía que: *"una Teoría que no sirve para la práctica, no es una Teoría; y una práctica sin Teoría, es mera rutina".*

[1] de Werner Goldsmith. Conocida como la **teoría trialista del mundo jurídico** o **tridimensionalismo jurídico**,

De aquí en más, abordaré el siguiente trabajo recopilando lo que se conoce hoy por cibercrimen, rescatando algunos conceptos técnicos necesarios para su mejor comprensión. Y no aleatoriamente, dejo como últimas líneas su vinculación con los DDHH, dado que más allá de términos que gustan abrazar a los que ahondan en esta materia, sean por estética o precisión, deberían ser la premisa, sin que por glosar términos, quede aislada de la necesidad de raudamente crear un sólido sistema jurídico, que los garantice. Por el contrario la expansión tecnológica, en cabeza de pocos, "gobernará" ante la ineficiencia de herramientas en la era del conocimiento, que un derecho positivo, amerita cambiar dogmas con carácter urgente.

2. SOCIEDAD E INFORMÁTICA

El término informática, proviene del francés "Informatique" que conjuga "Información" y "Automatique", como tratamiento automático/ o automatizado de la información.

Según el Diccionario (RAE) la Informática es el: *"Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras".*

Con la evolución de la tecnología y en especial con la introducción de la informática (luego explicaré sobre los elementos del sistema informático), se incorpora una herramienta que se destaca por su rapidez y eficiencia en el procesamiento de información, incluso más económico, y todo esto de mano de los ordenadores o computadoras en un principio, hoy extensible a otros "dispositivos". Siendo recién a mediados del s. XX, cuando las computadoras para poder procesar la información, primero como grandes terminales, que hoy hasta cabe en un reloj pulsera.

Cuando hablamos de evolución y también revolución[2], puedo remontarme a la **Era Industrial,** la que impacta en la sociedad por traer valores fundamentales como ser la producción, el capital financiero y el mercado, focalizado en la producción de bienes y en la industria. Ahora bien, la informática como elemento de análisis que hace a mi investigación, comienza a tomar relevancia a mediados de la década del ´50 en la asistencia de ciertas actividades, generando una mayor eficiencia en diferentes actividades como ser las bancarias como empresariales en general. Es recién a finales de los '90 cuando el uso de computadoras -hasta entonces un privilegio de pocos- comienza a masificarse pasando a ser parte de la vida cotidiana de la sociedad en general, dando origen a la **Era De La Información,** implicando el

[2] Revolución y Evolución, persiguen un mismo objetivo, pero con distintas metodologías. La primera es a corto plazo, con cambios bruscos (pueden tener efectos colaterales irreversibles en la sociedad), mientras que la evolución también busca el cambio, pero a largo plazo y con impactos sociales menos agresivos.

traspaso de una economía basada en la producción de bienes y en la industria a otra fundada en la información -**Economía De La Información**-. Se basa en la comunicación y la información electrónica, a gran escala. Se habla de "capital de información y digital" o de "capital del conocimiento" ya que su sistema de producción, circulación y acumulación de conocimiento tiene un carácter digital. Así es como nace el proceso hacia una Sociedad Globalizada. Donde si bien el mercado sigue existiendo, aparecen las redes (Internet: "red de redes"), y el capital a diferencia de lo que sucedía en la era industrial deja de ser exclusivamente físico, tomando protagonismo los bienes digitales. Por lo tanto se produce una traslación de contenidos físicos hacia la información.

Una nueva **economía de conocimiento**, donde se monetizan actividades por medio de Internet a través de la obtención de datos de los usuarios. Mercado, dinero y capital ya son digitales, son paquetes de datos, de información, de conocimiento.

Así, comienza a hablarse de una Sociedad de la Información, siendo un paradigma en el cual las tecnologías facilitan la creación, distribución y manipulación de la información y juegan un papel esencial en las actividades sociales, culturales y económicas.

Entendiendo que el derecho, regula el comportamiento de los personas en una sociedad, es claro que el proceso transformador de la informática, influenció en el derecho de dos maneras, una de ellas entendiendo a la Informática como **instrumento** al servicio del derecho para optimizar el trabajo de los distintos operadores jurídicos; y la otra, como **objeto** del derecho, donde las tecnologías de la información y de las comunicaciones (TIC) han producido una alteración en el "ADN SOCIAL", la consecuencia además de las ventajas, plantea **nuevos problemas e interrogantes que requieren una respuesta jurídica**.

3. DELITOS ANALÓGICOS VS. DIGITALES

En el pasado siglo XX hasta hoy, la teoría científica del delito ha tenido como fundamento la imputación causal-objetiva y subjetiva al autor de conductas que ocurren en el mundo exterior, como la muerte de una persona, el hurto de objetos materiales fungibles como el dinero, el incendio forestal, entre otros.

A estos delitos que -como ya anticipé en la introducción- se pueden denominar analógicos y sobrellevaron importantes transformaciones materiales durante el siglo XX, por ejemplo a través de imputación objetiva, a los fines de precisar la imputación legal, delimitar y esclarecer el alcance particular del nexo de causalidad en los delitos comisivos sean dolosos o

imprudentes; como también el uso "masivo" de tipos penales de amenaza como de peligro, buscando proteger *ex ante* bienes jurídicos personalísimos. Sin dejar de lado los delitos vinculados con la tutela de propiedad intelectual o industrial (donde a mi criterio ingresa la inteligencia artificial, que desarrollaré más adelante).

Es a finales de los años '70, se produce el nacimiento de los delitos informáticos y los cibercrímenes (daños informáticos, transferencias no consentidas de activos, obstaculización de datos e infraestructuras informáticas, etc), lo que ha demostrado la existencia de una serie de factores dogmáticos y político-criminales que obligan a repensar e incluso replantear muchas de las nociones y categorías entendidas como dogmáticas tradicionales.

Existe la necesidad no sólo de tipificar conductas, sino de **reformular un nuevo paradigma delictivo**, que tiene como principales características la virtualidad y el empleo medios tecnológicos avanzados en una sociedad que intempestivamente ha sido modificada digitalmente.

Son delitos que, **indudablemente lesionan o ponen en peligro efectivo la confiabilidad, la integridad y la disponibilidad de los datos, los sistemas y las infraestructuras informáticas necesarias para el adecuado funcionamiento social.**

Son conductas punibles que tienen ocurrencia en un "lugar" o **ámbito deslocalizado** como el ciberespacio o la Web. Más adelante daré atención a la validez del ámbito espacial del derecho penal**, ¿existe un nuevo concepto de "territorio"?**

Sin intentar desmerecer las ventajas que este nuevo ámbito que no conoce fronteras, sino atender la urgencia, desde la perspectiva que merece y no intentando adaptar las conductas que en él se desarrollan a lo existente (analógico). Es claro que la tecnología en manos de internet (a posteriori trataré técnicamente), ha beneficiado la gestión social globalizada en aspectos políticos, sociales y económicos, pero también conlleva nuevos riesgos delictivos que se reproducen en una sociedad hiperconectada, mediática y altamente vulnerable por su **analfabetismo digital, riesgos que se caracterizan por ser automáticos, descentralizados, masivos y técnicos, que no resultan comunes a los delitos físicos tradicionales, y cuyo estudio y aplicación −difícilmente− se satisface con la teoría del -delito analógico-. Como lo precisa Miró Llinares: "El ciberespacio es para las relaciones sociales, en ese sentido, tan real como el meatspace** (que es un término utilizado para referirse al espacio físico frente al ciberespacio) y todos los comportamientos socialmente identificables que no requieren de un contacto físico directo pueden realizarse en él del mismo modo que en el espacio físico; esto es solo lo cualitativo, pues, en lo cuantitativo, el

ciberespacio también potencia la capacidad de las personas para el contacto social al derribar las barreras del espacio físico".[3]

Así las cosas, exige atender este paradigma desde un punto de partida que deja a relieve una nueva modalidad criminal, y sumar una nueva definición de delito que excede al mundo físico y por lo tanto más compleja, técnica y especializada. Si tomamos en cuenta la teoría del delito como sistema de filtros, al referirnos a la acción, en este caso son comportamientos que involucran una complejidad de sus elementos típicos objetivos y subjetivos, sobre todo de la acción y sus 'resultados' en relación a este nuevo fenómeno social.[4]

Por otra parte, podemos decir como esboce en la introducción, modifica el concepto de sociedad deconstruida y reconstruida como una sociedad digitalmente alterada, estribando su funcionamiento en la gestión de la información, los datos y las infraestructuras informáticas necesarias para la subsistencia e interacción de sus miembros. Lo que apareja la consecuencia de captar las conductas desde otra perspectiva (ya no la analógica), para su correcta persecución.

Es evidente que, los datos informáticos y las bases de datos (con su ley desde el año 2000 ampliada años más tarde con otras normas vinculadas al tratamiento entre otros), son activos sociales de primer orden, por ser parte de la forma en que los seres humanos se relacionan con su entorno. En las últimas décadas hemos pasado de un mundo donde prevalecen los medios analógicos (diarios, revistas entre otros) a un despertar digital caracterizado por el incremento de un contexto social de **hiperconexión digital**, dando **surgimiento a sociedades y colonias virtuales** que permiten una mejor organización de la democracia deliberativa y participativa, y del ejercicio del control no institucional a las instancias públicas (Facebook, Twitter, etcétera).

Lo antes mencionado, refuerza la idea de **proteger la seguridad de la información como un bien jurídico** de naturaleza intermedia, que permita tutelar llegado el momento, otros derechos constitucionales y bienes jurídicos como el patrimonio económico, la intimidad personal y la autodeterminación informática. Cuestión no sólo es tratada desde el aparato estatal, sino también abordada desde el ámbito privado a lo que se denomina **ciberseguridad** (que también alcanza a la esfera estatal) y recientemente con la **ciberdefensa,** entendida en breves palabras esta última como la adopción de medidas que anticipen la concreción de un

[3] Miró Llinares, Fernando, (2016). "La cibercriminalidad 2.0: falacias y realidades", (pp. 58-59), Madrid, España.

[4] Enrique Pérez Luño, Antonio, (1996). "Manual de informática y derecho", (p. 75), Barcelona, España.

ciberataque por parte de actores diversos, como así también la respuesta ante incidentes que afecten intereses nacionales vitales y que comprometan la soberanía nacional.

Por último, tales avances tecnológicos complejizan cada vez más la delimitación de las categorías dogmáticas de la conducta punible, como estructuras jurídicas que permitirían revelar mejor estas nuevas formas de criminalidad. Por ejemplo, el contexto de comisión tecnológica, la conexión cibernética, el automatismo, la virtualidad, la deslocalización y desregulación del ciberespacio, la triada informática (Hardware, software y usuario) y los datos inmateriales, no son conceptos que se encuadran perfectamente con una teoría del delito pensada para acciones causales lineales que producen resultados ontológicos en el mundo real, porque, no se estaba pensando en la ciberdelincuencia cuando se desarrollaron la mayoría de las teorías criminológicas, y tampoco las teorías del crimen, pues los presupuestos negados y los datos aportados para hacerlo hacen siempre referencia a la delincuencia "física".[5] **Es por ello que me refería anteriormente, que ya no se puede solucionar esta demanda con "parches o enmiendas legales".**

Lo antedicho, anticipa que no resulta convincente construir la categoría del cibercrimen a partir de una noción ontológico-normativa pura que a pesar de contar con un cierto rendimiento en el análisis valorativo y normativo de la imputación de delitos clásicos, no consigue explicar todo lo que existe o sucede en una realidad simulada, porque no solo no incluye todas las potenciales formas de objetos y métodos lógicos, sino que tampoco resuelve de forma hábil y práctica todos los problemas que se producen a partir de la informática en la realidad criminal.[6]

4. CONCEPTO

El término cibercrimen o delitos informáticos se utiliza para expresar la característica esencial de esta forma delictiva diferenciada de otras. Cabe hacer una distinción en delito y crimen, donde si bien son utilizados como sinónimos, no es tan así, podemos decir que la relación entre ambos es de género - especie, dada por la gravedad de la conducta, siendo el crimen un delito más grave técnicamente hablando, como lo ilustra el caso de los crímenes de lesa humanidad. Teniendo en cuenta que el delito (como género) es toda acción expresamente estipulada y penada por la ley, y será el legislador en el afán de proteger determinados bienes jurídicos, le otorga a esa conducta el carácter de reprochable, y sancionable por su

[5] Miró Llinares, Fernando, (2016). "La cibercriminalidad 2.0: falacias y realidades", (cit, p. 72).

[6] Posada Maya, Ricardo (2017). Nuevo Foro Penal No. 88, Universidad EAFIT: El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual, (p. 72 - 78).

ordenamiento jurídico. Pero no radica aquí la cuestión que intento abordar, de lo contrario son tan amplios los caminos que se abren en este proceso investigativo, que por algún lado debo comenzar a delimitar en esta primera práctica en mi carrera profesional.

La particularidad, está dada por el nuevo ámbito o espacio, el cual posee características estructurales intrínsecas y extrínsecas, diferentes al espacio físico en el que se ejecuta la delincuencia tradicional, o que también me gusta denominar analógica, exigiéndose un análisis y estudio de la conducta específica para la persecución y prevención de las mismas.

Es dable destacar que además del elemento característico, desde donde se realiza la conducta -ordenadores- (hardware), surge el hecho de que tales sistemas informáticos están conectados en un ámbito de comunicación transnacional-universal, el ciberespacio, importa no solo el nuevo escenario -ciberespacio- sino que puede ejecutarse desde cualquier espacio físico "tocando" diferentes ordenamientos jurídicos, trascendiendo en lugares distintos y simultáneamente, a bienes jurídicos tan diversos.

La definición dada por la OCDE de 1983 y adoptada en Argentina por el grupo de trabajo sobre comercio electrónico y comercio exterior del Ministerio de Economía y Obras y Servicios públicos en su informe preliminar sobre la materia de septiembre de 1998. Se entiende por cibercrimen, ciberdelito o delito informático a ***"Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos".***

Por otra parte, **las Naciones Unidas** se refiere al Cibercrimen, separándolo en **tres tipos penales**:

1. Los fraudes cometidos mediante la utilización de computadoras;
2. Manipulación de los datos ingresados;
3. Daños y perjuicios o modificaciones de programas o datos computarizados.

Por su parte la doctrina también hizo su distinción en dos grandes grupos. El primero referido a los delitos informáticos de carácter económico, siendo aquellas conductas disvaliosas en las que sea mediante el uso de un sistema informático como herramienta, o tomando al sistema informático como objeto de la acción disvaliosa, se produce un perjuicio patrimonial. Mientras que el segundo referido a los delitos informáticos contra la privacidad: constituyen un grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos. Incluso la expansión y evolución cada vez más veloz de la informática ha hecho que sucedan delitos que van más allá de los dos tipos de delitos antes mencionados.

Lo antedicho nos permite arribar a una definición que sostiene nuestra nación. donde se entiende por Cibercrimen a *"cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos".*

De todas formas, ya quedó expuesto, que el término a utilizar para definir estas conductas, es **dinámico.**

5. El DEBATE

Si bien existen debates en relación a los términos utilizados, los cuales a priori parecen ser de índole estética o por ser pionero en abrazar uno de ellos, generalmente buscan contar con algún elemento comunicativo que exprese o refleje mejor el concepto.

En un primer momento, se utilizada la denominación de delitos informáticos mientras que ahora se opta por la de cibercrimen, en referencia al término anglosajón *cybercrime*, como unión entre el prefijo *cyber*, derivado del término *cyberspace*, y el término *crime*, concepto válido para englobar la delincuencia relacionada con el uso de las Tecnologías de la Información y la Comunicación[7] (TIC), siendo éste el que viene imponiéndose a otros, tales como *computer crime*, o bien haciendo uso de prefijos tales como *virtual, online, high-tech, digital, computer-related, Internet-related, electronic, y e-crimes*.

Aún hoy, el que parece ser más descriptivo de esta clase de delitos es el término cibercrimen, por expresar la característica esencial que une a esta forma de criminalidad diferenciándose de otro tipo de delincuencia. Siendo lo relevante el nuevo ámbito o espacio con características estructurales intrínsecas y extrínsecas diferentes a las dadas en el espacio físico donde se ejecuta la que podemos denominar "delincuencia tradicional".

Esta situación más allá de la terminología, tiene como consecuencia y necesidad la revisión criminológica de la explicación del evento delictivo, y por supuesto una adaptación de las normas jurídicas para su mejor prevención, que viene dándose significativamente en diferentes ordenamientos.

[7] **TIC** concepto dinámico, extensivo para la tecnología de la información que enfatiza el papel de las comunicaciones unificadas y la integración de las telecomunicaciones (líneas telefónicas y señales inalámbricas) y las computadoras, así como el software necesario, el middleware, almacenamiento y sistemas audiovisuales, que permiten a los usuarios acceder, almacenar, transmitir y manipular información. TIC es un término general que incluye cualquier dispositivo de comunicación, que abarca radio, televisión, teléfonos celulares, computadoras y hardware de red, sistemas satelitales, etc., así como los diversos servicios y dispositivos como videoconferencias y aprendizaje a distancia entre otros.

Anteriormente, la denominación delitos Informáticos o *computer crimes* cumplía con expresar la preocupación por un nuevo tipo de delincuencia que se instauraba con la aparición de los primeros sistemas informáticos, en la que estos sistemas eran el **medio** o el **objetivo** del crimen.

Por en cambio hoy, ya no interesa o basta con tener como elemento característico el realizarse desde ordenadores (ejemplo de falsificación de un documento por medio de hardware / software y usuario sin necesidad de estar conectado a una red), sino por el hecho de que tales sistemas informáticos estén conectados en un ámbito de comunicación transnacional-universal, el ciberespacio, y porque sea en ese nuevo "lugar" en el que, desde cualquier espacio físico ubicado en cualquier Nación, se cometen infracciones que pueden afectar, en lugares distintos y simultáneamente, a bienes jurídicos tan diversos como el patrimonio, la intimidad, la libertad y la indemnidad sexuales, el honor, la dignidad personal, la seguridad del estado, la libre competencia, entre otros muchos.

Al hablar de cibercrimen o cibercriminalidad, por tanto, lo hago para referirme a una macro categoría, paralela (aunque situada dentro de ella a la vez) a la de crimen o criminalidad, y únicamente diferenciada de ésta por no ejecutarse en el espacio físico, sino en el ciberespacio. Desde una perspectiva fenomenológica, incluye tanto los delitos que únicamente podrían ser realizados por la existencia del ciberespacio (o cibercrímenes puros, tales como el hacking, ataques DoS, infecciones de Malware, y demás que no existirían como infracciones de no hacerlo las TIC), como los delitos que tienen una modalidad de comisión en el espacio físico si bien en la concreta modalidad de ejecución en el ciberespacio (ciberfraudes de distinta naturaleza, ciberacoso sexual a menores, cyberbullying, cyberstalking, entre otros muchos), incluyendo dentro de éstos una particular, que podría ser tercera, categoría de infracciones, cuya ilicitud se caracteriza por la prohibición de la transmisión o difusión del contenido (pornografía infantil, hatespeech o difusión de mensajes de odio racial, ciberterrorismo, piratería intelectual en Internet, etc.); y todos ellos, bien sea la finalidad del cibercriminal la económica, política o ideológica social o personal, en el marco de la utilización de las TIC en la web 2.0 como instrumentos para las relaciones personales y la creación de redes y grupos sociales.

Sin dudas, cada una de estas grandes categorías, incluso cada uno de los crímenes, conlleva unas problemáticas criminológicas distintas. Tampoco debe olvidarse, y esto es ahora lo esencial, que a todos esos delitos les une algo que además, les va a caracterizar frente a los crímenes en el espacio físico, el lugar, nuevo, en el sentido de distinto, en el que se cometen.

6. CONCLUSIONES

Comprender su significado, y que el ciberespacio se configura como un nuevo ámbito de oportunidad criminal, obliga a repensar las estrategias de prevención de la delincuencia en él cometida desde el universo jurídico pero también sin caer en la última ratio, puede prevenirse adaptando las enseñanzas de la Teoría de las Actividades Cotidianas[8] (TAC) -a ese distinto "lugar" de comisión delictiva.

Es por ello, puedo arribar a la conclusión que el concepto más amplio es el de cibercrimen, como cualquier delito en el que las TIC juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que será tal cualquier delito (comportamiento humano que conforme a las normas jurídicas debiera ser enjuiciado como delictivo) llevado a cabo en el ciberespacio, con las particularidades criminológicas, "victimológicas" y de riesgo penal que de ello se derivan.

Por otra parte desde una perspectiva criminológica, existe la necesaria sustitución del vocablo "delitos informáticos"por los de cibercrimen y cibercriminalidad, al no centrarse el riesgo en la "utilización de tecnologías informáticas" o en la «información del sistema informático», sino en el sistema de redes telemáticas intercomunicadas, y en las interrelaciones que allí se configuran.

Mientras que la primera visión en sentido estricto, que ofrecía la criminalidad informática, estaba referida a una modalidad de delincuencia muy específica, con concretas tecnologías y reducidos usos de la misma. Hoy existe en cambio, un enfoque comprensivo de la cibercriminalidad como una delincuencia. En contrario sensu **es hoy toda la criminalidad cometida en el nuevo espacio**, al igual que la delincuencia tradicional es toda la ejecutada en el viejo o analógico. Se decide por un concepto amplio, variado y cambiante, el de cibercriminalidad, desvinculado de una concreta tecnología o bien de un determinado grupo de sujetos, incluso ni limitada a un sector concreto de la actividad social. Término que es comprensivo de todas aquellas conductas (cibercrimen) en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión (ciberespacio).[9]

[8] TAC: Se refiere a las Tecnologías del Aprendizaje y el Conocimiento que son las que incluyen a las TIC, más un componente metodológico necesario para que se genere un aprendizaje significativo. Además del uso de las TIC , los usuarios deben tener los conocimientos y habilidades necesarios para seleccionar y usar adecuadamente las herramientas para la adquisición de información en función de sus necesidades.

[9] Miró Llinares, Fernando, (2012). "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio", (pp. 37 - 38). Madrid, España.

CAPÍTULO 2

CIBERESPACIO ¿UN NUEVO LUGAR?

1. APROXIMACIONES: CIBERESPACIO. A PRIORI - NO LUGAR- PARA EL CRIMEN

Es el lugar, en este caso el -no lugar-, el que delinea y marca los eventos sociales en él realizados y el que configura también como distinta la delincuencia en él ejecutada.

Se suele utilizar como sinónimo de ciberespacio el concepto de "espacio virtual", como contrapuesto al espacio "real". La simultaneidad, la unicidad de momentos, puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea de espacio a la de distancia.

Es evidente, que el ciberespacio es real en el sentido de que existe, pero se trata de un nuevo espacio, invisible a nuestros directos sentidos y en el que las coordenadas espacio/tiempo adquieren otro significado y ven redefinidos su alcance y sus límites. El ciberespacio supone la contracción total del espacio (de las distancias) y, a la vez, la dilatación de las posibilidades de encuentro y comunicación entre personas.

Internet (término en el que haré hincapié más adelante) ha contraído el mundo acercando a un mismo lugar interactivo a personas que pueden estar en coordenadas espaciales separadas por miles de kilómetros. El espacio se contrae, la intercomunicación se expande. Y mientras que hasta el momento era necesario que las dos ocupasen (prácticamente) el mismo espacio para poder comunicarse, ahora pueden hacerlo al mismo tiempo (o en tiempos separados y en el mismo ciberespacio pero en distintos espacios geográficos (o a distancia).

Es el ámbito cambiante, y al parecer "inmortal", asociado al cibercrimen. Involucra desafíos de índole político criminal, de adaptación de todas estructuras, políticas, jurídicas y sociales, en atención de la necesaria protección de ya existentes y nuevos intereses frente a nuevas formas delictivas que son mutantes como también lo es el ámbito social en el que las mismas se producen.

Sin muchos artilugios, se puede decir que el ciberespacio es el ámbito, donde además de ciertas conductas lícitas (que no son objeto del presente estudio), se comete el cibercrimen comprendido como **el delito cometido en "el otro lugar", en el a priori no lugar.**

Es indubitable el carácter omnicomprensivo del término, ya que se entiende por **cibercrimen** a todo lo ejecutado en el **ciberespacio**.

Analizar el fenómeno del cibercrimen requiere, indudablemente, ahondar desde una perspectiva técnica esencialmente descriptiva de los efectos (en los sistemas y en las redes) y de las causas (en términos informáticos) de los distintos ciberataques. Es esencial adoptar una visión criminológica de la ciberdelincuencia en la que se analice la misma como lo que es: un evento social llevado a cabo por personas, individualmente o en grupo, con efectos sobre otras personas o instituciones sociales y ejecutado en un **nuevo ámbito de intercomunicación social que incide en las conductas, en quienes las realizan, sus efectos y en quienes sufren éstos**.

Por lo tanto, convertir el cibercrimen en un evento irremediable en el que **no** nos preguntamos por su **origen**, por las **causas** del mismo, por **quién** y **por qué** lo realiza, difícilmente nos ayudará a la prevención completa y real del fenómeno.

2. EL CIBERESPACIO. UN LUGAR DE COMUNICACIÓN SOCIAL TRANSNACIONAL

Las TIC (Tecnologías de la Información y la Comunicación) en general, e Internet como red global, en particular, han supuesto la creación de un **lugar de comunicación social transnacional, universal y en permanente evolución tecnológica,** que ha sido denominado **ciberespacio** y respecto al cual es dable plantear si el mismo puede definirse como un nuevo ámbito de oportunidad delictiva, un contexto de riesgo criminal distinto al espacio nacional físico tradicional o, por el contrario, idéntico a éste en sus caracteres esenciales.

Existe una metáfora de Grabosky donde la cuestión es: ¿en qué sentido el cibercrimen *es "old wine in new bottles".* Puede serlo en el de constituir un tipo de delincuencia esencialmente nueva y respecto de la cual no son válidas las teorías criminológicas aplicables al delito llevado a cabo en el espacio físico-nacional o en el de tratarse de la misma delincuencia con un aspecto diferente, pero para la que son válidas las mismas teorías y los mismos instrumentos usados frente al crimen en el espacio físico; y también, por último, puede tratarse de una criminalidad con elementos configuradores idénticos, pero que se ven afectados, de forma esencial, al plasmarse en el ciberespacio de modo tal que ello puede influir significativamente en la explicación del delito y, por tanto, en su prevención.

Sin entrar todavía en el fondo de estas cuestiones sí puede adelantarse lo obvio: que el crimen, como cualquier otro evento social, cambia en Internet, por lo menos si integramos en la comprensión del evento el lugar en el que el mismo se produce.

Si como señalaran hace ya más de tres décadas Cohen y Felson, el crimen se produce cuando se unen en el espacio y en el tiempo un objetivo adecuado, un delincuente motivado y sin un guardián capaz de darle protección al primero, es evidente entonces que los especiales caracteres del ciberespacio, en los que se ven modificados los parámetros espacio-temporales, pueden incidir en una modificación de los condicionantes del delito.

Voy a tratar, por tanto, de analizar en qué cambia el ciberespacio, cuáles son las singularidades de ese nuevo espacio que conllevan a que cualquier evento social en él se caracterice de forma distinta a como lo es en el otro espacio de comunicación social; antes de tratar de adivinar cómo influye ello en el evento social que es el cibercrimen.

3. NUEVO Y "DISTINTO" ÁMBITO DE OPORTUNIDAD CRIMINAL

La hipótesis de partida es que el cibercrimen, como evento criminal, también depende de la presencia de los elementos constitutivos de la ecuación del delito; de un delincuente capacitado y motivado para ello; de un objetivo o víctima adecuada; de la ausencia de un guardián capaz, en la primera fórmula de la TAC; y de los demás elementos incorporados en las siguientes fórmulas, pero todos y cada uno, se ven modificados en algún sentido al darse en el ciberespacio. No de una forma tal que cambie su esencia, pero sí de modo que la confluencia de los mismos en el evento resulta distinta a la que define al crimen en el espacio físico.

Se trata, por tanto, de contrastar los elementos del delito con los caracteres intrínsecos y extrínsecos del ciberespacio para definir los rasgos más singulares de ese nuevo ámbito de oportunidad delictiva y en comparación con el otro ámbito de oportunidad criminal, el del espacio real. El resultado de tal comparación deberá servirnos para comprender las peculiaridades del cibercrimen que deben ser tomadas en consideración para definir los instrumentos de prevención del mismo. Voy a hacerlo de forma separada, dividiendo el análisis entre los elementos que conforman el triángulo del delito (tal y como quedaría con la primera configuración de Cohen y Felson), añadiendo a los gestores del lugar que se incorporan en el segundo triángulo y eliminando, por motivos obvios, al lugar (que es el propio ciberespacio).

Ello no significa que crea que se trate de elementos separados: a mi parecer la TAC aporta la idea de que para la comprensión del delito no sólo hay que mirar al agresor sino también otros elementos del evento, pero es obvio que todos los que lo conforman están interrelacionados, de modo tal que la propia motivación del agresor depende de los demás factores, así como el objetivo es definido como adecuado por la conducta del agresor, etc. El estudio separado de los elementos es, por tanto, meramente a efectos didácticos. El cibercrimen, como delito en el espacio físico, es la confluencia de las partes en el todo.

4. INCORPORACIÓN DE APROXIMACIONES TÉCNICAS

4.1. **INTRODUCCIÓN**

Antes de quedar inmersos en el mundo jurídico que se abre ante este nuevo escenario para el derecho, es importante destacar algunos conceptos técnicos que involucran y hacen posible, tanto facilitar la vida social y comercial como la delictiva.

Luego de, anteriormente, haber hecho hondada referencia al término cibercrimen, en el cual se involucra al ciberespacio también tratado, voy a hacer un breve recorrido sobre algunos conceptos relevantes de cómo el usuario (sea víctima o delincuente) se conecta formando parte de esa "constelación" integrada por internet, las webs y los diferentes software que "conversan" entre sí, como los dispositivos desde los cuales se opera.

4.2. **SISTEMA INFORMÁTICO: CÓMO Y DESDE DÓNDE INGRESAMOS**

Un sistema informático se compone de los siguientes elementos: un soporte físico, denominado Hardware; otro lógico, llamado Software; más la información y los usuarios, que paso a detallar.

Soporte Físico - Hardware: Conjunto indeterminado de elementos que permiten el ingreso (input) de datos, su recuperación, o egreso (output) por distintos medios (impresos,visual, sonoro, etc.) y su tratamiento automatizado por aplicación de tecnologías electrónicas y programas de computación. Es la denominada parte "dura" del sistema informático, conforme a su etimología "hard" (inglés) equivalente a "duro" (español). En pocas palabras son los diferentes "dispositivos" (computadoras, tabletas, teléfonos, relojes inteligentes, entre otros)

Soporte Lógico - Software (programa de computación): Conjunto de instrucciones en código binario que pueden ejecutarse en un soporte físico dado y posibilitar la obtención de información procesada de acuerdo a una finalidad dada. En contraposición al anterior elemento del sistema informático, esta es la parte blanda, "soft" en inglés.

Información y Usuarios: El destinatario final en los sistemas informáticos es el usuario. Por tanto, para que éste tenga utilidad se requiere que los soportes, lógico y físico, y la información procesada se adapten a un usuario determinado. De lo contrario, el Sistema informático puede no cumplir con la actividad que el usuario pretenda desempeñar, siendo por tanto inútil.

Aquí es donde aparece la rama del derecho que estudia este fenómeno y que tiene por objeto atender a las Tecnologías de la Información y la Comunicación (TIC) junto a Internet.

4.3. **INTERNET: CONECTÁNDONOS**

Podemos entender a Internet como una vía de comunicación efectiva que conecta a dos o más sujetos en incontables e ilimitadas posibilidades y que a través del uso de protocolos denominados TCP/IP (Protocolo de Transmisión / Protocolo de Internet) garantiza que las redes físicas heterogéneas que la componen funcionen como una única red lógica (de ahí percibida como la Red de Redes). Siendo, asimismo, una herramienta que comprende:

1. Nuevo espacio de expresión humana;
2. Espacio internacional que trasciende las fronteras;
3. Espacio descentralizado que ningún Estado domina por completo;
4. Espacio heterogéneo donde cada uno puede actuar, expresarse y trabajar;
5. Espacio de libertad.

Estas redes de computadoras interconectadas hacen posible tanto la comunicación como el intercambio de archivos entre usuarios; facilitando el nacimiento de situaciones y relaciones jurídicas.

4.4. **RED INFORMÁTICA. PUNTO INICIAL A LA RED DE REDES: HIPERCONEXIÓN**

Una **red informática** es un sistema de comunicación donde los elementos que la componen (por lo general ordenadores), autónomos e interconectados entre sí por medios físicos y/o lógicos, actúan de emisor y de receptor de manera alterna.

Independientemente a esto, definir el concepto de red implica también, diferenciar entre el concepto de red física y red de comunicación.

Mientras los modos de conexión **física**, los flujos de datos, etc. constituyen una red que comparte determinados recursos de hardware (impresoras, almacenamiento) o de software (aplicaciones, archivos, etc.), la **comunicativa** es aquella donde se encuentran involucrados un componente humano que comunica, un componente tecnológico (ordenadores, TV, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios).

4.5. **PROTOCOLO TCP/IP: UNA FAMILIA DIVERSA**

El protocolo denominado TCP/IP, o mejor dicho la familia de protocolos que se agrupan bajo este nombre, dado en referencia a sus dos componentes más importantes (Protocolo de Transmisión / Protocolo de Internet), permite que los dispositivos se comuniquen entre sí; abarcando una amplia gama de hardware y soportando distintos sistemas operativos. Es decir, es un protocolo multiplataforma.

Ahora bien, este protocolo que se define como un conjunto de normas —lenguaje de reglas y símbolos— establecidos convencionalmente, rige cada tipo de comunicación entre los ordenadores y permite que los mismos establezcan una red, definiendo además, la forma en que se comunican dentro de ésta, desde que se envían los datos hasta que son recibidos.

Para lograrlo utiliza un sistema de capas, en el cual cada capa se construye a continuación de la anterior y se comunica únicamente con su capa superior, a la que envía resultados, y con su capa inferior, a la que solicita servicios.

Este conjunto de protocolos es el modelo que se utiliza para acceder a Internet o a redes internas (Intranet) y se compone, entre otros, por los siguientes:

1. TCP (Protocolo de Control de Transmisión): Es el creador de las conexiones a través de las cuales pueden enviarse un flujo de datos, garantizando que éstos llegarán a destino y en el orden propuesto;
2. IP (Protocolo de internet): Es un identificador numérico que se asigna de manera única a cada ordenador conectado a Internet;
3. ARP (Protocolo de Resolución de Direcciones): Es el responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP;
4. POP (Protocolo de Oficina de Correo): Es el que se utiliza para hacerse de los mensajes de correo electrónico, alojados en un servidor remoto;
5. SMTP (Protocolo para Transferencia Simple de Correo): Es el que usamos a la hora de transmitir mensajes de correo electrónico;
6. HTTP (Protocolo de Transferencia de hipertexto): Es el utilizado para descargar una página web desde el lugar en el que esté almacenada;
7. FTP (Protocolo de Transferencia de Archivos): Es el que se emplea para el intercambio de archivos;

8. DNS (Sistema de Nombres de Dominio): Es el encargado de asignar un dominio a una dirección IP; [10]

9. PPP (Protocolo Punto a Punto): Es el protocolo que establece una conexión directa entre dos nodos de una red.

Si bien, todo este conjunto de resoluciones permiten, entre otras cosas, conectar ordenadores de manera efectiva, algunos elementos de la red de comunicación, como los cortafuegos (firewall), pueden llegar hasta las capas superiores para detectar ataques o filtrar contenido. [11]

4.6. **VPN. RED PRIVADA Y "GPS RECALCULANDO"**

Una VPN (Red Privada Virtual) es una red que evita que el ordenador se pueda rastrear; creando una conexión segura y encriptada desde un ordenador a otro ordenador —que actúa como servidor— permitiéndole navegar por Internet a través de su conexión. De esta manera, una parte del tráfico se envía cifrado y seguro mediante este nuevo túnel de comunicación.

El uso de una VPN permite acceder a recursos restringidos en redes privadas de empresas e instituciones; ocultar datos de navegación si se está utilizando una red pública; el acceso a redes de trabajo o redes hogareñas remotamente; y también evitar la censura a determinados servicios o contenidos que por ejemplo, muchos gobiernos restringen como es el caso de China.

4.7. **PROTOCOLO IP: NUESTRO DNI VIRTUAL**

El protocolo IP (Protocolo de Internet) es aquel que identifica, de manera única, a cada equipo que se encuentra conectado a la red mediante su correspondiente dirección numérica.

La dirección IP es una dirección numérica de 32 bits expresada en cuatro números de 0 a 255 separados por puntos, por ejemplo: 208.70.965.226; se utiliza para identificar tanto al procesador como a la red a la que éste pertenece. Es así que se divide en dos partes: una dirección que identifica a la red y una dirección que identifica al ordenador dentro de ella.

[10] DNS Inicialmente, el protocolo que identificaba a las máquinas conectadas a la red ARPANET, consistía en un código numérico. El crecimiento, desmilitarización y apertura de las redes, la necesidad de un código numérico (finito) para cada computadora complicó su identificación, siendo el momento cuando se crea este protocolo.

[11] China bloquea Whatsapp, independientemente de cuestiones políticas dadas por la proximidad del Congreso del Partido Comunista, donde la ACC (Administración del Ciberespacio de China), de alguna forma lanza una campaña contra los servicios de VPN. Permiten a los usuarios acceder a páginas censuradas por las autoridades.

No pueden existir en una misma red, y por lo tanto en Internet, dos dispositivos conectados con una misma dirección IP; aunque sí se pueden repetir en redes privadas no conectadas entre sí.

La dirección IP es, entonces, una identificación única y exclusiva para cada equipo conectado.

5. TEORIA DEL ICEBERG – SURFACEWEB. DEEPWEB. DARK WEB

5.1. **DISTINCIÓN PRELIMINAR ENTRE WEB E INTERNET**

Internet es una inmensa red de computadoras alrededor de todo el mundo conectadas entre sí. En cambio, la **web** (World Wide Web) es una enorme colección de páginas que se asienta sobre esa red de computadoras. Es decir, que cuando navegamos a través de un dispositivo móvil o una computadora usamos **Internet** para acceder a la **web**.

Si bien los términos Internet y web están relacionados y son interdependientes son conceptos diferentes. A pesar de ello, son muchas las ocasiones en que las personas suelen confundir dichos términos, Internet y web, considerando erróneamente a ambos como sinónimos.

En principio, el surgimiento del Internet es previo al de la web. El Internet tuvo su origen en el año 1960, aproximadamente, con el nombre de ARPANet; tenía como fin dar una respuesta más rápida a la organización de datos y al uso de los equipos informáticos.

Para aquel entonces, la agencia de investigaciones avanzadas en Estados Unidos logró realizar con éxito la primera conexión entre dos computadoras, que más tarde fue empleada para usos gubernamentales y universitarios.

Años después, el científico británico Tim Berners-Lee desarrolló en la década de 1990 la World Wide Web, conocida como web, que es un sistema de transferencia de hipertextos a través de internet.

5.2. **¿QUÉ ES LA TEORÍA DEL ICEBERG?**

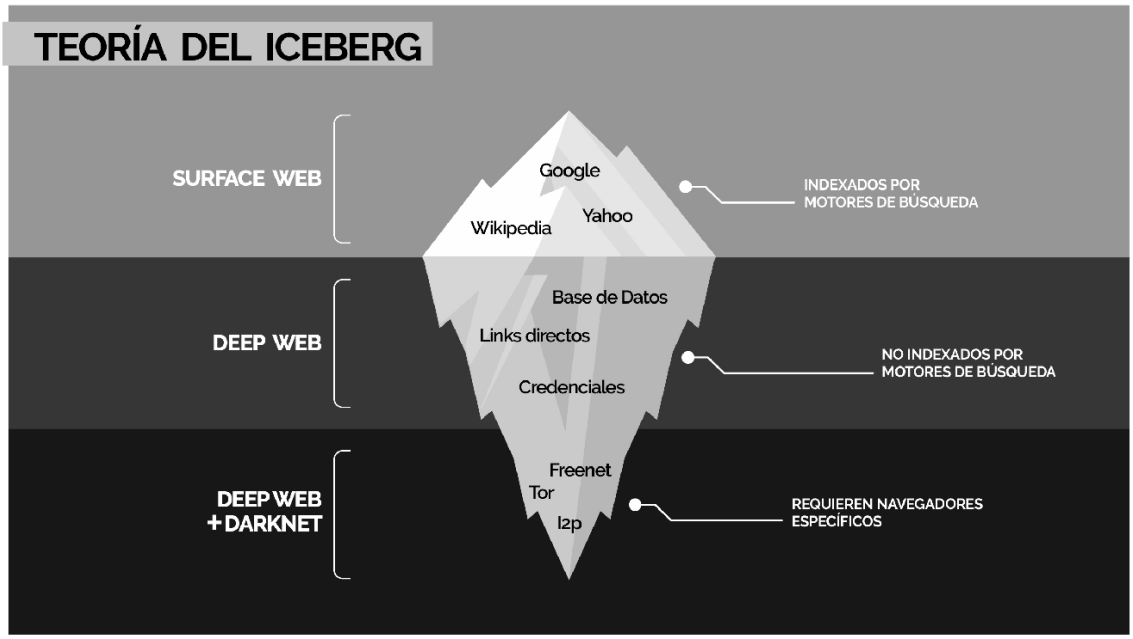
La teoría del iceberg es un teorema propuesto por Hemingway, que se basa en la percepción de la realidad y el cual nos dice que solo vemos el 20% del ICEBERG total y debajo del agua se encuentra el 80% restante.

Esta teoría ha sido vista desde diversos enfoques y aquí la vemos aplicada a la web, representada con esta imagen.

5.3. **TEORIA DEL ICEBERG APLICADA A LA WEB**

Mi intención, es vislumbrar, la cantidad de conductas que se suceden en la web, y cómo en cada una de las "capas", va *in crescendo* la voluntad del actor, para la comisión de los delitos. Asimismo, colabora a un mejor análisis de todo lo vengo tratando en relación al nuevo y denominado CIBERESPACIO.

Términos como SurfaceWeb, DeepWeb, DarkWeb y Darknet son muy utilizados hoy en día, pero muchas veces las personas los usan de manera incorrecta; por ejemplo, la DeepWeb siempre fue catalogada por contener información y contenido ilegal, pero esto no es del todo cierto.



5.3.1. SURFACEWEB O WEB SUPERFICIAL

En español significa "Red limpia" o "Red superficial". Es la web conocida por la mayoría de las personas; donde las direcciones IP son fácilmente rastreables e indexadas por buscadores convencionales como Bing o Google y a la que podemos acceder utilizando cualquier navegador web. Además está compuesta por todas las páginas y servicios como Facebook, Youtube, Twitter, blogs, entre otros.

Hoy en día es complicado estimar la cantidad siquiera aproximada de las páginas existentes en la SurfaceWeb. Aun pudiendo conocer este enorme número la web superficial solo se trata de una parte muy pequeña del espacio de datos en Internet.

Asimismo, el hecho de ser fácilmente rastreable permite atender cuestiones de efectos y resultados, en relación al derecho aplicable, en caso se identifique una conducta delictiva.

5.3.2. DEEPWEB O WEB PROFUNDA

El término fue empleado por primera vez, en 1994, por Mike Bergman, informático de Bright Planet (empresa especializada en indexado web), con la desmantelación de Silk Road (VER ANEXO 1 - SILK ROAD) a manos del FBI en 2013, salieron a la luz los negocios que se podían realizar en páginas web no indexadas como la venta de drogas, el tráfico de personas, la venta de armas, etc., motivo por el cual la prensa internacional empezó a usar el término DeepWeb para referirse erróneamente a acciones propias delictivas de la DarkWeb. pero el término se popularizó tanto al punto de confundir ambos conceptos.

Ya para el año 2010 se estimaba que al menos 200 mil sitios componían la DeepWeb. Datos más recientes aseguran que aproximadamente **el 90% de todos los sitios de internet forman parte de la web profunda (en atención a la teoría del iceberg de Hemingway planteada)**

Pero estas no son las páginas que solemos confundir con aquellas donde se venden o trafican ilegalmente (DARKWEB), simplemente puede tratarse de muros de pago, base de datos o archivos guardados en servicios como Google Drive, Dropbox entre otros.

El término fue utilizado, para describir contenido no indexable, es decir que su contenido no está incluido en el índice de buscadores de la web convencional como por ejemplo Google. Es necesario reconducir el tráfico con algunas trampas como servidores proxy o VPN que actúan como intermediarios para que nuestro rastro no pueda ser seguido.

Es importante destacar que no nació con esa característica de clandestinidad y peligro como la conocemos hoy en día (a pesar de su primer uso con el caso de Silk Road) , en sus inicios la DeepWeb era conocida por contener datos privados como por ejemplo repositorios en la nube de organizaciones o empresas, correos electrónicos, bases de datos remotas y hasta movimientos bancarios o reservas de viajes; toda esta información es claramente confidencial y generan archivos temporales que se almacenan en la DeepWeb.

Cómo no va a importarnos conocer sobre estos temas, si además de tener. Legislación en relación a los datos, contamos con una garantía constitucional como el Habeas Data.

5.3.3. DARKWEB o WEB OSCURA

La DarkWeb es otra porción de la web que no se ve (junto con la deepweb) cuyas direcciones IP están enmascaradas u ocultas de manera intencional y que solo pueden ser accesibles usando navegadores específicos (Onion Browser el más popular). Aún haciendo estas aclaraciones la DeepWeb y la DarkWeb son términos que han generado confusiones en la mayoría de las personas, a manera de analogía podría decirse que si la DeepWeb fuera como una ciudad la DarkWeb representaría los suburbios de dicha ciudad, los barrios o zonas más alejadas y de difícil acceso.

Estas páginas, que normalmente utilizan los dominios ".onion" o ".i2p" los cuales solo son accesibles con un **software especial** (por ejemplo TOR, i2p y freenet) que dan acceso a las Darknets en las que se alojan. Podemos decir que el TOR, navega como el Google Chrome, y onion tiene la función de "despistar".

Las "Darknets" son una colección de redes y tecnologías que suponen una revolución a la hora de compartir contenido digital, no obstante es cierto que por su naturaleza y su capacidad de anonimato han provocado que muchos usuarios aprovechen la tecnología para intercambiar contenidos o servicios no legales.

Se podría decir que la DarkWeb (contenido) es el equivalente al contenido de la World Wide Web (www), que existe en Darknets ("web propia").[12]

[12] La DarkNet es un término utilizado por primera vez en el año 2002 en el documento "The Darknet and the Future of Content Distribution", escrito por ingenieros de Microsoft, para referirse a un conjunto de redes y tecnologías que podrían cambiar la manera de compartir y acceder a contenido en Internet.

A su vez, TOR sigue siendo el más usado para ingresar a la Deepweb ya que tiene más cantidad de servicios. Todo ello gracias a su propio navegador que facilita comenzar a curiosear en "Hidden wiki", casilla obligatoria para comenzar a navegar por la Deep Web porque en ella se encuentra un directorio que permite explorar en las Darknets. En el Hidden wiki se encuentra una lista de enlaces actualizada a mano por los propios usuarios puesto que estas páginas cambian de IP y dominio frecuentemente.

Cabe destacar que existen páginas que se encuentran entre la Surfaceweb y la Deepweb, las cuales son las típicas páginas legales, pero que solo tienen indexado el título de la página ó no están indexadas dentro de los buscadores web.

En la Darkweb se puede encontrar páginas con servicios financieros para lavado de Bitcoins, cuentas robadas de Paypal o tarjetas de crédito. También se encuentra páginas de explotación sexual, mercado negro, armas robadas, municiones, droga, venta de documentación falsa y hasta pornografía infantil.

6. ESCENARIO E IMPACTO EN LA PANDEMIA: ASPO / DISPO

La aparición del virus conocido como COVID-19 originado en China en diciembre de 2019, y reconocido posteriormente como Pandemia, modificó y alteró aún más nuestra forma de comunicarnos.

Se implementaron restricciones y prohibiciones de movilidad, que nos llevaron a resguardarnos en nuestros hogares. El nuevo y forzado estilo de vida trajo como consecuencia el reemplazo de conductas desplegadas en el mundo real, a una intensiva "realidad virtual". Por otro lado, reactivó la hiperconexión, incluso en sectores de la sociedad que no la celebraban.

Si bien físicamente hemos transcurrido la mayor parte de nuestros días en nuestros hogares, habitamos, a consecuencia del aislamiento, el ciberespacio. La circulación cada vez menor, la ocupación de nuestros hogares mayor, y nuestras conductas ejecutadas en el mundo virtual o ciberespacio, incrementaron la criminalidad en este ámbito.

Por un lado, nos protegemos de un virus, que paradójicamente actúa de la misma forma que lo hace un virus informático o malware; y por otro, nos exponemos a un nuevo escenario delictivo.

Uno de estos ejemplos es el phishing, que permite hacer un paralelismo con "fishing", que significa "pescar" en inglés. Donde el "pescador" es el cibercriminal, su línea un correo electrónico o un mensaje de texto, y utiliza como "anzuelo" hipervínculos (enlaces o vínculos

que hacen referencia a otro recurso) y/o archivos adjuntos con algún recurso que capte la atención de su presa: el usuario.

Uno de los ejemplos más utilizados fue la circulación de mails y mensajes que utilizaban COVID-19 como carnada para ocultar el verdadero virus (el informático). El contenido de lo milagrosos correos era de suma atracción para el "pez" en la mira: curas mágicas, información para no contagiarse, mapas de contagio, entro otros; simulando que el contacto provenía de un organismo oficial, como puede ser la OMS o un ministerio de Salud, o un laboratorio de renombre invitando a acceder a un enlace (link / domicilio en la web) o a un archivo a descargar.

Esto trae un término llamado INGENIERÍA SOCIAL, que consiste en utilizar técnicas de manipulación psicológica para obtener información o para que el sujeto pasivo (el usuario) actúe de forma tal, que le produzca un perjuicio.

CAPÍTULO 3

INTELIGENCIA ARTIFICIAL (IA)
NOCIONES. APLICACIONES. INTERROGANTES

1. INTRODUCCIÓN Y APROXIMACIONES CONCEPTUALES

Se cree que los comienzos de la inteligencia artificial (IA de aquí en más) ocurrieron al definirse la neurona, en 1943, como un dispositivo binario con varias entradas y salidas. En el año de 1956, es cuando se acuña formalmente el término **"inteligencia artificial"** durante la conferencia de Dartmouth[13], donde se establecieron las bases de la IA como un campo independiente dentro de la informática. De todas formas, para entonces ya se había estado trabajando en ello durante cinco años en los cuales se habían propuesto muchas definiciones distintas que en ningún caso habían logrado ser aceptadas totalmente por la comunidad investigadora. La IA es una de las disciplinas más nuevas junto con la genética moderna.

En los años '60, la IA no tuvo mucho éxito, su viabilidad requería de mucha inversión, quedando acotada su desarrollo en manos de los grandes centros de investigación. Fue recién en las décadas siguientes que se lograron algunos avances significativos en una de sus ramas, los sistemas expertos.

Es menester recordar, que las ideas más básicas se remontan a los griegos, antes de Cristo. Aristóteles (384-322 a. C.) fue el primero en describir un conjunto de reglas que describen una parte del funcionamiento de la mente para obtener conclusiones racionales.

Por otra parte, continuando por el concepto, debe comprenderse que la **inteligencia** está vinculada a saber elegir las mejores opciones para resolver algún tipo de problema. Existen diversos tipos de inteligencia según sus atributos y procesos, como la inteligencia operativa, la biológica o la psicológica.

Mientras que **Artificial,** por otra parte, es un adjetivo que señala aquello hecho por mano, arte o ingenio del hombre. Lo artificial puede extenderse a lo no natural o falso.

[13] La Conferencia de Dartmouth, en inglés: Dartmouth Summer Research Project on Artificial Intelligence, siendo el nombre del encuentro que tuvo lugar en el verano de 1956 en la universidad Dartmouth College, ubicada en Hanover, Nuevo Hampshire (Estados Unidos), considerado como el evento germen de la Inteligencia Artificial como esfera o campo de actividad.

La noción de IA fue desarrollada en referencia a ciertos sistemas creados por los seres humanos que constituyen **agentes racionales no vivos**. Racionalidad comprendida como la capacidad para maximizar un resultado esperado.

La IA, consiste en el diseño de procesos que, al ejecutarse sobre una arquitectura física, producen resultados que maximizan una cierta medida de rendimiento. Estos procesos se basan en secuencias de entradas que son percibidas y almacenadas por la mencionada arquitectura (en manos de un ALGORITMO). Coloquialmente, el término inteligencia artificial se aplica cuando una máquina imita las funciones "cognitivas" que los humanos asocian con otras mentes humanas, como por ejemplo: percibir; razonar; aprender y resolver problemas.

Algunos expertos en la materia, que me pareció interesante compartir, aunque la lista podría ser infinita la definen como: *"la ciencia e ingenio de hacer máquinas inteligentes, especialmente programas de cómputo inteligentes*" En 1956, John McCarthy[14] acuñó la expresión en la conferencia de Dartmouth

"La capacidad de un sistema para interpretar correctamente datos externos, para aprender de dichos datos y emplear esos conocimientos para lograr tareas y metas concretas a través de la adaptación flexible", así definieron la IA, Andreas Kaplan y Michael Haenlein.

"Es una rama de las ciencias computacionales encargada de estudiar modelos de cómputo capaces de realizar actividades propias de los seres humanos con base en dos de sus características primordiales: el razonamiento y ***la conducta****".*

Los dispositivos en sentido amplio, que cuentan con IA pueden ejecutar distintos procesos análogos al comportamiento humano, como la devolución de una respuesta por cada entrada, similar a los **actos reflejos** de los seres vivos, la búsqueda de un estado entre todos los posibles según una acción o la resolución de problema mediante una lógica formal.

Esencialmente, la IA es aquella que trata de explicar el funcionamiento mental basándose en el desarrollo de algoritmos para controlar diferentes cosas. Combina varios campos, como la robótica, los sistemas expertos y otros, con un mismo objetivo, tratar de crear máquinas que puedan pensar por sí solas. Derivando en la existencia de varios estudios y aplicaciones, dentro de las que se encuentran las redes neuronales, el control de procesos o los **algoritmos genéticos.** (VER ANEXO 2 - IA)

[14] John McCarthy (1927-2011) fue un prominente informático que recibió el Premio Turing en 1971 por sus importantes contribuciones en el campo de la Inteligencia Artificial.

Por último, se dice que la IA es un campo que por sus investigaciones trata de ser independiente de la informática, definida como la técnica de software que los programas utilizan para dar solución a algún tipo de problema, pero tratando de asemejar el comportamiento inteligente que se observa en la naturaleza. Es decir trata de resolver problemas y tomar decisiones similares a las que toman los seres humanos al afrontar la vida diaria, realizando programas de computadora que aumenten la capacidad o "inteligencia" de las mismas; el objetivo de las investigaciones de la IA es, aumentar la utilidad de las máquinas y sus procesos.

2. ALGUNAS ÁREAS DE APLICACIÓN DE LA IA

Estos procesos de la AI se aplican en los sistemas reales en una gran variedad de ramas y problemas. Algo muy usual es el denominado **asistente automático** en línea dando servicio de atención al cliente en un sitio web, una de las muchas aplicaciones primitivas, de gran uso durante la pandemia.

Las técnicas desarrolladas en el campo de la IA son cuantiosas y ubicuas. Comúnmente cuando un problema es resuelto mediante IA la solución es incorporada en ámbitos de la industria y de la vida diaria de los usuarios de programas de computadora, pero la percepción popular se olvida de los orígenes de estas tecnologías que dejan de ser percibidas como tal, fenómeno al que se le conoce como el efecto IA.

A su vez se manifiesta en áreas de gestión y control; fabricación; educación; ingeniería: diseño, control y análisis; equipamiento; cartografía: profesiones: **abogacía; software;** sistemas de armamento; proceso de datos (educación, interfase en lenguaje natural, acceso inteligente a datos y gestores de bases de datos, análisis inteligente de datos, minería de datos -**Data Mining**- que anticipe en otro capítulo, el comercio de estos datos segmentados en la **DARKWEB**); Finanzas, entre otras de diferentes aplicaciones comerciales.

3. CRÍTICAS A LA IA

Las principales críticas a la IA están vinculadas con su **capacidad de imitar por completo a un ser humano.** Expertos en el tema, indican que ningún humano individual tiene capacidad para resolver todo tipo de problemas. En los humanos, la capacidad de resolver problemas tiene dos aspectos: los **aspectos innatos** y los **aspectos aprendidos**. Los aspectos innatos son aquellos que permiten ejemplo, almacenar y recuperar información en la memoria, mientras que en los aspectos aprendidos reside el saber resolver un problema

matemático mediante el **algoritmo** adecuado. Del mismo modo que un humano debe disponer de herramientas que le permitan solucionar ciertos problemas, los sistemas artificiales deben ser programados de modo tal que puedan llegar a resolverlos. (VER ANEXO 3 - TEST DE TURING Y LA IA)

Uno de los mayores problemas en sistemas de IA, se vincula a la comunicación con el usuario, obstáculo relacionado a la ambigüedad del lenguaje, que se retrotrae a los inicios de los primeros sistemas operativos informáticos. La capacidad de los humanos para comunicarse entre sí implica el conocimiento del lenguaje que utiliza el interlocutor. El humano tiene dos opciones para poder comunicarse con un sistema inteligente, o bien éste aprende el lenguaje del sistema como si aprendiese a hablar cualquier otro idioma distinto al nativo, o que sea el propio sistema quien posea la capacidad de interpretar el mensaje del usuario en la lengua que el usuario utiliza.

Un humano, durante su vida aprende el vocabulario de su lengua nativa, siendo capaz de interpretar los mensajes (a pesar de la polisemia de las palabras), apoyándose en el contexto para resolver ambigüedades. Sin embargo, debe conocer los distintos significados para alcanzar la interpretación, motivo por el cual ciertos lenguajes especializados y técnicos son conocidos solamente por expertos en determinadas disciplinas. Un sistema IA se enfrenta al mismo problema, la polisemia del lenguaje humano, su sintaxis poco estructurada, y los dialectos entre grupos.

Los desarrollos en IA son mayores en campos, en los que existe mayor consenso entre especialistas. Un sistema experto es más probable que sea programado en física o en medicina que en sociología o en psicología, donde se dificulta la creación de sistemas inteligentes porque siempre habrá desacuerdo sobre la forma en que **debería actuar el sistema** para diferentes situaciones. A pesar de esto, hay grandes avances en el diseño de sistemas expertos para el diagnóstico y toma de decisiones en el ámbito médico y psiquiátrico (Adaraga Morales, Zaccagnini Sancho, 1994).

Por su parte, dentro del ámbito de personalidades relevantes vinculadas a la "revolución digital" y en especial a la AI, como sostuvo **Stephen Hawking** quien advirtió sobre los peligros de la inteligencia artificial y lo consideró una amenaza para la supervivencia de la humanidad. Así como tampoco oportunidad para expresarse en torno a los temores y preguntas, **Bill Gates** (ex director general de Microsoft) y **Elon Musk** (director general de Tesla) opinan que la IA exige particular cautela; sobre todo prestando específica atención a ciertas aplicaciones sofisticadas, las cuales pueden llegar a tener derivaciones por completo impensadas, por constituir "nuestra mayor amenaza a la existencia".

4. DESAFÍOS PARA EL DERECHO. "TODO" ES ALGORITMO

El desafío para el derecho, impacta a mi parecer en el análisis de la conducta,entendida en la teoría del delito, como aquella realizada por el hombre, habiendo analizado en el comienzo de este capítulo, que las respuestas que un sistema de inteligencia artificial, como su nombre lo dice es artificial, es decir premeditada por intervención de la mano del hombre, cuando crea el algoritmo "madre" ¿Será la puerta entonces para que estas conductas "automáticas", sean entendidas como derivaciones de conductas humanas por el creador del algoritmo? será un camino de relevancia jurídica. Debido a esta hipótesis es que analizaré aspectos técnicos para su comprensión, y asimismo comenzando por la propiedad intelectual, siendo el lazo jurídico que abordaré y dejando planteado a modo de incógnita si es posible hacer un paralelismo con el tratamiento que se le da hoy a la manipulación genética y sus límites. Por último es importante saber que los algoritmos son "instrucciones predeterminadas por el hombre" que forman parte (pudiendo tener más de uno) de "todo el universo del ciberespacio e informático".

5. IA. TEORÍA DEL DELITO, ACCIÓN. CAUSALIDAD Y PROPIEDAD INTELECTUAL: ¿SOLUCIÓN O ESTRATEGIA?

5.1. LA TEORÍA DEL DELITO. ACCIÓN

Es dable destacar y recordar lo que entiende el derecho penal como conducta lo cual nos remite a revisar la Teoría del Delito. De esta forma, buscamos apartarnos de la IA en sí, para perseguir la acción de quien crea a ese software que es el hombre, independientemente de otros conflictos en materia penal, como puede ser la fuerza probatoria.

Luis Jiménez de Asúa (1969) decía que: *"una Teoría que no sirve para la práctica, no es una Teoría; y una práctica sin Teoría, es mera rutina",* tomando esta premisa podemos decir que la Teoría del Delito, sirve para saber que es DELITO, y como toda Teoría obliga a una abstracción. Para determinar la existencia de un delito, debe haber una Conducta Típica Antijurídica y Culpable, lo que supone un pragma conflictivo como sostiene Zaffaroni, entendido como un orden sistemático, mediante un sistema de "filtros", por ponerlo en palabras coloquiales. En el ejercicio del *ius puniendi*, el Estado como único legitimado para imponer una pena a un delito. La función práctica de esta teoría es permitir tanto a fiscales y jueces realizar sus imputaciones y decisiones apartadas de criterios emocionales que de ser ejercidos deriva en **inseguridad jurídica**.

Los presupuestos de la teoría deben ser armónicos, lo que implica que el derecho positivo no puede contradecirse y debe a su vez haber unidad, dada esta por una estructura común a todo delito (en este caso al cibercrimen ejercido de la mano de AI, con previo desarrollo del hombre) y por último debe ser funcional al derecho penal y sus instrumentos: Penas (art 5 CP); y a las MEDIDAS DE SEGURIDAD (art. 34 inc. 1)

La acción, es el primer elemento de esta teoría como punto de partida de la imputación. Así las cosas, en nuestro país existe una fidelidad por el Derecho Penal de acción lo que produce un rechazo al Derecho Penal de Autor. Es en este elemento donde quiero hacer foco.

Se comprende por acción **al comportamiento humano relevante para el Derecho Penal**, limitado por un común denominador a Modalidades delictivas (comisión, omisión sea dolosa o culposa). Tanto Causalistas y Finalistas coinciden en que son **actos voluntarios**, objetivamente dado por movimientos corporales que causa una modificación en el mundo exterior –resultado – y en subjetivamente, es que el resultado debe coincidir con el fin que se propuso. La **solución** a estos ya postergados puntos de vista "objetivos o subjetivos se da mediante un **concepto social de acción**, que involucra una conducta humana socialmente relevante que se aprecia por su cualidad de ser subsumida en un tipo penal.

La función de este elemento se da por tres destacados pilares, entendidos por la **delimitación**, **referencia** y **enlace**. La **delimitación** implica que la Acción requiere voluntad, por lo tanto en los actos involuntarios no hay acción, haciendo caer a esta teoría y por tanto no hay delito. La **referencia,** se vincula al suficiente contenido material, que agrega la cualidad (típica) permitiendo una conexión (**enlace)** con las demás nociones o elementos de la Teoría.

En cuanto a sus aspectos relevantes tenemos, por tanto, un **comportamiento** que trasciende al exterior, lo cual limita el poder punitivo estatal dentro del *iter criminis*. Otro aspecto es la **evitabilidad**, donde solo una conducta evitable como su palabra lo expresa, puede expresar el sentido social que interesa al derecho penal. Referida ésta a conductas que un sujeto pueda "dominar" (DOLO) o haya podido dominarlo (CULPA) y por último el **resultado**, que haya trascendido (aunque de manera trunca – tentativa-) al mundo exterior que rodea al autor.

Existen ciertas conductas, que no son perseguidas por caer en una causal de exclusión como ser: **ACTO REFLEJO**, donde no hay voluntad, no es un acto intelectivo, si es un movimiento biológico, donde no hay participación de la psiquis a diferencia de los actos impulsivos, instintivos o permanentes donde si participa la psiquis, por lo tanto hay acción siendo cuestiones que de todas formas, deberán ser revisadas si así se plantean por la

defensa en la culpabilidad. **FUERZA FÍSICA IRRESISTIBLE**, prevista en el art 34 inc. 2 del código penal: "el que obrare violentado por fuerza física irresistible (…)" donde existe una vis absoluta y no hay voluntad, sino que se actúa de forma mecánica, sea por la acción de otros individuos (v.g. avalancha) o por causa de una fuerza natural (v.g. corriente de agua) existiendo diferencia con la coacción donde la vista es relativa y se analiza en otra instancia de la Teoría (culpabilidad). **ESTADO DE INCONSCIENCIA ABSOLUTA:** Excluyen la acción por cuanto no interviene la voluntad del sujeto y ello ocurre tanto en los casos ejecutados durante el sueño normal o anormal (sonambulismo). También se excluye como causa de exclusión de la acción la denominada embriaguez letárgica, donde se produce una total anulación de la conciencia, pero también una paralización del cuerpo. La hipnosis en los estados de inconsciencia, queda descartada porque nunca pierden por completo la consciencia de sus actos, pero se analiza en la culpabilidad.

Por tanto más allá de cuestionar si la conducta es humano o no, que para mí hay conducta humana utilizando como medio la tecnología (hardware, software y conectividad) restara "encontrarla" en este nuevo escenario del Ciberespacio, además de factores vinculados a la fuerza probatoria y el ámbito de validez espacial del derecho penal.

5.2. CAUSALIDAD. EL HOMBRE DETRÁS DEL ALGORITMO

Causalidad es la realidad fáctica según la cual a toda causa le sigue un resultado y por lo tanto, el nexo que les une es la relación de causalidad. Es de interés del Derecho Penal atribuir resultados perniciosos a una determinada conducta, por lo que es necesario, en primer lugar, establecer si entre la acción humana penalmente relevante y resultado existe una relación de causalidad desde una perspectiva natural. Dicho vínculo debe trascender al derecho penal, por lo que el segundo paso, en consecuencia, es un juicio normativo, conocido como juicio de imputación objetiva.

Además de las referidas situaciones objetivas, para que el reproche sea penalmente válido, es necesario tomar en cuenta la intención del autor, su grado de imputabilidad al momento de cometer el hecho, las eximentes de responsabilidad, etc., entendido como la "imputación subjetiva" del resultado.

Para que sea posible determinar ambos tipos de imputación (la objetiva y subjetiva), es necesario establecer la llamada causalidad concreta, dónde se procede a valorar si la conducta del imputado se adhiere a esa causalidad científica como causante del resultado, por lo que de

probarse la imputación en ambos sentidos, previa otras valoraciones, se **impondrá la sanción correspondiente al delito cometido**.

En ese sentido, la causalidad es la condición mínima de la imputación objetiva del resultado; pero no la única, ya que a ella debe añadirse aún la relevancia jurídica de la relación causal entre la acción y el resultado. Naturalmente, la relevancia de los cursos causales no se limita sólo objetivamente, sino que también la exigencia de un aspecto subjetivo del hecho, tiene un efecto limitador. [15]

Resultando de gran importancia el estudio de la causalidad dentro de la teoría de la imputación objetiva, ya que todo comportamiento delictivo es imputable como fenómeno físico. Entre **las teorías de la causalidad** de mayor trascendencia están las siguientes:

TEORÍA DE LA EQUIVALENCIA DE CONDICIONES: para esta teoría, es causa toda condición que interviene en la producción de un resultado, siendo imposible diferenciar entre causas y condiciones. Para determinar cuando estamos en presencia de una causa, hay que usar la formula conditio sine qua non, que establece que si suprimimos mentalmente determinada condición y el resultado desaparece, dicha condición es su causa. (v.g.: conductor ebrio, así como un cúmulo de ulteriores circunstancias que hayan influido en el suceso como ser la construcción de la carretera y del vehículo, etc.). En esta teoría, no se realiza ninguna selección de las muchas condiciones de cualquier resultado, sino que todas se consideran equivalentes (o sea de igual valor), por lo que a ese juicio de equivalencia se le debe su nombre a la teoría de la equivalencia.[16] El criterio preponderante es que todo resultado es determinado y verificado por un conjunto de antecedentes causales, por lo que la causa será el conjunto de condiciones o antecedentes que han contribuido a la producción causal del resultado. También se le denomina teoría de la ***conditio sine que non***, entendida del latín "condición esencial" o "condición indispensable", como un mecanismo para atribuir a un factor la categoría causa, que implica que un acontecimiento es causa de un resultado, cuando no pueda ser suprimido mentalmente, sin que el mencionado resultado desaparezca.

TEORÍAS INDIVIDUALIZADORAS: Estas teorías consisten en agrupar una serie de criterios que perseguían limitar la extensión de la equivalencia de condiciones. Se pretende seleccionar en cada caso concreto el factor que resulta determinante en la realización del resultado, diferenciando así entre causa y condición, en el entendido de que estas últimas son meras circunstancias acompañantes. Atendiendo a dichos criterios, una causa podría ser la

[15] Günther Jackobs, (2002). Los pormenores del tipo objetivo mediante la acción, en Imputación objetiva y antijuridicidad. Estudios de Derecho Penal (p. 107).

[16] Claus Roxin, (2002). La imputación al tipo objetivo, en Imputación objetiva y antijuridicidad. Estudios de Derecho Penal(p. 122-123)

condición más eficaz, la última condición que antecede al resultado, la más preponderante, o la que se considere decisiva atendiendo su esencia y manifestación, tal y como explico a continuación:

Primero **la Teoría de la adecuación:** esta teoría no sustituye a la anterior, sino que suprime la equivalencia de todas las condiciones. Conforme a esta teoría, una causación sólo será jurídicamente relevante sino no es improbable[17]. Situación donde sólo es causal una conducta que posee una tendencia general a provocar el resultado típico, siendo irrelevantes jurídicamente, las condiciones que sólo por casualidad han desencadenado el resultado. Por ello, no toda condición del resultado es causa en sentido jurídico, sino sólo aquella que es adecuada para producir el resultado. Por su parte, la causa será adecuada siempre y cuando haya **probabilidad o previsibilidad objetiva de producción del resultado**.

Luego **la Teoría de la causalidad adecuada:** también llamada causalidad típica, entiende que para la existencia de la relación de causalidad se requiere que el agente haya determinado o producido el resultado con una conducta proporcionada y adecuada. A fin de que exista una relación de causalidad en el sentido del Derecho, se hace necesario que el hombre haya determinado el resultado con una acción proporcionada, adecuada. La consecuencia fundamental de la teoría es que no se consideran causados por el agente, los efectos que en el momento de la acción se presentasen como **improbables**, es decir, los efectos extraordinarios o atípicos de la acción misma. Para determinar, se realiza un juicio de probabilidad por el juez, que debe situarse en el momento de la acción, quien debe considerar aquellas condiciones que al tiempo de la acción sean "**conocidas y cognoscibles**" por un hombre medio prudente. **También hay que incluir los conocimientos particulares del autor del hecho**.

Por último, la Teoría de la causalidad relevante: La causa es aquella condición que al suprimirla mentalmente conduce a la desaparición del resultado, sólo en cuanto este último sea entendido como categoría jurídica. Para Mezguer, al derecho penal sólo le interesan las causas que sean adecuadas para producir el resultado, empero para él, la determinación de la adecuación de la causa opera en un plano estrictamente jurídico, basándose en los tipos penales.

Así las cosas, es indubitable todo lo que resta estudiar, para arribar a un derecho robusto, solo posible con conocimiento del aporte de doctrina en esta materia. Situación que nunca llegará, si no se comprende el fenómeno que la tecnología nos plantea, pero por medio de estas teorías, llegamos a la conducta humana precedente.

[17] Günther JAKOBS, (2002). *Los pormenores del tipo objetivo mediante la acción,* en Imputación objetiva y antijuridicidad. Estudios de Derecho Penal, 2002, (p. 107).

5.3. ¿PUEDE AUTÓNOMAMENTE, LA IA GENERAR DERECHOS DE AUTOR?

Al hablar acerca de la propiedad intelectual atribuida a creaciones de la IA surge un fuerte debate alrededor de si una máquina puede tener derechos de autor. Según la Organización Mundial de la Propiedad Intelectual (OMPI), cualquier creación de la mente puede ser parte de la propiedad intelectual, pero no especifica si la mente debe ser humana o puede ser una máquina, dejando la creatividad artificial en la incertidumbre.

En el **derecho comparado**, han comenzado a surgir distintas legislaciones con el fin de manejar la IA, relacionada con su uso como también su creación. Legisladores y miembros del gobierno han comenzado a pensar acerca de esta tecnología, enfatizando el riesgo y los desafíos complejos de esta. Observando el trabajo creado por una máquina, las leyes cuestionan la posibilidad de otorgarle propiedad intelectual a una máquina, abriendo una discusión respecto a la legislación relacionada con IA.

Recientemente, el 5 de febrero de 2020, la Oficina del Derecho de Autor de los Estados Unidos y la OMPI asistieron a un simposio donde observaron de manera profunda **cómo la comunidad creativa utiliza la IA para crear trabajo original**. Se discutieron las relaciones entre la IA y el derecho de autor, qué nivel de involucramiento es suficiente para que el trabajo resultante sea válido para protección de derechos de autor; los desafíos y consideraciones de usar inputs con derechos de autor para entrenar una máquina; y el futuro de la IA y sus políticas de derecho de autor.

El Director General de la OMPI, Francis Gurry, presentó su preocupación ante la falta de atención frente a los derechos de propiedad intelectual, ya que hoy las comunidades tienen dirigido su interés hacia temas de ciberseguridad, privacidad e integridad de datos al hablar de la IA. Gurry cuestionó si el crecimiento y la sostenibilidad de la tecnología IA, llevarán a desarrollar dos sistemas para manejar derechos de autor- uno para creaciones humanas y otro para creaciones de máquinas (no humanas).

Aún existe falta de claridad alrededor de la IA. **Los desarrollos tecnológicos avanzan rápidamente, aumentando su complejidad en políticas, legalidades y problemas éticos que merecen la atención globa**l. Antes de encontrar una manera de trabajar con los derechos de autor, es necesario entenderlo correctamente, porque aún no se sabe cómo juzgar la originalidad (elemento necesario para su protección) de un trabajo que nace de una composición de una serie de fragmentos de otros trabajos.

La asignación de derechos de autor alrededor de la IA, aún está en una **fase "exploratoria", por la falta de conocimientos y definiciones, existiendo incertidumbre**

sobre la capacidad de producir contenido de manera autónoma, sin ningún humano involucrado, algo que podría influenciar si sus resultados pueden ser protegidos por derechos de autor.

El sistema general de derechos de autor aún debe adaptarse al contexto digital de IA, pues están centrados en la creatividad humana. Los derechos de autor no están diseñados para manejar cualquier problema, pudiendo ser dañino extender excesivamente los derechos de autor para resolver problemas periféricos dado que:

"Usar los derechos de autor para gobernar la IA es poco inteligente y contradictorio con la función primordial de los derechos de autor de ofrecer un espacio habilitado para que la creatividad florezca". Siendo esta última el objetivo de estos derechos subjetivos.

Con esto intento quiero sostener, que cualquier derivación de conductas artificiales y los derechos que autónomamente puedan derivar una una creación original, no debemos olvidar que fue dirigido por la mano del hombre, en la creación de un algoritmo que compone un software inteligente (IA), y destacar algunos aspectos ya que si se pretende cuestionar como una posibilidad futura de protección de derechos, como contracara se debe encarar la responsabilidad incluso penal, si por medio de IA, se vulneran bienes jurídicos tutelados.

5.3.1. PROPIEDAD INTELECTUAL Y DERECHOS DE AUTOR. SOFTWARE Y SUS ALGORITMOS

Al hablar de propiedad intelectual del software, primero debemos saber que éste es un programa de computación. Es el soporte lógico del sistema informático, siendo que la conjunción de la interacción entre el hardware y el software hace operativa a una computadora o bien otro dispositivo por ejemplo un celular o una tableta.

En relación al software como ya referí en otro capítulo, *"es un conjunto de instrucciones en código binario que pueden ejecutarse en un soporte físico (hardware) y que posibilita la obtención de información procesada de acuerdo a una finalidad dada"* [18]. Es decir, son instrucciones escritas en algún lenguaje de programación y el mismo debe ser interpretado para poder ser ejecutado para cumplir su finalidad. Sin buscar ser redundante, decimos que son instrucciones ordenadas y codificadas en un lenguaje de programación que expresa un algoritmo y puede ser ejecutado en un dispositivo.

[18] Tratado de informática jurídica / definición proporcionada por la Universidad de Belgrano en la cátedra de estudio en informática jurídica.

A los fines de analizar cada uno de los elementos que se desprenden del concepto de software, sin olvidar que las sistemas operativos de nuestros celulares, computadores, sistemas de monitoreo online de cámaras, plataformas de aprendizaje como el de nuestra universidad, juegos, redes sociales, comprendiendo todas estas manifestaciones son un software, y a continuación comparto.

LENGUAJE DE PROGRAMACIÓN: es el conjunto de símbolos y reglas sintácticas y semánticas que definen su estructura y significado de sus elementos y expresiones. Entre estos lenguajes podemos enumerar a los más conocidos por el JAVA; PHP; SQL; VISUAL BASIC, entre otros, los cuales se utilizan para crear programas y expresar algoritmos.

CÓDIGO FUENTE: es aquel elaborado por un programador en algún lenguaje de programación y debe ser traducido a otro lenguaje (máquina / objeto), para ser ejecutado por el hardware (dispositivo)

ALGORITMO: Este es independiente del lenguaje (es el que expresa al algoritmo), se entiende por la secuencia o conjunto preescrito de instrucciones; operaciones; reglas o como quieran llamarse que representar un modelo de solución para determinado tipos de problemas. Esas instrucciones deben estar **definidas** (si se sigue dos veces se obtiene un mismo resultado); **precisas** (implica el orden de realización de cada uno de los pasos) y **finitas** (siendo esto el número determinado de pasos, que tienen un fin). Por lo tanto se encuentra vinculado por un lado con las ciencias exactas, por otro un pseudo código para la lectura humana y con los conocidos diagramas de flujo, realizado en un lenguaje que lo expresa. De manera sucinta, implica que responde a:

1. **Entrada de datos:** Los necesita para que el algoritmo sea ejecutado;
2. **Proceso:** Secuencia de pasos para ejecutar el algoritmo;
3. **Salida de Resultados:** Son los datos obtenidos después de la ejecución del algoritmo.

En mis palabras, un algoritmo vendría a ser un conjunto de acciones, o una lógica de un proceso para resolver un problema o realizar una acción.

Por ejemplo: puedo tener un algoritmo para ingresar a mi casa, que sería tomar la llaves, colocarlas en la cerraduras, girar y abrir el picaporte para ingresar. Esto traducido a un algoritmo de programación sería tomar el nombre y la clave de usuario que quiere ingresar a una página y buscarlo en la base de datos para cotejar si tiene permiso de acceso.

Los algoritmos son procesos lógicos para hacer o resolver, motivo por el cual los encontramos en todos los programas (software) pero solo son una parte de ellos, por tanto un programa **está** compuesto de algoritmos, es decir el programa o software está formado por uno

o más algoritmos y escrito en un lenguaje de programación que logró otro software interpreta para producir un resultado. Un ejemplo de esto, sería en una página web, una parte de ella es código de programación escrito en un lenguaje específico que contiene unos algoritmos y que a su vez será interpretada por otro software como el navegador (Chrome).

En este juego de piezas, de instrucciones, códigos y lenguajes a fin de lograr que la interpretación de los sistemas informáticos que operan y se conectan al ciberespacio - a modo de constelación - muchas veces voluntariamente escondan una amenaza para los usuarios que "no hablamos en ese idioma". Como se verá en el próximo capítulo al ver Phishing.

5.4. TIPOS DE SOFTWARE DEFINIDOS EN TRES GRANDES GRUPOS

Los tipos de Software pueden ser definidos en tres grandes grupos:

DE SISTEMA (USUARIO Y PROGRAMADOR): Son interfaces de alto nivel que brindan tanto al usuario y/o programador herramientas y utilidades de apoyo que permiten su mantenimiento. Incluye sistemas operativos; controladores de dispositivos; herramientas de diagnóstico, corrección y optimización y servidores.

DE PROGRAMACIÓN (PROGRAMADOR): Es el conjunto de herramientas que le permiten al programador desarrollar programas informáticos, usando numerosas alternativas y lenguajes. Incluye editores de texto; compiladores; intérpretes; enlazadores; depuradores (antivirus) e IDE (en español Entornos de desarrollos integrados).

DE APLICACIÓN (USUARIO): permite al usuario hacer tareas específicas y actividades autorizadas. Incluye aplicaciones para control de sistemas y automatización industrial; software educativos, empresariales y médicos; bases de datos; telecomunicaciones; videojuegos; diseño asistido CAD y de control numérico CAM.

6. NORMATIVA

En el año 1998, se modifica la ley 11.723 por medio de la sanción de la 25.036, incorporando a los programas de computación y se establece que la acción penal alcanza al software en virtud del tratado ADPIC/TRIPS. (VER ANEXO 5 - EVOLUCIÓN NORMATIVA)

6.1. DELITOS EN ESTA RAMA EN NUESTRO DERECHO POSITIVO

La **Piratería** y el **Plagio** son aquellos delitos que vulneran la propiedad intelectual, sin descartar que pueden cometer los propios desarrolladores tanto culposa como dolosamente delitos que lesionan bienes jurídicos de los usuarios, por no tomar ex ante ciertas precauciones, como ser las medidas de seguridad.

En relación a la **piratería,** es la reproducción sin autorización de una obra ajena, en este caso el software. A su vez esta reproducción puede darse como:

1. Falsificación, lo que implica ser realizada a gran escala con fines comerciales, donde se confunde al público simulando ser el legítimo;
2. La copia, con fines comerciales o gratuitos grabado en un dispositivo;
3. La copia ilícita que hace el usuario corporativo;
4. La copia con fines individuales.

Jurisprudencia sobre este tema, encontramos entre los relevantes, al CASO COMPURAMA del 2007, sobre venta de software. Cabe procesar en orden al delito de defraudación a los derechos de propiedad intelectual, previsto en el art. 72 inc. a de la ley 11.723 (Adla, 1920-1940, 443), a quien habría vendido una computadora con programas instalados sin sus respectivas licencias de uso. CNCC, Sala IV, "Compurama Computación", 8/8/07

La PIRATERIA EN EL DERECHO COMPARADO, España ya persigue en el artículo 270 inciso segundo del código penal está dedicado a conductas llevadas a cabo por prestadores de servicios de la sociedad de la información. Este precepto se centra en quien "facilite de modo activo y no neutral" el acceso a obras pirata. En concreto, se centra en aquellos que ofrecen "listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente". Es decir, este artículo castiga el estilo de explotación económica de las plataformas de contenidos pirata como MegaUpload, como podría ser el caso de CUEVANA, MIRADETODO, SERIESFLIX, entre otras plataformas.

El plagio, surge entre las infracciones previstas en la Ley de Propiedad Intelectual 11.723 y sus reformas que si bien no se lo menciona literalmente, la protección ante este tipo de infracciones surge de los artículos 71 y 72 (inciso c) de esa norma.

El concepto de plagio en sí mismo lo han ido delineando la doctrina y la jurisprudencia, en el convencimiento de que *"hay plagio cuando existe imitación de cierta magnitud respecto de la obra plagiada, no de la idea, cuando pese a diferencias triviales, variaciones, agregados o resoluciones, la obra presenta en comparación con la anterior una semejanza tal que permite*

reconocer que se trata, en el fondo, de una misma representación individual", (según fallo de julio de 1983 de la Sala E de la Cámara Nacional Civil).

Un elemento relevante, para evaluar la existencia de plagio es la pericia, que verificará la inclusión de la totalidad, partes o fragmentos de una obra en otra, el cotejo dependerá del género expresivo, debido a que al no protegerse las ideas sino la expresión de esas ideas, deberán compararse los elementos formales propios de cada disciplina. Situación que variará si se trata de literatura, música, e imaginemos este cotejo en caso de tutela del software.

En caso de ser un plagio burdo, evidente y palmario, que no requiera producción adicional de prueba, se pueden solicitar las medidas provisionales previstas en la Ley Nº 11.723 (artículo 72 bis, y 79), y las cautelares previstas en los códigos procesales locales, incluyendo las correspondientes al artículo 50 del Acuerdo sobre los Derechos de Propiedad Intelectual (ADPIC).

En todos los casos es sumamente importante solicitar a la Dirección Nacional del Derecho de Autor que acompañe el ejemplar de registro, para que el juez pueda hacer el cotejo entre la obra original y la presuntamente plagiaria.

Por último el plagio puede clasificarse en **-NO ELABORADO-** implicando copia sin multiplicación del original, donde se omite hacer referencia al autor y se atribuye falsa autoría, incluyendo "cosmética para disimular". Por otra parte –ELABORADO- teniendo como diferencia con el no elaborado, que existe un mayor esfuerzo para disimular la conducta ilícita.. Por último, resta hablar de la -EMULACIÓN "LOOK & FEEL"- donde la intención del "segundo software" no es confundir al público de la autoría sino, porque opere siendo familiar al usuario/consumidor del primer software (el plagiado). Generalmente es ejecutado por un competidor usando formatos similares. En este caso el primer autor puede exigir que el segundo autor se abstenga de utilizarlos e imitarlo.

7. EL ROL DE LA IA EN LOS CIBERATAQUES

7.1. DISTINCIÓN PREVIA ENTRE CIBERSEGURIDAD Y CIBERDEFENSA

La evolución de las TIC ha provocado un cambio de paradigmas que exige la adopción de procedimientos especializados para neutralizar y controlar las amenazas cibernéticas. La ciberdefensa, además de prevenir los ataques, les da respuesta con el fin de salvaguardar la seguridad. Para distinguirlas cabe mencionar que la **ciberdefensa encuentra en su concepto**

una dimensión militar. Cada país tiene su propio concepto de ciberseguridad y ciberdefensa, los cuales dependen de la concepción de defensa y seguridad.

Si bien no existe un concepto único en estas cuestiones, por encontrarse en pleno desarrollo, vemos que el término ciberdefensa se refiere a los componentes militares del Estado que son utilizados para defender el ciberespacio. En esta línea, la OTAN la define como la habilidad de salvaguardar los sistemas de comunicación y de información en respuesta a acciones potenciales e inminentes que hayan sido o no originadas en el ciberespacio.

La ciberseguridad, por su parte, también cuenta con una concepción de protección de infraestructuras, redes, sistemas de comunicación y de información, pero no se acota a lo estrictamente militar, es decir, la ciberseguridad se enmarca en una concepción mucho más amplia. Es decir, el concepto **de ciberseguridad es complementario al de ciberdefensa y materializa la defensa nacional digital**. Pero el desarrollo de conceptos como el ciberterrorismo o el cibercrimen, cada vez más presentes en nuestra sociedad, hacen fundamental la existencia de mecanismos exclusivos de ciberdefensa.

Por otra parte, **me atrevo a extender que la ciberseguridad es aquella ejercida en manos de fuentes privadas no estatales** a los fines de resguardar sus desarrollos intelectuales lucrativos o no, y en ciertos casos atendiendo a la responsabilidad que les cabe, como el denominado DEBER DE SEGURIDAD.

En nuestro país, la Subsecretaría de Ciberdefensa del Ministerio de Defensa y el Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas son los organismos que se encargan de dar respuesta ante amenazas o agresiones que puedan afectar a la defensa nacional.

7.2. RECIENTE INFORME DE DIFERENTES INSTITUCIONES INTERNACIONALES

Recientemente con fecha 20 de noviembre de 2020, instituciones internacionales realizaron un informe con la finalidad de estudiar el rol desplegado por la IA en los ciberataques. El mismo es atribuido a EUROPOL junto con el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI), y TREND MICRO[19]

[19] María E. Darahuge - Luis Arellano Gonzálz, (2018). Empleo de las direcciones virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad. Buenos Aires, Argentina.

A fin de introducir a los que formaron parte de esta investigación que vengo a compartir, paso a describir a los "players".

Acerca de EUROPOL, es el Centro Europeo de Ciberdelincuencia (EC3) que se creó en 2013 para fortalecer la respuesta policial a la ciberdelincuencia en la UE, con fines de ayudar a proteger a los ciudadanos, empresas y gobiernos europeos de la delincuencia en línea. Su enfoque está en el ciberdelito cometido por **grupos del crimen organizado (como sujetos activos)**, que generan grandes beneficios (fraude en línea), dañan gravemente a las víctimas (explotación sexual infantil en línea) o impactan en la infraestructura crítica y los sistemas de información en la UE, los que incluyen ciberataques. Sus aportes desde la creación hasta el día de hoy, en manos del EC3 de Europol han sido significativos, en la lucha contra la ciberdelincuencia: participando en operaciones complejas de alto perfil y apoyo operativo, permitiendo cientos de detenciones.

UNICRI, por su parte, que es el Instituto Interregional de Investigaciones sobre Delincuencia y Justicia de las Naciones Unidas, establecido en el año 1968, dentro de otros aspectos abarcativos de su mandato, es un instituto que contribuye investigando, capacitando y tomando acción en esta área, recopilando el intercambio y la difusión de información, a la formulación y aplicación de mejores políticas en el ámbito de la prevención del delito, la justicia y las nuevas amenazas a la seguridad, prestando la debida atención a la integración de dichas políticas en relación a otras más amplias para el cambio socioeconómico y el desarrollo y en atención a la protección de los DDHH, aspecto que destaque de relevancia en mi introducción al cibercrimen. En 2017, la UNICRI abrió su **Centro de Inteligencia Artificial y Robótica en La Haya, Países Bajos, para avanzar en la comprensión de la inteligencia artificial, la robótica y las tecnologías relacionadas con la prevención del delito, la justicia penal, el estado de derecho y la seguridad.** La forma que plantea, compartiendo conocimientos e información sobre las posibles aplicaciones beneficiosas de estas tecnologías y contribuir a abordar los **efectos nocivos y el uso malintencionado**.

Por último, resta hacer mención de Trend Micro, empresa líder mundial en ciberseguridad, la que busca ayudar a la comunidad internacional en el intercambio seguro de información digital. Empresa que nace en la década del 90' con más de 30 años de experiencia en seguridad, investigación de amenazas globales e innovación continua, Trend Micro permite la resiliencia de empresas, gobiernos y consumidores con soluciones conectadas referidas a cargas de trabajo en la nube, terminales, correo electrónico, IIoT y redes. Su estrategia de seguridad XGen ™ impulsa soluciones con una combinación intergeneracional de técnicas de defensa **contra amenazas que están optimizadas para entornos clave y aprovechan la inteligencia de amenazas compartida para una mejor y más rápida protección**. La empresa tiene presencia en 65 países, con más de 6.700 empleados y la

investigación e inteligencia de amenazas globales más avanzadas del mundo, Trend Micro permite a las organizaciones proteger su mundo conectado.

Continuando, si bien el avance de la tecnología nos ha facilitado la vida, por su parte la dependencia de internet, dispositivos y aplicaciones también nos vuelve más vulnerables, a los que era antes de su existencia. Es por ello que el objetivo del informe fue analizar cómo los delincuentes están empleando IA para elaborar ataques y cómo se espera que la utilicen en el futuro.

"La IA promete al mundo mayor eficiencia, automatización y autonomía. En un momento en el que el público está cada vez más preocupado por el posible uso indebido de la IA, tenemos que ser transparentes en cuanto a las amenazas, pero también examinar los posibles beneficios de la tecnología de la IA", afirma en el comunicado de prensa, Edvardas Sileris, Jefe del Centro de Ciberdelincuencia de Europol, palabras abordadas con ciertos recaudos, ya que la IA lleva años transformando progresivamente la economía global y la vida de los ciudadanos. Solo en 2020, según datos de Trend Micro, el 37% de las **empresas** y organizaciones utilizan la IA de alguna forma dentro de sus sistemas y procesos. Gracias a ella, las compañías pueden conocer mejor a sus clientes y, de esta forma, mejorar sus opciones comerciales. Sin embargo, su **abuso,** así como su **uso indebido** puede plantear problemas al internauta como lo viene haciendo desde hace algunos años.

En concreto, el informe destaca los potenciales peligros detrás del auge de los **"deep fakes**", que son los contenidos audiovisuales en los que se cambia el sonido y/o la imagen original de una grabación. **Si esta tecnología**, que ha evolucionado enormemente en los últimos dos años, **se emplea con el fin de desinformar puede causar graves problemas**. Tanto políticos como empresariales. Así lo demuestra, por ejemplo, el caso de una conocida empresa energética del Reino Unido, que perdió más de 200.000 euros debido al empleo de un audio falso en el que se había utilizado IA para copiar la voz de un ejecutivo de la compañía, según publicó "The Wall Street Journal".

Según ha descubierto Trend Micro estudiando los mercados del cibercrimen, los delincuentes **también están utilizando la IA en sus sistemas destinados a adivinar contraseñas de plataformas en internet.** Esta tecnología, además, les permite utilizar bots automatizados maliciosos en redes sociales y engañar a los sistemas de detección o realizar ataques asistidos. Y este solo es el principio; el estudio también recopila cuáles son las previsiones de Europol, Unicri y la empresa de ciberseguridad sobre cómo emplearán esta tecnología en el futuro. "Estoy convencido de que veremos estos ataques en algún momento, si no es en **2021 será al año siguiente**", explica a este diario David Sancho, jefe de análisis de amenazas de Trend Micro y uno de los participantes en la elaboración del estudio.

El informe concluye que los ciberdelincuentes aprovecharán la IA como vector de ataque y como superficie de ataque. Las falsificaciones profundas son actualmente el uso más conocido de la IA como vector de ataque. Sin embargo, el informe advierte que se necesitarán nuevas tecnologías de detección en el futuro para mitigar el riesgo de campañas de desinformación y extorsión, así como las amenazas que apuntan a conjuntos de datos de IA.

Se plantean diferentes modalidades de uso de la IA para respaldar lo que paso a enumerar:

1. Convencer a los ataques de ingeniería social a gran escala;
2. Malware de rastreo de documentos para hacer que los ataques sean más eficientes;
3. Evasión del reconocimiento de imágenes y biometría de voz;
4. Ataques de ransomware, mediante la evasión y la focalización inteligente;
5. Contaminación de datos, mediante la identificación de puntos ciegos en las reglas de detección.

Por su parte, Irakli Beridze, director del Centro de Inteligencia Artificial y Robótica de UNICRI, *"a medida que las aplicaciones de IA comienzan a tener un gran impacto en el mundo real, se hace evidente que esta será una tecnología fundamental para nuestro futuro*", dijo, pero "*sin embargo, así como los beneficios de la IA para la sociedad son muy reales, también lo es la amenaza del uso malintencionado. Nos sentimos honrados de apoyar a Europol y Trend Micro para arrojar luz sobre el lado oscuro de la IA y estimular un mayor debate sobre este importante tema".*

Las tres organizaciones hacen varias recomendaciones para concluir el informe, que atienden los siguientes temas:

1. Aprovechar el potencial de la tecnología de inteligencia artificial como herramienta de lucha contra el crimen para preparar la industria y la policía de la ciberseguridad en el futuro;
2. continuar la investigación para estimular el desarrollo de tecnología defensiva;
3. Promover y desarrollar marcos de diseño de IA seguros;
4. Reducir la retórica políticamente cargada sobre el uso de IA con fines de ciberseguridad;
5. Aprovechar las asociaciones público-privadas y establecer grupos de expertos multidisciplinar.

CAPÍTULO 4

DELITOS PLURIOFENSIVOS

"INGRESO" DE BIENES JURÍDICOS AL ESPACIO FÍSICO VS. VIRTUAL

1. DELITOS PLURIOFENSIVOS

Los delitos pluriofensivos son aquellos que afectan a más de un BIEN JURÍDICO a la vez, es por ello que también se los denomina DELITO O TIPO PLURIOFENSIVO, v.g. el hurto es un delito que afecta únicamente a la propiedad, mientras que el robo, al exigir la violencia, puede afectar también a la integridad física de las víctimas. Nuestra normativa en materia del objeto de esta tesina - cibercrimen -, y como así también sostiene la mayoría de la doctrina, permite calificar a los delitos allí tipificados como pluriofensivos, admitiendo la aplicación de sus normas en resguardo de bienes jurídicos distintos, como el patrimonio o la intimidad.

El bien al que se hace referencia, es el determinado previamente como tal por una comunidad, ubicada en el tiempo y en el espacio, pudiéndose decir que implica que entidad merece ser considerada como bien con el objeto de atender necesidades tanto individuales como sociales.[20]

En cuanto al bien como producto de esa elección que asigna un valor, se independiza del sujeto que lo elige. Aparece entonces una relación entre la entidad ***bien*** y el **sujeto,** que recibe el nombre de interés. El interés es de carácter individual y social, relación que se denomina reflejo subjetivo.

El interés es recogido por el Derecho para ser asegurado, apareciendo la norma que prohíbe y que manda: el precepto o presupuesto que describe la conducta atentatoria – en este caso el delito - y al mismo tiempo el objeto de protección. Situación que hace que el *bien se "transforme"* en bien jurídico y penalmente protegido.

Por lo tanto es **necesario el conocimiento del objeto de la protección de cada figura penal,** para no caer en el defecto, recordando que la descripción de una conducta que aún circunstanciada, por sí sola no puede ser considerada delictiva no resulta suficiente para informarnos acerca de la existencia de un delito. Esto es algo más, es ontológicamente, la

[20] Antonieta Goscilo, (1981). Lecciones y Ensayos Nº 46-0: "Los bienes jurídicos penalmente protegidos". (p. 25).

resultante de la coincidencia entre el objeto de la conducta lesiva (de un modo peligroso o efectivo) y el objeto de la protección jurídico penal.

El bien jurídico ilumina la interpretación de una disposición penal, a fin de permitir la comprensión su trato jurídico, sirve para superar las dificultades que puedan surgir al efectuarse el encuadramiento legal de un hecho que así lo exige, que según el rol desempeñado será por ejemplo en el caso del juzgador para encontrar argumentos en favor de la defensa o la acusación, o bien sea como funcionarios o en el ejercicio de la profesión.

El análisis de los bienes jurídicos protegidos en los distintos títulos del Código Penal, tiene una regla, un recorrido obligado, que exige una lectura detenida de las figuras delictivas para desentrañar qué es lo protegido, que es lo susceptible de lesión, dañosa o peligrosa.

Al observar los diferentes bienes jurídicos, que se busca proteger en nuestro código de fondo en su parte especial, sistematiza y muestra una clasificación en dos grandes grupos, por un lado aquellos bienes jurídicos personales o individuales, como ser la propiedad, el honor, la libertad, la integridad sexual entre otros; y por otro lado aquellos bienes jurídicos del Estado o la comunidad, como la Seguridad de la Nación, la seguridad pública, el orden público, etc. Lo que asoma en su introducción al código una cierta jerarquía de los bienes jurídicos, dada por el orden de preferencia y tratamiento dado por el legislador. Es decir al legislador, darle primero tratamiento a los bienes personales ante los estatales, es porque de alguna forma implícitamente los está considerando más valiosos socialmente en relación a los otros, lo cual depende de la filosofía u orientación política de cada esta. Incluso esto se aprecia tanto en el orden de preferencia como el de la escala penal propuesta para cada delito. Siempre de todas formas, hay un "sector de la biblioteca" que no sostiene esta apreciación. Pero basta ver a mi humilde entender, considerando al derecho comparado, el caso del código penal alemán, que trata de manera inversa a la nuestra a los bienes jurídicos. De todas formas, si bien es un paréntesis a lo que vengo estudiando, la protección es igual para todos los bienes jurídicos.[21]

Como anticipa la parte Especial de nuestro código Penal a partir del art 79 se clasifica y de algún modo jerarquiza (a pesar de doctrinarios que no comparten tal jerarquización) los bienes Jurídicos Tutelados en diversos capítulos, a saber Delitos Contra Las Personas; el Honor; la Integridad Sexual; el Estado Civil; la Libertad; la Propiedad; la Seguridad Pública; el Orden Público; la Seguridad De La Nación; los Poderes Públicos y el Orden ; la Administración Pública; la Fe Pública; el Orden Económico y Financiero.

[21] Dice Soler, que "basta comparar, por ejemplo las escalas penales que protegen el bien jurídico de la vida, para admitir que, en la jerarquía de valores sociales que el Derecho recoge y estables, el bien -vida- es superior a la propiedad."

Asimismo la importancia para nuestra ciencia de derecho de un bien jurídico, es su grado de afectación y sirven de criterio para el establecimiento de penas proporcionales de las conductas que lo lesionan o bien lo ponen en peligro y además permite determinar el injusto específico de cada delito, sistematizar (cómo analice *ut supra*) los tipos penales que conforman la Parte Especial y orientar la interpretación de los comportamientos que ellos reprimen, sin caer en la analogía *in malam partem*, prohibida en materia penal, y la necesidad de subsunción en un tipo penal.

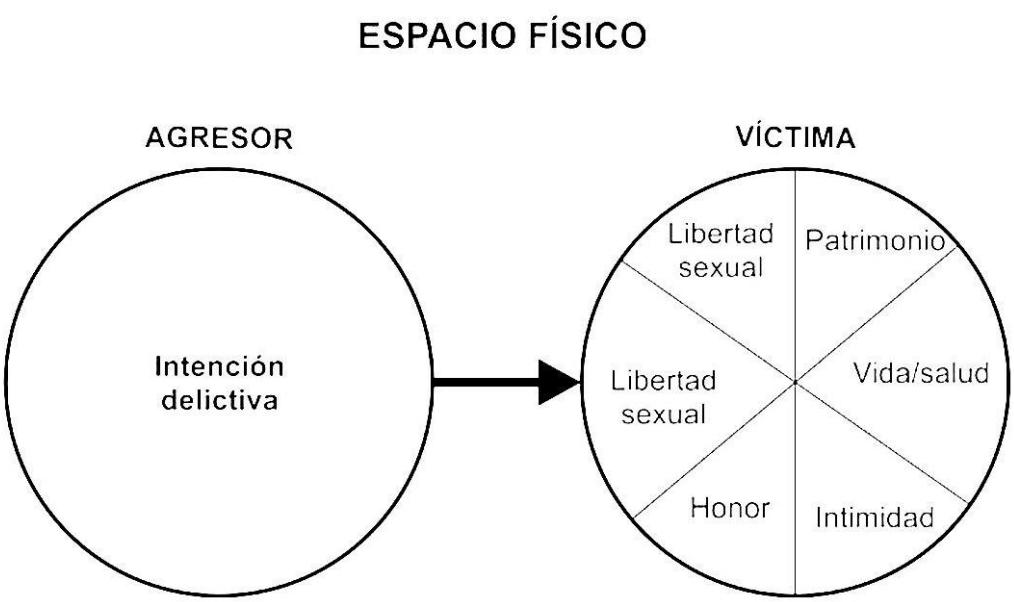
2. PARALELISMO DE OFENSA DE BIENES JURÍDICOS EN EL ÁMBITO FÍSICO VS. VIRTUAL (CIBERESPACIO)

Uno de los presupuestos teóricos de la TAC: es que el aumento del contacto entre las personas, derivado del desarrollo tecnológico, explica en parte el aumento de la criminalidad en las últimas décadas. Pero, obviamente, ese tipo de contacto difiere en cuanto a su naturaleza del contacto, potencialmente mayor en lo cuantitativo, pero quizás menor en lo cualitativo, por excluir el ámbito físico, que puede tener lugar entre las personas en el ciberespacio. Y esta es, a mi parecer, una de las importantes precisiones que deben hacerse a la idea del aumento potencial del contacto entre agresores y objetivos pero, a la vez, el punto de inicio argumental desde el que definir las condiciones que pueden hacer adecuado a un objetivo en el ciberespacio.

2.1. ESPACIO FÍSICO

El contacto entre víctima y agresor en el espacio físico es, generalmente, un contacto físico directo e inmediato, en el que todos los bienes personales de la víctima y los patrimoniales que lleve con ella están expuestos y se convierten en potenciales objetivos adecuados para el ataque del agresor. Es cierto que la víctima potencial puede determinar en gran parte aquello que puede convertirse en objetivo adecuado, seleccionando los bienes con valor económico que lleva consigo, etc.; pero no puede eliminar del ámbito de contacto con las personas, otros bienes personalísimos que van indisolublemente unidos a ella. Prácticamente todo lo que ella es como persona, todo lo que forma parte de ella, se pone en contacto con el agresor en el espacio físico.[22]

[22] Revista Electrónica de Ciencia Penal y Criminología, (13-07-2011). Art. SISSN 1695-0194 RECPC RECPC: LA OPORTUNIDAD CRIMINAL EN EL CIBERESPACIO. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Fernando Miró Llinares, Profesor Titular de Derecho Penal, Universidad Miguel Hernández de Elche.



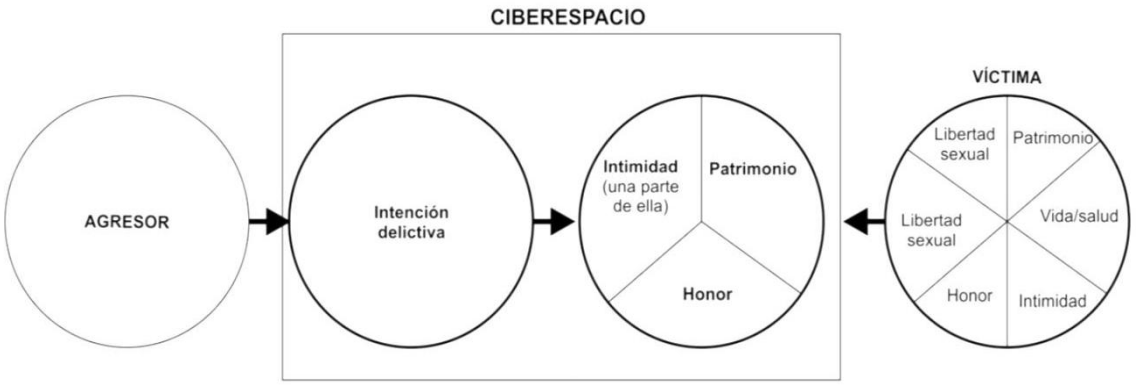
Contacto en el espacio físico. Agresor contacta con la víctima (con todos sus bienes) y selecciona los bienes a los que quiere afectar de todos los que posee.

2.2. ESPACIO VIRTUAL O CIBERESPACIO

En el espacio virtual o ciberespacio, el contacto entre personas es distinto: no es la persona física la que se comunica directamente, en un contexto espacio temporal determinado, con otra persona, sino una representación de la misma, en lo más esencial por ella definida, la que contacta en ese ámbito comunicativo que es Internet.[23]

La persona no entra con todos sus bienes y valores en el ciberespacio, sino básicamente con aquellos que ella elige de entre los que puede hacerlo. Al fin y al cabo, el primer límite que tiene la víctima para comunicarse con otra o para contactar en el ciberespacio, es que no puede poner a disposición de otros su entidad física, de modo que los ataques a la persona que se dirijan directamente contra bienes como la vida o la salud, no podrán ser llevados a cabo en Internet. Además, y pese a que la persona puede ver atacados algunos bienes personalísimos aunque ella no quiera ponerlos a disposición de terceros en el ciberespacio (como ocurre con la libre formación de la sexualidad de los menores, que puede ser atacada al recibir una imagen de contenido sexual o similar), en otros bienes como los relacionados con la privacidad o el propio patrimonio es la víctima la que decide, al incluir información personal en el ciberespacio o compartirla con otros, realizar actividades económicas, y demás, situar tales bienes en ese ámbito de riesgo nuevo.

[23] Revista Electrónica de Ciencia Penal y Criminología, (13-07-2011). Art. SISSN 1695-0194 RECPC RECPC: LA OPORTUNIDAD CRIMINAL EN EL CIBERESPACIO. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Fernando Miró Llinares, Profesor Titular de Derecho Penal, Universidad Miguel Hernández de Elche.



Contacto en el ciberespacio: La víctima no entra en toda su integridad en el ciberespacio, sino que lo hace con algunos bienes, siendo estos los atacables según la intención del agresor.

Los usuarios del ciberespacio pueden, por tanto, eliminar del ámbito de ataque aquellos bienes que no incorporen al ciberespacio. Apoyándonos en uno de los elementos del acrónimo CRAVED, utilizado por Clarke para definir los bienes preferidos por los ladrones (Concealable, Removable, Available, Valuable, Enjoyable and Disposable), podríamos decir que si una víctima no introduce un bien en el ciberespacio, el mismo no estará disponible (not Available) y no podrá ser objeto del ataque. El crimen, por tanto, en cuanto al objetivo concreto sobre el que se dirige, puede ser evitado por la propia víctima en el ciberespacio desde el momento que no es situado el mismo en el espacio virtual. Independientemente de su valor, si la víctima no se incorpora al ciberespacio, el objetivo no existe y, por el contrario, la introducción de elementos en Internet conlleva inmediatamente el riesgo de que puedan ser victimizados. En este sentido, por ejemplo, podríamos citar los estudios empíricos que demuestran la relación entre la entrega de información personal *online* y la victimización por los delitos más relacionados con los jóvenes como víctimas como el cyberbullying y el ciberacoso sexual a menores. En este último caso, hay estudios que constatan que prácticamente todas las modalidades de ataque se configuran en torno a una similar dinámica en la que el paso inicial suele ser el previo envío (la introducción), por parte de la víctima, de información personal a personas desconocidas.

Ahora bien, y como se profundizará después, la mera introducción del objeto no es per se peligrosa, sino que constituye un primer paso que, si se une a la interacción de la víctima en el ciberespacio, ya puede conllevar riesgo de victimización. En efecto, los estudios victimológicos existentes sobre el online grooming parecen demostrar que mientras que el mero hecho de colgar información personal en páginas web o redes sociales, no es un factor que incide en el aumento de riesgo de recibir un ataque de grooming, sí lo es el enviar directamente información personal a desconocidos.

La introducción de un objetivo en el ciberespacio, sin embargo, no siempre es voluntaria. En ocasiones se trata de un proceso casi fortuito: el mero hecho de disponer de un sistema informático y de utilizarlo conlleva la introducción de elementos relacionados con la privacidad que, sin quererlo, pueden conllevar afectaciones a la intimidad o al propio patrimonio. La respuesta a un correo electrónico con el número de una cuenta bancaria supone la introducción del patrimonio disponible en esa cuenta, en el ciberespacio, y del mismo modo el acto de compartir una foto familiar en Facebook o información sobre un viaje reciente, conlleva el riesgo de que esto sea utilizado en contra de la dignidad o la intimidad de la persona.

En todo caso, el **primer condicionante** para que un objetivo sea adecuado a los efectos de la fórmula del cibercrimen, es su introducción en el ciberespacio. A partir de que un objetivo se introduce en el ciberespacio, **voluntaria o involuntariamente**, el mismo puede convertirse en adecuado dependiendo de su valoración por parte del agresor motivado.

Pues bien, el primer elemento a analizar es el del valor del objetivo. Independientemente del tipo de objetivo de que se trate (patrimonial, intimidad, libertad sexual, etc.), en el ciberespacio se da la particularidad de que cosas con poco valor por sí mismo pueden adquirir un valor muy importante gracias a la facilidad para obtener información, relacionarla con la obtenida y convertirla en un objeto de riesgo. Así, cuatro dígitos parecen no ser valiosos, pero si a ellos, por medio del Data Mining, se asocia el concepto "pin", y se relaciona con un determinado usuario, y si después se hace lo mismo con los números de una cuenta bancaria, etc., finalmente tales números acaban por tener mucho valor. En todo caso, es evidente que a mayor valor del objetivo, mayor es la posibilidad de ataque, y esto será igual en el ciberespacio, y las empresas más valiosas serán más buscadas por sus secretos comerciales que las no conocidas, por poner un ejemplo, y el cibercriminal decidirá según el valor que él mismo otorgue al objetivo.

Es indudable que la entrada en el ciberespacio conlleva la irrupción en un espacio público, pero eso no significa que sea "visible", pues puede ocurrir que alguien acceda a Internet y nadie, excepto quienes le proveen el acceso, se aperciban de ello. El ciberespacio es tan ingente y tan universal, que más bien es difícil hacerse visible, hasta el punto de que todos los usuarios conforman una maraña en la que es difícil distinguir a unos y otros. Hay algo, sin embargo, que hace visibles a los sujetos en el ciberespacio, su interacción con otros sujetos y con otros servicios. La interactividad sí es la esencia de Internet, y a mayor interacción con otros agentes, con diferentes páginas web, con variados servicios, mayor posibilidad de ser percibido (ser visible) por parte de otros.

3. CLASIFICACIÓN. SÍNTESIS GRÁFICA

A continuación haré una clasificación que existe en la doctrina[24] que podemos comprenderla dos grandes grupos.

El primero a la atendiendo a la incidencia de las TIC en el comportamiento criminal, que a su vez se subclasifica en: **cibertaques puros**, entendidos como comportamientos únicamente ciberdelictivos, ya que no sería posible su realización sin la existencia de las TIC; **ciberataques réplica**, como comportamientos que ya existían en el mundo físico, pero su comisión en el ciberespacio los modifica y **ciberataques de contenido**, los cuales si bien entrarían dentro de los ciberataques réplica, presentan una problemática que un tratamiento privativo, que englobaría a todos los comportamientos cuyo núcleo delictivo es la transmisión de información a través del uso de las TIC.

El segundo grupo de cibercrímenes responde a un criterio estrictamente criminológico, ya que tiene en cuenta el interés social afectado. Fracciona este grupo en tres grandes categorías: cibercriminalidad económica, social y política- Si bien resalta el predominio cuantitativo de la cibercriminalidad económica, advierte sobre el progresivo protagonismo, tanto cuantitativo como cualitativo, de los cibercrímenes sociales, ya que al extenderse las interacciones sociales al ciberespacio, reducidas antes en el mundo físico, se multiplican las posibilidades de conductas delictivas. Es esta última categorización (económica, social y política) la que el autor utilizará a lo largo de toda la obra para explicar las modificaciones que el ciberespacio ha provocado en los diferentes elementos del delito.

A continuación se procede a la clasificación. (pág. 64)

[24] Miró Llinares, Fernando (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio (pp. 51 a 135), Madrid, España.

CLASIFICACIÓN ATENDIENDO A LA INCIDENCIA DE LAS TIC EN EL COMPORTAMIENTO CRIMINAL.

1. CIBERATAQUES PUROS:

1.1. El hacking;

1.2. Infecciones de malware y otras formas de sabotaje cibernético;

1.2.1. Sabotaje de insiders;

1.2.2. Ataques DoS;

1.2.3. Spam;

1.3. Ocupación o uso de redes sin autorización;

1.4. Antisocial networks;

2. CIBERATAQUES RÉPLICA:

2.1. Los ciberfraudes (auction fraud y otros);

2.1.1. Los ciberfraudes burdos o scam;

2.1.2. **El phishing;**

2.2. Identity theft y cibersuplantación de identidad o spoofing;

2.3. El ciberespionaje;

2.4. Ciberblanqueo de capitales y ciberextorsión;

2.5. El ciberacoso;

2.5.1. El cyberbullying o acoso escolar o a menores en Internet;

2.5.2. El cyberstalking (y el online harassment);

2.5.3. El ciberacoso sexual, el sexting, el online grooming;

3. CIBERATAQUES DE CONTENIDO:

3.1. La **ciberpiratería intelectual;**

3.2. Pornografía infantil en Internet;

3.3. Difusión de otros contenidos ilícitos (especial atención al online hate speech o difusión por Internet de odio racial).

OTRA CLASIFICACIÓN ES POSIBLE: SEGÚN MÓVIL Y CONTEXTO CRIMINOLÓGICO.

1. El cibercrimen económico: la simbiosis de los ciberataques con finalidad económica;

2. El cibercrimen "social" en la web 2.0: redes sociales, desarrollo de la personalidad en el ciberespacio y nuevos cibercrímenes;

3. El cibercrimen político: ciberterrorismo, hacktivismo, y otras formas de delincuencia política en el ciberespacio;

3.1. El ciberterrorismo;

3.2. La ciberguerra;

3.3. El ciberhacktivismo.

4. PRINCIPALES MODALIDADES DELICTIVAS EN ESTE NUEVO ESCENARIO

A continuación selección algunos delitos en este nuevo escenario, que tienen una respuesta y están descritos en nuestro Código penal de la Nación, haciendo foco en aquellos de mayor comisión durante la pandemia.

Los más común son los ciberfraude, motivo por el cual, a continuación, me focalizaré en la ESTAFA INFORMÁTICA, como así la recepta nuestro CP. Recordando que entre Defraudación y Estafa hay una relación de género especie.

4.1. ESTAFAS INFORMÁTICAS

"La estafa informática es la acción genérica prevista es defraudar mediante una manipulación que altera el funcionamiento del sistema informático o la transmisión de datos, con lo que se consagró una suerte de tipo penal abierto en relación con cualquier abuso informático, nota que ya he señalado viene del propio Convenio de Budapest y luce, en cierto grado, ineludible. El segmento concerniente a la transmisión de datos, apunta el nombrado, es el supuesto en que al sistema no se lo altera pero "se lo engaña" en la recepción de información lo que se logra, por ejemplo, impidiendo el funcionamiento de rutinas de chequeo o validación de datos".[25]

Entonces nos encontramos ante un tipo penal abierto, surge del convenio sobre ciberdelito de **BUDAPEST,** Ley 27.411[26]. Sus elementos configurativos del tipo penal son el ardid o engaño; el sujeto pasivo debe caer en error por ser engañado por el sujeto activo y existir un perjuicio patrimonial. Asimismo es un delito de resultado, por tanto se aplica la ley donde este se produjo. Al haber engaño hay estafa siendo esta una diferencia con el daño, donde no lo hay (engaño) y por último admite la tentativa. Las especies son:

[25] Palazzi, Pablo A. (2016). Los delitos informáticos en el código penal. Buenos Aires, Argentina.

[26] CONVENIO DE BUDAPEST: Este Convenio del año 2001, como fuente internacional de derecho de fondo, forma y cooperación internacional, convenio que para su ingreso requiere consentimiento de los Estados parte. Asimismo surge la terminología, obliga al país a adoptar a nivel nacional normas de fondo y forma; actuar en cooperación internacional y es el único convenio que se encarga de la seguridad informática, es decir la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Argentina a realizado algunas reservas vinculada a la portación de material (por entenderlo como anticipación de la pena); definición de pornografía infantil (se hizo una reserva parcial vinculado a adultos que se hacen pasar por menores); otra relativa a la jurisdicción en cuanto a los nacionales que cometan delitos, por ser contrario al principio de terriorialidad y otra dada por la doble jurisdicción (por la conservación de datos que exige doble tipificacion). Tambien hay otras fuentes como ser el protocolo adicional de ciberdelincuania del año 2003 que amplia delitos de naturaleza racista y xenofaga por medio de sistemas informáticos, y otra fuente internacional es el Consejo de Europa, que se ocupa de la protección del niño en relación a la explotación y abuso sexual.

EL CARDING: O bien el **uso no autorizado de tarjetas y claves falsas o sustraídas o de sus datos**, Incorporado al Código Penal Argentino por ley 25.930 que introdujo en inc. 15 al art. 173. La norma contempla diferentes supuestos - es el uso de la información de una tarjeta de crédito sea con o sin el plástico, este supuesto se aplica aunque lo hiciere por medio de una operación automática. Esta última modalidad ha receptado la posibilidad de estafar a sistemas automatizados.

Por tratarse de un supuesto especial del delito de estafa, el cual es un delito de resultado, ambos subtipos de defraudación previstos en el **inc. 15 del art. 173 CP** requieren para su consumación la realización de un perjuicio patrimonial que sea real y efectivo, y constituya una disminución del valor económico del patrimonio del sujeto pasivo provocado como consecuencia del accionar del autor. Por consiguiente, la tentativa es admisible en tanto y en cuanto existe la posibilidad de que una vez iniciada la maniobra fraudulenta, la misma no pueda concretarse por razones ajenas a la voluntad del sujeto activo.

En la actualidad existen organizaciones internacionales dedicadas a intercambiar este tipo de información con fines delictivos. En el año 2008 autoridades norteamericanas decidieron combatir este delito, y en la operación denominada "SHADOWCREW" (VER ANEXO 6 - CASO SHADOWCREW) desbarataron una banda formadas por individuos alrededor del mundo que se dedicaba a este cambio Este Sistema no solo puede falsificar la tarjeta de crédito sino también la de débito.

ALTERACIÓN DE REGISTROS INFORMÁTICOS: Previsto en el art. 173 inc. 16 CP. Es una de las formas más tradicionales de realizar estafas informáticas. En la misma se altera un registro informático, cuyo contenido el sistema toma en cuenta para adoptar decisiones de pago o de disposiciones patrimoniales. Así el sujeto activo obtiene fraudulentamente sumas de dinero o beneficios, que de otra manera no le corresponderían. Ejemplo de ello es aquel que accede a la cuenta bancaria y altera el monto, para tener más dinero del que le corresponde o se realiza una transferencia no autorizada a la misma. Esto es, en parte, aquello que legisla la ley tributaria al penalizar la modificación de registros de la AFIP que tengan finalidades impositivas, con fines de defraudar al Fisco.

LA ESTAFA NIGERIANA: consiste en ilusionar a la víctima con una fortuna inexistente y persuadir para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Estas pueden realizarse por distintos medios como email, Whatsapp, etc. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con la fortuna que las víctimas esperan recibir. La estafa nigeriana puede entenderse como una versión contemporánea del llamado cuento del tío. (VER ANEXO 7 - ESTAFA NIGERIANA)

EL ROBO DE IDENTIDAD: aún no tipificada, cabe hacer la siguiente distinción:

- **Suplantación de identidad**: Suele ser realizada por la creación de un perfil falso, pero con la identidad de otra persona a la que se pretende suplantar.
- **Robo de identidad:** Se produce cuando el que suplanta la identidad lo realiza por haber sustraído los datos de acceso a Internet y redes sociales.

En ambos casos la gravedad del hecho es el mismo, la suplantación de identidad de otra persona, con fines presumiblemente delictivos.

SKIMMING: es aquel supuesto en se utilizan dispositivos unidos a una laptop y disimulados en el cajero automático con el fin de copiar datos sensibles de diferentes clientes de tarjetas de crédito para posteriormente, proceder a su duplicación. Este mecanismo, es considerado idóneo para cometer una defraudación por lo cual la jurisprudencia lo ha incluido entre los casos previstos en el art. 173 inc. 5º del Código Penal,

Asimismo también se considera delito la mera tenencia de instrumentos destinados a la falsificación, aún en los casos en que no se haya acreditado la existencia de movimientos destinados a cometer este delito. Se recurre al delito de tenencia de elementos destinados a cometer falsificaciones en concurso material con tentativa de defraudación porque con estos datos se crean tarjetas de crédito falsas[27]. Sin embargo otros tribunales entienden que la mera clonación no alcanza, pero que sí cabe dentro del tipo especial de defraudación.[28]

PHISHING: Los ejemplos a dar son infinitos, pero la modalidad siempre coincide, una alerta o la promesa de un beneficio, a tan solo un click de distancia, que deriva a un archivo o un enlace. La consecuencia, deriva en diferente escenarios pero todos nocivos, un enlace (una dirección URL, el www._____.com, que nos redirija a una página para completar un formulario con información sensible, según como haya sido esa captación, poder incluir nombres, documentos, personas con la vivimos o deseamos beneficiar, incluso tarjetas de crédito, en el cual preparamos el banquete para los ciberdelincuentes. Seguramente el despliegue de los ciberdelincuentes haya tenido antecedentes a través de noticias falsas distribuidas por la redes sociales incluso Whatsapp, que incluso facilitamos la distribución, compartiendolas. Así se prepara el banquete de datos, datos que son mega lucrativos en la DARKWEB, que haciendo un paralelismo es un Mercado Libre ilícito, que incluso se clasifican entre sí. Se recopila la

[27] Castellini, Alfredo J. y otros (2005). CN Crim y Corr., Sala 7.

[28] Oliveira Rivas, Fabio y otros (2008). CN Crim y Corr., Sala 4.

información (datos) se segmenta y hacen bases de datos masivas a modo de "combos" a cifras que mínimo superan los 4 dígitos. (VER ANEXO 8 - PHISHING. PREVENCIÓN)

Ese primer delito deriva en otros, ya que con esos datos, pueden suplantar la identidad haciéndose pasar por nosotros en esa comunidad, hacer operaciones financieras o a modo "loop" volver a captar más y nuevos datos por medio de la técnica inicial phishing,

También mientras creíamos estar seguros en nuestros hogares, la peligrosidad puede darse que el archivo que abrimos, infecte a todo nuestro dispositivo, sería como una "inhalación digital" invisible que como la historia del caballo de Troya, ingresan para hacer un caos, por eso también se los llaman virus troyanos. Durante el COVID - 19, ha crecido cada vez más estos virus conocidos como "EMOTET", TRICKBOT, AZORULT, camuflados en un pdf o archivo Excel o de descarga automática al recurrir al enlace.

Por último me resta hablar de la tipificación en nuestro código de fondo, el phishing está regulado en el inciso 16 del art. 173 CP, por lo tanto se lo considera como un tipo especial de la estafa común del art. 172 CP.

5. CÓDIGO DE FONDO. DELITOS TIPIFICADOS Y NO TIPIFICADOS

La **Ley 26.388 denominada de delitos informáticos** ha incorporado las figuras típicas a diversos artículos del Código Penal de la Nación. Incorpora a las nuevas tecnologías como medios de comisión de distintos tipos previstos en el Código Penal. Es así que la ley generó un número muy limitado y específico de tipos penales y la reforma o actualización de otros ya existentes como:

- **Ofrecimiento y distribución de imágenes de pornografía infantil (art. 128 y ss);**
- **Violación de correspondencia electrónica (art. 153 CP);**
- **Acceso ilegitimo a un sistema informático (art. 153 bis CP);**
- **Publicación abusiva de correspondencia (art. 155 CP);**
- **Revelación de secretos (art. 157 CP);**
- **Delitos relacionados con la protección de datos personales (art. 157 bis CP);**
- **Defraudación informática (art. 173 inc. 16 CP);**
- **Daños a los sistemas informáticos tanto tangibles (hardware) como intangibles (software) (art. 183 y 184 CP);**
- **Interrupción o entorpecimiento de las comunicaciones (art. 197 CP);**
- **Alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP), a los que deben agregarse las terminologías (art. 77 CP);**

- **En cuanto a la defraudación de derechos de propiedad intelectual está previsto en los arts. 71 y ss. de la ley 11.723, modificada por la ley 25.036 de 1998.**

Asimismo existen proyectos de ley para nuevas incorporaciones, pero hasta ahora a modo de "parche".

Existen otros delitos no tipificados aún, dado que el avance de la tecnología hace que la legislación nunca pueda terminar de tipificar la cantidad de delitos nuevos que existen y que van apareciendo con los nuevos tiempos. Por eso hay delitos que no fueron contemplados en la ley 26.388, aunque para muchos de ellos ya hay proyectos de ley que permitirá incorporarlos al Código Penal. Entre los que podemos mencionar están: Robo y Suplantación de Identidad; Ciberocupación; Ciberacoso; Ciberbullying; Sexting; "Porno Venganza"; Spamming.

6. OTROS: LA "INFODEMIA". FAKE NEWS DURANTE LA PANDEMIA

Las *fake news* o noticias falsas son informaciones que han sido manipuladas, tergiversadas e incluso inventadas con un objetivo específico.

Con el uso de internet se ha hecho muy sencillo no solo crear noticias falsas, sino transmitirlas, por lo cual es muy frecuente que un contenido de este tipo se vuelva viral en pocas horas o días. Y si bien se puede intentar revertir su efecto (desmintiendo los hechos que se afirman en la supuesta noticia o corrigiéndola), lo cierto es que **esta medida no suele tener el mismo impacto que generó la noticia falsa.**

Debe tenerse en cuenta, que desinformar y confundir son actos preparatorios de los que se vale inicialmente un cibercriminal, creando así un contexto para luego mediante el uso de técnicas de ingeniería social incrementar las probabilidades de su objetivo.

En el contexto actual de pandemia desde enero 2020 incrementaron notablemente los dominios registrados en la red vinculados con el COVID, creándose tan solo en los primeros 90 días más de 1500 dominios, algunas legítimas y otras con el fin de difundir información erróneas con el fin de cometer phishing y otros fraudes, valiéndose de técnicas de ingeniería social como advertí, aprovechando la angustia, estrés, miedo y confusión. [29]

[29] Litvin, Jorge L. (2020). HACKEADOS - Delitos en el mundo 2.0 y medidas para protegernos. (Publicación Digital) Buenos Aires, Argentina.

Por último, en atención al principio de ULTRAACTIVIDAD[30] de la ley penal, referida a la validez temporal de la ley penal, el cual adquiere especial relevancia en 2 situaciones: que paso a describir. En primer lugar, cuando se trata de **leyes temporales**, que prevén en su texto su tiempo de vigencia y en segundo lugar, las **leyes excepcionales**, donde su vigencia depende de la subsistencia de situaciones que por su índole son temporales o transitorias.

En ambos casos se trata de situaciones de excepción, y la finalidad por lo general consiste en reforzar la protección de ciertos bienes jurídicos por lo que se prevén incriminaciones o aumentos de pena excepcionales. Cuestiones que atienden a la regla de irretroactividad de la ley penal y sus excepciones: el principio la ley más favorable y también de la ultraactividad en los casos ut supra mencionados.

¿No ameritaba, y aún hoy, crear una ley excepcional (mientras dure la pandemia, o el contexto ASPO/DISPO) **que incremente la pena para los delitos cometidos en el ciberespacio, dado que era el único medio para contactarnos entre nosotros?**

[30] Righi, Esteban (2016). Derecho Penal. Parte General. Segunda Edición (p. 111 y 112). Buenos Aires, Argentina.

CAPÍTULO 5

CIBERESPACIO Y ÁMBITO DE VALIDEZ ESPACIAL

1. INTRODUCCION

El motivo por el cual traigo a colación estos conceptos se debe a que ningún ordenamiento jurídico puede pretender validez universal -espacial y temporal-, lo que acarrea la existencia de estos ámbitos de estudio, sin perjuicio que en nuestra nación conforme al art. 16 CN, somos todos iguales frente a la ley, aunque con ciertas limitaciones funcionales.

Como en el trabajo que vengo desarrollando hago referencia al nuevo ámbito delictivo denominado **CIBERESPACIO,** considero oportuno recordar estos pilares de ámbitos de validez que rigen al derecho penal, que se presenta como obstáculo a la hora del ejercicio de la pretensión punitiva estatal. Por lo tanto es válido soslayar algunos preceptos en base a los ámbitos de validez espacial junto a las excepciones en razón de la personas (como excepción al principio de igualdad) que limitan la aplicación de la penal.

1.1. AMBITO ESPACIAL [31]

El problema radical que debe tratarse consiste en determinar a qué hechos le deben ser aplicadas las normas penales, lo que a priori corresponde a cada Estado en función de su soberanía para satisfacer su propio poder punitivo.

Para la determinación de lo planteado ut supra, debe partirse del **principio de territorialidad**, donde la ley que corresponde aplicarse a un hecho en concreto, es la ley penal del Estado donde fue cometido (territorio) sin importar la nacionalidad del autor (principio de igualdad art 16 CN).

Existen casos, donde el responsable de un delito, luego de la comisión del mismo viaja al exterior se aplica el **procedimiento de extradición,** lo que habilita como sistema normativo, el enjuiciamiento y la aplicación del derecho penal de un Estado a un sujeto que se encuentra materialmente bajo la autoridad de otro Estado.[32]

[31] Righi, Esteban (2016). Derecho Penal. Parte General. Segunda Edición (p. 98 y ss). Buenos Aires, Argentina.

[32] Como el caso de Wikileaks. / panamá papers.

1.1.1. PRINCIPIO DE TERRITORIALIDAD

Es el Estado soberano quien tiene la facultad de ejercer coacción jurídico penal en relación a las acciones cometidas en su territorio, y demás lugares sometidos a su jurisdicción, ya sea en relación a los responsables de un hecho punible como en la comunidad internacional.

El principio de territorialidad, surge de la regla consagrada en nuestro código de fondo, según la cual el código penal se aplicará "por delitos cometidos... en el territorio de la nación Argentina o en los lugares sometidos a su jurisdicción (art 1, inc. - 1 hipótesis - CP).

La consecuencia es que la ley penal se aplica al autor del hecho, sin importar su condición de nacional o extranjero, domiciliado a transeúnte, pues lo determinante es que el delito haya ocurrido en el territorio de la Nación. El fundamento del principio territorial recogido por la norma antes mencionada, encuentra fundamento en que todas las personas deben respetar la ley del Estado en que se encuentran. Aseveración que obliga a establecer tanto el concepto de *territorio,* como el de lugar de comisión.

El concepto de ***territorio,*** que viene dado por el derecho internacional, resulta comprensivo de: el *espacio territorial* comprendido dentro de los límites fijados geográfica o políticamente; las aguas jurisdiccionales (art. 2340 CCCN); el subsuelo y el espacio aéreo correspondiente a los límites precedentemente fijados. Considero aquí que la definición se encuentra desactualizada en razón al ciberespacio.

Por otra parte, el principio de territorialidad se complementa con **la *teoría del territorio flotante o principio del pabellón*** (bandera), haciendo extensiva la aplicación del código penal a "*los delitos cometidos*... ***en los lugares sometidos a jurisdicción"*** de la Nación Argentina (art. 1 inc. 1 CP), referida está -la jurisdicción- a los hechos cometidos en buques o aeronaves que lleven su bandera. Debiendo distinguirse según la doctrina dominante entre aquellos bienes (buques o aeronaves - art. 201 C.Aer.), que son *públicos y privados*, ya que los públicos siempre son considerados territorio del Estado, y rige siempre la aplicación de la ley del pabellón, sea que se encuentren en aguas jurisdiccionales o en altamar (aspectos que son estudiados en la rama del Derecho Internacional Público). La misma ley rige respecto de los buques privados mientras no ingresen en aguas territoriales de otro Estado, quedando sometidos a la ley del lugar, habiendo anticipado que el territorio de una nación también se extiende al *espacio marino* sobre el cual continúa ejerciendo su soberanía, y por ello la importancia del alcance de lo entendido por territorio. Mientras que las aeronaves *privadas* están regidas por el derecho argentino cuando se produce una infracción a leyes de seguridad pública, militares, fiscales, reglamentos de circulación aérea, lesiona la seguridad y el orden

público. No mediante extradición (procedimiento citado anteriormente), también se aplica la ley argentina, cuando el primer aterrizaje posterior al hecho se produce en nuestro territorio (art 200, C. Aer.). **¿Será esta una posibilidad de aplicación al ciberespacio?**

Por otra parte, si bien **no queda comprendido dentro del concepto de territorio** el edificio en el que se instalan las embajadas argentinas en el exterior y en consecuencia, tampoco se excluye el derecho argentino respecto de hechos cometidos en las edificaciones donde se han establecido embajadas de países extranjeros ante nuestro país, *inmunidades* respecto a determinadas personas o lugares. Cuestiones también estudiadas bajo la rama del derecho internacional público.

Lo que sí interesa revisar, para cuestionar **cómo son tratados los delitos que son realizados en el nuevo espacio o "no lugar**", escapando a ciertos dogmas, es que a los efectos de la aplicación del principio de territorialidad, incide el concepto de *lugar de comisión del delito*, cuya determinación gira en torno a los siguientes Teorías:

Teoría de la Acción: Los seguidores de la ***teoría de la acción*** vinculan la cuestión con la definición del *tiempo* de comisión del delito, postulando así una respuesta unitaria. A este punto de vista se adjudica la virtud de considerar la ley aplicable teniendo en cuenta el lugar de *manifestación de la voluntad*, lo que ofrece soluciones más adecuadas para resolver los casos en que el hecho es realizado por un inimputable. Además, la teoría de la acción resulta preferible cuando se han producido cambios legislativos, existen dificultades para determinar el resultado.

Teoría del Resultado: En contrario sensu existe otra teoría que considera que el derecho aplicable se determina en relación al lugar que la serie causal en curso alcanzó al objeto amenazado, es decir el lugar del resultado. El fundamento es que corresponde al Estado que padece el resultado, sancionar la alteración del orden doblegado.

Teoría de la Ubicuidad: siendo esta la dominante en nuestro país, tanto por la CSJN como por la doctrina, según la cual el delito debe considerarse cometido tanto en el lugar donde se ejecutó la acción como donde se produjo el resultado. Con la salvedad que si el delito fuese del tipo de omisión, se considera aplicable el derecho del del lugar donde el omitente debió actuar

1.1.2. EXTRATERRITORIALIDAD

Existen situación donde resulta insuficiente el principio de territorialidad, para tutelar los bienes jurídicos situados en el país, lo que hace necesario recurrir a la aplicación

extraterritorial de la ley penal, siendo supuestos en los que se justifica su aplicación a hechos ocurridos fuera del territorio del Estado, en función los principios Real o de Defensa; Nacionalidad o Personalidad y Universal. Los que paso sucintamente a desarrollar.

1.1.3. PRINCIPIO REAL O DE DEFENSA

Como anticipa, ante supuestos que ponen en relieve la insuficiencia del principio territorial, nuestro derecho consagra el principio real o de defensa, donde se aplica la ley a delitos cometidos por extranjeros o nacionales, fuera del territorio del país o de los lugares sometidos a su jurisdicción, pero cuyos efectos deben producirse en ellos. Principio que se consagra mediante normas que prevén la aplicación de nuestro Código Penal a delitos "cuyos efectos deben producirse en el territorio de la nación Argentina o en los lugares sometidos a su jurisdicción" (art. 1 inc. 1 CP) como también "por delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo" (art. 1 inc. 2 CP).

La norma al aludir a delitos cometidos en el extranjero no se refiere a **delitos cometidos a distancia,** como es el caso de cuando se comete un homicidio mediante el envío de un paquete que contiene una bomba, **si la acción se cometió en el extranjero y el resultado se produjo en el país**. Es que en realidad, en esos casos la aplicación del derecho argentino es consecuencia del principio de territorialidad, porque ese homicidio ha sido cometido en el país, lugar de la consumación. Igual consideración merece la tentativa comenzada ejecutar en el extranjero para que sea consumado en el país, pues conforme al principio territorial rige en la tentativa la ley del lugar donde se preveía la producción del resultado.

No debe confundirse con efectos, lo cual es controvertido y suele confundirse. Sin embargo, si el resultado se produjo en el país, el delito debe entenderse como cometido en territorio nacional y es aplicable el principio general de territorialidad. Distinta es la situación cuando de lo que se trata es de aplicar el derecho argentino a delitos cometidos en el exterior, pero que produjeron efectos en nuestro país. Así por ejemplo, un falso testimonio rendido en otro país por exhorto diplomático ha sido cometido fuera pero como el bien jurídico se encuentra en territorio nacional, produce efectos dentro del país. En consecuencia, la expresión efectos del delito no debe entenderse como sinónimo de resultado.

Continuando con los efectos, la norma alude a los bienes jurídicos que pretende proteger, como lo prevén los tipos de traición (art. 214 CP) o falsificación de moneda (art. 282 CP) que si bien han sido cometidos en el extranjero, resulta aplicable la ley argentina porque son susceptibles de producir efectos en el país, por afectar el orden constitucional o la

incolumidad de nuestro signo monetario. Siendo hechos cometidos fuera de la nación pero se dirige a bienes jurídicos que se encuentran dentro del territorio nacional, pudiendo tratarse de la afectación de bienes **supraindividuales,** como el caso de los tipos ya mencionados o bien el falsedad de documentos nacionales (art. 292 CP) o alteraciones del orden público (art. 209 y ss. CP).

Principio que no se aplica ante hechos que lesionan o ponen en peligro bienes **individuales**, casos donde se suele aplicar el principio de nacionalidad pasivo.

Nuestro derecho, por otra parte, alcanza a los delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo (art. 1 inc. 1 cp), en aras de proteger el interés de proteger la incolumidad de la función pública.

Cuando nos encontramos frente a un delito de omisión, puede incidir este principio cuando no coincide el ámbito territorial en que el sujeto se encuentra con el del lugar en que debió obrar, por ejemplo si el sujeto abandona a una persona incapaz impedida de valerse por sí misma y a la que debe mantener y que está en el país (art 106 CP), siendo esta una hipótesis de aplicación de la ley argentina en razón del principio real o de defensa.

En los delitos impropios de omisión, cuando se imputa un resultado ocurrido en el país a un omitente que está en el exterior, puede entenderse que la consumación en territorio nacional hace aplicable nuestras normas por el principio de territorialidad. Pero aun admitiendo que en todos los casos de omisión prevalece el lugar donde el autor debió obrar, resulta contradictorio fundamentarse en el principio territorial en relación a que todo individuo debe respetar la ley del sitio en que se encuentra, pero precisamente el omitente no está en ese lugar.

1.1.4. PRINCIPIO DE LA NACIONALIDAD O PERSONALIDAD

Si bien es un principio en desuso por el derecho contemporáneo, es dable destacar que este principio surgió como una exageración de la doctrina de las nacionalidades, que pretendía que todo sujeto fuera juzgado conforme al derecho de su país, lo que admite como posibilidades que la ley aplicable esté determinada por la nacionalidad del autor (principio de nacionalidad activo) o de la víctima del delito (principio de nacionalidad pasivo).

En nuestro derecho, se asoman manifestaciones de este principio, en las normas que preveían la aplicación de la ley penal argentina respecto de delitos cometidos en el extranjero,

cuando se denegaba la extradición en función de la nacionalidad Argentina de la persona requerida (Ley 1612, art. 3 inc. 1 y 5).

Hoy en razón al sistema de cooperación internacional rigen en materia penal (Ley 24.767), criterios que favorecen el principio de juzgamiento por tribunales competentes, y asociado a criterios de inmediatez en materia procesal, en cuya virtud debe existir coincidencia territorial entre el lugar de comisión del hecho y el tribunal de enjuiciamiento. Por lo tanto, si el requerido para la realización de un proceso fuese nacional argentino, estaría solo en condiciones de optar por ser juzgado por los tribunales argentinos, si no fuera aplicable al caso "un tratado que obligue a la extradición de nacionales" (Ley 24767, art.12, párr. 1). La calidad y nacional argentino deberá haber existido al momento de comisión del hecho, y subsistir al momento de la opción (párr 2). Si el nacional ejercer esta opción, la extradición será denegada, debiendo en ese caso ser juzgado en el país según la ley argentina, siempre que el Estado requirente preste conformidad para ello, renunciando a su jurisdicción, y remita todos los antecedentes y pruebas que permitan el juzgamiento (párr. 3).

Sí fuere aplicable al caso un tratado que faculta la extradición de nacionales, una vez declarada procedente en sede judicial, el poder ejecutivo resolverá si hace o no lugar a la opción (art. 12, párr. 4 y 36), considerando la existencia u ofrecimiento de reciprocidad (art. 3). Mientras que no procederá la extradición cuando existan razones de soberanía nacional, seguridad y orden público, u otros intereses esenciales para la Argentina, que tornen inconveniente el acogimiento del pedido del país requirente (art. 10).

1.1.5. PRINCIPIO UNIVERSAL O DE JUSTICIA MUNDIAL

Por otra parte, en virtud del principio universal o de justicia mundial, un estado aplica su propio derecho aunque el hecho haya sido cometido por un extranjero fuera de su territorio, motivado por el fundamento que están en juego bienes jurídicos protegidos universalmente, o autores peligrosos para todos los estados civilizados, sea por la finalidad perseguida o la forma de ejecución.

Una referencia a este principio, surge del texto constitucional, según la cual cuando el delito "se cometa fuera de los límites de la Nación, contra el Derecho de Gentes, el Congreso determinará por una ley especial el lugar donde haya de seguirse el juicio" (art. 118 CN). Destacando que existen reglas vinculadas a la aplicación de este principio en numerosas convenciones internacionales.

Por razones de política criminal, se vuelve innecesario tomar en cuenta el derecho vigente en el lugar del hecho, por tratarse de la persecución de delitos reprobados en general, o cometidos por organizaciones internacionales, siendo aconsejable que esto ocurra allí donde el autor es apresado. Debido a que este principio tutela bienes jurídicos reconocidos por todas las naciones civilizadas, atacados por bandas de delincuentes organizadas internacionalmente, de modo que en abstracto cada hecho sería peligroso para cada nación.[33]

En definitiva, aplicar este principio resulta una intromisión inadmisible que surge del derecho internacional, ya que de alguna forma busca actuar contra la voluntad de los Estados en cuyo territorio ocurrieron los hechos, y de conformidad con la de aquellos a los que pertenecen las víctimas. Razón por la que todo supuesto en que un Estado pretenda aplicar unilateralmente el derecho penal propio, procurando intervenir en las cuestiones de otro Estado, deberá considerarse un límite a este principio.

1.1.6. PRINCIPIO DE ADMINISTRACIÓN DE JUSTICIA PENAL

Este principio de representación de naturaleza subsidiaria, tiene fundamento en la solidaridad interestatal y acotado a los bienes jurídicos más importantes, rigiendo cuando un Estado que por alguna razón no hizo lugar a la extradición, aplica en cambio su propia ley.

1.2. VALIDEZ TEMPORAL (EN BREVES LÍNEAS)

1.2.1. PRINCIPIO GENERAL: IRRETROACTIVIDAD

En materia de validez temporal de la ley penal, rige la regla general según la cual se aplica la ley vigente en el momento de comisión del delito. Dicha regla es consecuencia del principio de legalidad, en cuya virtud las leyes penales rigen para el futuro. Por lo tanto *"es un presupuesto de punibilidad, que la incriminación derecho es anterior a su comisión*".[34]

El principio de legalidad con jerarquía constitucional, prohíbe la aplicación retroactiva de la ley, comprendiendo esa exigencia de ley previa: la previsión del hecho como punible; la amenaza de pena; las medidas de seguridad; y las consecuencias accesorias.

[33] Günther Jackobs, (2002). Los pormenores del tipo objetivo mediante la acción, en Imputación objetiva y antijuridicidad. Estudios de Derecho Penal (p. 135).

[34] Günther Jackobs / Claus Roxin

Este principio de legalidad también se plasma en el código de fondo civil y comercial que establece "las leyes no son obligatorias sino después de su publicación, ideas del día que determinen. Si no designan tiempo, serán obligatorias después de los ocho días siguientes al de su publicación oficial" (art. 2 CCCN).

Lo que vengo desarrollando implica un lineamiento por el cual la ley afecta solamente los hechos cometidos después de su entrada en vigencia y antes de su derogación, lo cual requiere considerar que debe entenderse como momento de comisión: 1) el momento en que se ejecutó la acción, 2) la omisión propia, cuando debía ejecutarse la acción omitida, y 3) en los delitos impropios de omisión, el momento en que se produjo el resultado que el omitente no impidió.

Es dable destacar que la determinación del momento de comisión requiere otras precisiones como ser, 1) considerar que un autor mediato realiza la acción, cuando comienza a utilizar al instrumento, 2) respecto de coautores y cómplices, se toma en consideración el momento en que concretan su primer aporte al último hecho, 3) en los delitos continuados, la acción se realiza desde el primero hasta el último hecho, y 4) en los permanentes, cuando se crea el estado típico constitutivo del delito.

Así las cosas es dable destacar que existen teorías preventivas de la pena, que fundamentan la exigencia de la ley previa, ya que para que una norma penal pueda motivar a sus destinatarios, debe ser previa a la comisión del hecho punible. Pero el principio de irretroactividad recibe una fundamentación decisiva, en principios constitucionales vinculados a la seguridad jurídica.

EXCEPCIONES A ESTE PRINCIPIO RECTOR: El principio de irretroactividad no es absoluto pues resultan de aplicación las leyes penales posteriores a la comisión del hecho siempre que resulten más favorables para el acusado lo que constituye una excepción prevista para proteger al ciudadano.

Se inspira esta excepción en un motivo político social que fundamenta la aplicación retroactiva de una ley posterior más benigna, ya que carece de sentido dictar o mantener la ejecución de penas por hechos que ya no se consideran delitos, o en su caso tienen previstas penas que se aprecian desproporcionadas.

Por lo tanto podemos decir que de acuerdo al derecho vigente "si la ley vigente al tiempo de cometerse el delito fuere distinta de la que exista al pronunciarse el fallo con el tiempo intermedio, se aplicará siempre la más benigna. Si durante la condena dictaron la ley

más benigna, la pena se limitará a la establecida por esta ley. En todos los casos del presente artículo, los efectos de la nueva ley se operará de pleno derecho" (art 2 CP).

La aplicación retroactiva de la ley penal más benigna es denegada en relación a las medidas de seguridad totalmente la unos casos y parcialmente en otra, con lo que se omite considerar que por tratarse de restricciones coactivas de derechos previstos en leyes penales no hay fundamento suficiente para no aplicar principios análogos a los que rigen respecto de las penas (art. 2. CN).

ULTRAACTIVIDAD: Por último este principio de ultractividad adquiere singular relevancia en dos supuestos: el primero, cuando se trata de leyes temporales, porque en su texto está fijado de antemano su tiempo de vigencia; el segundo, leyes excepcionales, cuando la vigencia depende de la subsistencia de situaciones que por su índole son temporales o transitorias.

A modo de comentario personal, considero que dada la cantidad de estafas realizadas en el ámbito del ciberespacio, deberían haber derivado en la sanción de una ley que aseverar las penas mientras perdure la pandemia.

2. DETERMINACIÓN DE LA COMPETENCIA. ÁREA GEOGRÁFICO-POLÍTICA[35]

2.1 INTRODUCCION [36]

Considerando que la jurisdicción es el poder del Estado de juzgar o de ejercer la función judicial, la competencia es la medida en que ese poder del Estado le es dado a un tribunal determinado. La competencia delimita la zona de conocimiento, intervención, decisión y ejecución del juez o tribunal, determinando el **espacio,** materia y grado de los asuntos que le incumben. La competencia es improrrogable por simple voluntad de los sujetos de un procedimiento. Además, es inalterable, ya que el único parámetro para atribuir competencia a un tribunal es la ley y, por lo tanto, deviene en absoluta.

[35] Parada, Ricardo Antonio ; Errecaborde, José Daniel (2018). Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet. Buenos Aires, Argentina.

[36] Darahuge, María E. - Arellano González, Luis. Empleo de las direcciones virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad. (p. 183 y 189).

De ahí que sea sumamente importante establecer con claridad y precisión reglas que permitan deslindar la misma en los casos en los que ocurre oposición a recibirla o reclamo para ejercerla por parte de un determinado tribunal ("aceptación de competencia o declaración de incompetencia" normalmente sometida al arbitrio del respectivo superior).

En nuestro caso, nos abocaremos al problema de **determinar dicho espacio de competencia, en relación con el área geográfico-política** donde ocurrió un determinado evento susceptible de judicialización.

Por el contrario, no pretendemos decidir sobre las múltiples cuestiones que facultan o sustentan a un tribunal en su declaración de incompetencia, sino **aportar un elemento de decisión más a dicha cuestión y su posterior aprobación** o desestimación por parte del superior que resuelve el incidente cursado. Este elemento es la ubicación, cierta, precisa y delimitada de un evento físico en cuanto a su **ocurrencia espacial y geográfica** a partir de los datos resguardados como resultado de un **evento digital asociado al tema a dilucidar.**

2.2. CONCEPTOS DESTACADOS

- La competencia provincial es la regla y se ocupa del juzgamiento de los delitos comunes y contravenciones o faltas dentro de cada provincia.
- La territorialidad es la nota característica de la competencia. Es decir, los jueces, por regla, son competentes para resolver todas las causas suscitadas en el territorio que la ley les asigna para el ejercicio de su jurisdicción.
- La primera regla es que el juez competente es el del lugar de comisión del delito, su base dogmática se encuentra en el artículo 118 de la CN. Para llevar a la práctica esta regla, cada provincia, al dictar las leyes orgánicas del Poder Judicial, ha dividido sus territorios dentro de cuyos límites se atribuye la competencia penal a un juez o grupo de jueces entre los cuales se reparte, a su vez, el conocimiento de las causas. Sobre la base de esta distribución no debería quedar ningún espacio del territorio sin juez.
- La finalidad se funda en la **proximidad** del tribunal al lugar del hecho para favorecer la garantía de defensa en juicio y el principio de economía procesal, pues favorece la rápida, sencilla y más económica investigación.
- Aunque el problema de la competencia afecta transversalmente a la totalidad de la jurisdicción y los distintos fueros del derecho argentino, pondremos énfasis en el **derecho procesal penal**, ya que las nuevas modalidades delictivas soportadas en medios digitales

(narcotráfico, trata de personas, pornografía infantil, terrorismo, entre otros) agregan un nuevo componente de incertidumbre a dicha problemática.

Este potencial se relaciona con ciertos problemas que, aunque integran el derecho internacional público, no están absolutamente definidos y delimitados.

Código Procesal Penal de la Nación / Libro I / Título III / Capítulo II / Sección Tercera y Cuarta:

DETERMINACIÓN DE LA COMPETENCIA

Determinación - Art. 34*: "Para determinar la competencia se tendrá en cuenta la pena establecida por la ley para el delito consumado y las circunstancias agravantes de calificación, no así la acumulación de penas por concurso de delitos de la misma competencia.*

Cuando la ley reprima el delito con varias clases de pena, se tendrá en cuenta la cualitativamente más grave".

Declaración de Incompetencia - Art. 35: *"La incompetencia por razón de la materia deberá ser declarada aun de oficio en cualquier estado del proceso. El tribunal que la declare remitirá las actuaciones al que considere competente, poniendo a su disposición los detenidos que hubiere.*

Sin embargo, fijada la audiencia para el debate sin que se haya planteado la excepción, el tribunal juzgará los delitos de competencia inferior".

Nulidad por Incompetencia - Art. 36: *"La inobservancia de las reglas para determinar la competencia por razón de la materia producirá la nulidad de los actos, excepto los que no pueden ser repetidos, y salvo el caso de que un tribunal de competencia superior haya actuado en una causa atribuida a otro de competencia inferior".*

COMPETENCIA TERRITORIAL

Reglas Generales - Art. 37: *"Será competente el tribunal de la circunscripción judicial donde se ha cometido el delito.*

En caso de delito continuado o permanente, lo será el de la circunscripción judicial en que cesó la continuación o la permanencia. En caso de tentativa, será el de la circunscripción judicial donde se cumplió el último acto de ejecución".

Regla Subsidiaria - Art. 38: *"Si se ignora o duda en qué circunscripción se cometió el delito, será competente el tribunal que prevenga en la causa".*

Declaración de Incompetencia - Art. 39: *"En cualquier estado del proceso, el tribunal que reconozca su incompetencia territorial deberá remitir la causa al competente, poniendo a su disposición los detenidos que hubiere, sin perjuicio de realizar los actos urgentes de instrucción".*

Efectos de la declaración de Incompetencia - Art. 40. *"La declaración de incompetencia territorial no producirá la nulidad de los actos de instrucción ya cumplidos"*

El momento de la comisión de un delito: en principio, un delito penal se considerará cometido en el lugar de su consumación definitiva, cuando ya se realizaron todos los actos previstos por la ley como constitutivos del delito. Pero no todos los casos se presentan de manera sencilla. Si el delito ha sido tentado, en ese caso, será competente el juez del lugar donde se cumplió el último acto de ejecución. Si se tratara de un delito continuado (varias acciones típicas autónomas que se consideran como un solo delito, como una sola acción típica que se prolonga en el tiempo), será competente el juez del lugar donde cesó de cometerse. Finalmente, si se ignora o duda en qué lugar se cometió el delito, será competente el juez que primero haya prevenido.

En cualquier estado del proceso, el tribunal que reconozca su incompetencia territorial deberá remitir la causa al competente, poniendo a disposición a los detenidos, si los hubiere. Sin perjuicio de realizar los actos urgentes de la investigación. La declaración de incompetencia territorial no produce la nulidad de actos cumplidos.

Otras formas de competencia son aquellas delimitadas por la materia, por conexidad, por acumulación de procesos

Cuestiones de competencia: son aquellas que surgen cuando dos órganos jurisdiccionales se declaran en forma simultánea y contradictoria competentes o incompetentes para la investigación o juzgamiento de un mismo hecho. Asimismo, se presenta de modo **positivo** cuando dos o más jueces pretenden conocer del mismo hecho, y de manera **negativa**, cuando rehúsan su intervención. El conflicto surge tanto cuando el juez decide oficiosamente sobre su competencia o cuando ello es planteado por las partes.

Inhibitoria, declinatoria: el trámite para resolver estos conflictos se concreta mediante la "inhibitoria" o "declinatoria". Si ante los referidos planteos los jueces no aceptan lo pertinente, corresponde la decisión a quien resulte superior jerárquico común de los enfrentados.

Las cuestiones de competencia no suspenderán la investigación que será continuada por el juez que primero haya conocido en la causa. **Este punto es muy importante en el tema que vamos a analizar, ya que la celeridad y la confidencialidad en los actos preliminares a la constitución de prueba documental informática son de tal pertinencia que su retraso puede derivar en la pérdida o nulidad de los elementos probatorios necesarios para delimitar físicamente el evento y decidir sobre la competencia en ciernes.** Al respecto, todos los actos practicados hasta la definición del tribunal competente serán válidos, aunque el tribunal a quien corresponda definitivamente el proceso podrá ordenar su ratificación y/o ampliación.

2.3. LA PROBLEMÁTICA TECNOLÓGICA

Considerando que la evolución de la tecnología nos ha llevado a escindir el conocido "lugar del hecho", en sus nuevas versiones: lugar del hecho real (LHR), lugar del hecho virtual impropio (LHVI) y lugar del hecho virtual propio (LHVP), deviene necesario analizar cada una de las situaciones que estos novedosos escenarios implican para establecer la ubicación cierta de un componente digital determinado o determinable.

2.3.1. LUGAR DEL HECHO REAL (LHR)

El lugar del hecho real es el área definida y determinada en espacio y tiempo donde ocurre un evento o una serie de ellos. Los operadores del derecho están familiarizados con el mismo y acostumbrados a gestionarlo con solvencia judicial (en particular, procesal meridiana). Múltiples teorías respecto de la competencia a partir de la ubicación geográfica del mismo han obtenido una serie muy extensa de resultados jurisprudenciales que avalan la resolución de un problema de competencia basado en el territorio. No es motivo de este trabajo analizar sus pormenores e implicancias jurídicas. Sin embargo, es imprescindible considerar:

Toda información es información codificada (en cualquier lenguaje que pueda ser concebido e implementado: castellano, binario, ruso, cobol, latín, hexadecimal, etc.). En tanto y en cuanto la información pueda ser representada (recordemos que si algo no puede ser representado, entonces simplemente no existe, al menos para la ciencia), entonces podrá ser codificada y almacenada en algún soporte físico (Hardware).

Esta información codificada está en uno de tres estados: almacenada, en tránsito o en transformación, pero siempre ocupa un lugar en el espacio y es contenida por elementos materiales, de existencia real.

En tal sentido, siempre es posible establecer dónde se encuentra determinada información en un momento dado. A veces, el tiempo de permanencia en el lugar es casi efímero, pero nunca es nulo. El caso más crítico es aquel en el que la información está siendo transformada en el núcleo de una computadora (ALU, registros, buses de datos y direcciones y otras circunstancias similares), lo que agrega complejidad a la determinación de la posición exacta de la información, pero no la sustrae al espacio tiempo en que discurrimos nuestras terrenales existencias.

Como conclusión, podemos afirmar que **siempre existe un lugar del hecho real**, ya sea que esté restringido a un área determinada o que se encuentra distribuido en varias áreas geográficas, relacionadas por eventos informáticos en desarrollo. Aunque pueden existir múltiples copias idénticas de un archivo digital, eso no implica que un mismo archivo pueda existir en dos dimensiones al mismo tiempo.

Incluir, asimilar y adoptar como propio el concepto anterior resulta imprescindible para el **operador del derecho del siglo XXI**. Pretender que existe un "ciberespacio", desprendido de la realidad y solo accesible a los jóvenes que integran la cultura "digital", es la principal causa de los errores en la gestión de la prueba documental informática que a diario debemos sufrir los justiciados y/o justiciables, violentando profundamente el orden y la seguridad jurídica en que la mayoría de los mortales pretendemos convivir. La solución no reside en la edad del analista, sino en su capacidad de adaptarse a la evolución tecnológica que lo rodea, a su interés por capacitarse y sobre todo a la necesidad de abandonar la creencia soberbia y reemplazarla por la crítica lógica y constructiva (a pesar de lo que pretendan las teorías en boga, los vocablos "sano" y "crítica" pocas veces se pueden compatibilizar entre sí, en particular porque ambos son ambiguos, relativos y multívocos).

2.3.2. LUGAR DEL HECHO VIRTUAL IMPROPIO

Cuando el lugar del hecho real es relevado, registrado y almacenado por medios digitales, en una simulación estática o dinámica, con la fidelidad, detalle y definición que la tecnología moderna permite, estamos ante un lugar del hecho virtual impropio. Se lo denomina impropio porque existe una correspondencia biunívoca entre el lugar del hecho real y su representación digital (estática o dinámica). De esta forma se pueden hacer reconstrucciones de hechos para determinar si los resultados obtenidos se corresponden con la evidencia

registrada en el lugar del hecho real. Pensemos, por ejemplo, en la dinámica del movimiento vehicular, que se desarrolla en el marco de una pericia de accidentología vial y la posibilidad de repetir las veces necesarias el experimento, modificando las condiciones iniciales, hasta que la correspondencia con lo comprobado en el lugar del hecho real sea lo más perfecta y ajustada posible. Tiene múltiples ventajas, por ejemplo, la comparación entre expertos locales o remotos, el resguardo del lugar a pesar del paso del tiempo (correctamente resguardado, certificado y con su correspondiente cadena de custodia), evitar la coordinación de agendas entre profesionales hiper especializados y con escaso tiempo disponible, encuentros que pueden ser reemplazados por videoconferencias, con resultados similares a los obtenidos mediante la inspección o el reconocimiento judiciales clásicos. En este caso, no existen problemas de competencia, ya que la misma está determinada específicamente por el lugar del hecho real, del cual **el lugar del hecho virtual impropio es solo una reconstrucción.**

2.3.3. LUGAR DEL HECHO VIRTUAL PROPIO

En este caso, las acciones ocurren completamente en entornos virtuales. Por ejemplo, un falsario desde Buenos Aires utiliza, por medios remotos, una granja de servidores en Medio Oriente, para descubrir una clave de acceso a una cuenta bancaria en Holanda y transferir fondos desde Barcelona a Punta del Este, con el objeto de cobrar el dinero en una sucursal de Piriápolis. **La única forma de representar estas transacciones es por medio de una simulación virtual, no existe la correspondencia con un LHR.**

En este caso, no es posible emular y solo queda la solución de la simulación, es imposible escapar a la subjetividad de quien propone e implementa dicha simulación; en realidad, **la labor pericial se diluye y sólo resta la tarea testimonial del experto**. Solo se puede contrastar mediante el empleo de un colegio de peritos, con asistencia del juez, en reemplazo del clásico careo testimonial. Es decir, **el colegio de peritos es al careo lo que el testigo experto al testigo**.

La única figura que se puede utilizar es **el reconocimiento/inspección judicial virtual**, local o remota, no se encuentra específicamente descrito, ni detallado en la codificación procesal vigente en nuestro país. Por lo tanto, los temas relacionados con delitos informáticos propios, como ser la sustitución de identidad virtual, suelen ser muy difíciles de probar, ya que la prueba no se puede encuadrar en las figuras procesales vigentes.

Al igual que la obtención (legítima o ilegítima) de prueba confesional y/o testimonial, utilizando mecanismos de análisis de contenido neuronal (memoria) por métodos no invasivos, sustentados por neurociencias, constituyen una **auténtica laguna procesal por el momento**.

Este es el **punto álgido de la cuestión**. Ahora, el problema de la competencia se vuelve crítico, ya que podría ocurrir que existan elementos probatorios del delito en distintos lugares del mundo y la comisión del mismo no siempre está perfectamente definida. Las situaciones posibles pueden devenir en:

Suponiendo establecida la competencia de un tribunal nacional:
a) Elementos probatorios obrantes en un país con el cual existen **convenios bilaterales** de asistencia judicial/policial recíproca. El caso más sencillo es Argentina-Uruguay.

b) Elementos probatorios obrantes de un país con el cual existen **tratados multilaterales** de similar índole (por ejemplo, Paraguay-Argentina y su inserción en el Mercosur o Argentina y otro país que integre la OMC -Organización Mundial del Comercio- o la UIT - Unión Internacional de Comunicaciones). Se comienza a complicar porque estos convenios normalmente son mucho más limitados que los anteriores.

c) Elementos probatorios obrantes en un país con el cual **no existen vínculos** de asistencia judicial/policial de ningún tipo, por ejemplo, Iraq o Irán. El peor de los casos implica que no va a ser posible obtener dato alguno por medios judiciales lícitos. El ejemplo típico es el uso de granjas de servidores situados en Medio Oriente (por ejemplo, Siria) para romper claves bancarias.

Suponiendo la indeterminación o duda sobre la competencia de un determinado tribunal, ya sea que se excusen o sean recusados. El problema es de difícil solución.

2.4. CONTRIBUCION DE LA INFORMÁTICA. ASPECTOS TÉCNICOS

Cada dispositivo informático fijo o móvil está asociado mediante su placa de red/comunicaciones con una dirección física única que identifica a dicha placa. Es decir, es un número hexadecimal, normalmente denominado **dirección MAC**, que es propio del dispositivo y único respecto de los demás. Luego, cada usuario que utiliza el dispositivo se identifica con el mismo de manera biunívoca mediante una **dirección IP.**

Ahora bien, como dijimos, la información siempre se encuentra en algún lugar fijo, más aún en un dispositivo determinado. Por lo tanto, **si determinamos la dirección IP de origen o destino (según el caso de que se trate) de una transacción digital, habremos establecido el lugar de ocurrencia de un evento virtual, que puede resolverse de manera unívoca el problema de la competencia judicial.**

Es cierto que si la dirección IP está asociada a un dispositivo móvil, el problema se traslada a establecer con precisión dónde se encontraba dicho dispositivo al momento en que ocurrió el evento investigado. Este problema no es un problema informático y deberá ser considerado por otras pruebas complementarias, como testimonios, geolocalización, pruebas de informes, reconocimiento/inspección judicial y cualquier otro que contribuya a reducir la incertidumbre acerca de la localización del dispositivo en un momento dado. Por supuesto, este método no soluciona la problemática general de la competencia, ya que dependerá del criterio que utiliza quien analiza y determina la misma (el lugar de ocurrencia, el lugar donde se lo ejecutó, la nacionalidad del delincuente). Insistimos, no solucionamos los problemas teóricos y prácticos que la determinación de competencia en lugares de hecho reales ha provocado a lo largo de los siglos. Sin embargo, sí permite establecer con claridad en qué lugar lógico ocurrió un evento y dónde se encontraba el dispositivo que generó el evento en el momento en que dicho evento se produjo.

2.5. ALGUNAS SOLUCIONES

En el caso de resolver problemas de competencia relacionados con lugares del hecho virtuales propios (LHVP), la determinación de la dirección IP de cada dispositivo/usuario comprometido en el mismo permite esclarecer su lugar de ubicación. No soluciona los problemas de fondo de la competencia, los cuales siguen siendo los que históricamente se han relacionado con el lugar del hecho real (LHR), aunque permite dilucidar ubicaciones y localizaciones que facilitan dicha determinación

En aquellos casos en los que la determinación de la competencia requiera establecer la ubicación político-geográfica de un determinado usuario/dispositivo correspondiente al origen o destino de un evento digital, el magistrado decisor debería solicitar un informe técnico que determine la dirección IP del referido dispositivo, su dirección MAC asociada y su geolocalización al momento del evento considerado. Procesalmente, la medida debería ser incluida en autos **como medida previa, preliminar o prueba anticipada**, según el fuero y derecho procesal codificado que corresponda. El resultado de este informe brindaría sustento objetivo al argumento de declinación o aceptación de la competencia cuestionada legalmente.

TÍTULO 3

CONCLUSIÓN

INTRODUCCION

A lo largo de mi trabajo, en todo momento celebré y celebro los avances tecnológicos, sin olvidar que fue la tecnología la que me permitió en un contexto de pandemia estar redactando estas líneas para alcanzar mi título de grado. Claro que requirió una rápida respuesta por parte de la universidad y una adaptación forzada y colaborativa de todos los que formamos parte desde diferentes ángulos.

Así las cosas, su evolución tan facilitadora para la vida social y profesional, revelan cada vez más consecuencias negativas no previstas, o mejor dicho no atendidas con la celeridad que amerita, a tan solo, figurativamente un "click" de distancia para lesionar bienes jurídicos tutelados de quienes intuitivamente en su gran mayoría interactúan en el ciberespacio.

Los ciberdelincuentes, como sujetos activos de estos delitos sometidos a análisis, parecen colonizar este nuevo territorio, su herramienta o "superpoder" está dada por el manejo "nativo" de un "idioma", un lenguaje que expresa un algoritmo, como uno de los pilares indispensables de lo todo lo que hace posible no solo la hiperconectividad sino su contenido. Son quienes escriben las instrucciones para que su voluntad se cumpla y su responsabilidad se esfume como una estrella fugaz.

Dada las circunstancias, desafíe este trabajo desde un análisis conceptual del fenómeno en su primer capítulo, luego del escenario de hiperconexión, continué con el impacto de la inteligencia artificial como medio, el contexto de la pandemia como potenciador delictivo, repasando sucintamente las principales conductas delictivas tipificadas y aún no por nuestro ordenamiento, y rescatando algunos conceptos generales teórico-penales a los fines del encuadramiento, incluso frustrado desde una mirada analógica o bien no contemplativa de lo que aflige a millones de internautas. Procurando ser transversal a las doctrinas existentes.

PROBLEMAS

La amenaza que presenta este fenómeno, radica en poner masivamente en riesgo la afectación constante y sistematizada de los **DDHH** con rango jerárquico que podría extenderse al supranacional, e indubitablemente al bloque constitucional, por encima de cualquier derecho de fondo además del penal. Como corolario de las relaciones y diferencia entre las nociones de bien jurídico, valores constitucionales, derechos humanos, derechos fundamentales. Mientras que en la dogmática penal es concebido como bien jurídico, siendo que en definitiva remiten a intereses, relaciones o posiciones esenciales para la vida comunitaria, que indubitablemente son objeto de derechos, libertades o competencias establecidos por la Constitución y el derecho positivo.

Así las cosas, los delincuentes o ciberdelincuentes preparan a diario "banquetes" para operar desde cualquier punto geográfico (físico) del mundo estando en el – no lugar -, manipulando la tecnología para conseguir una reservada y hasta anónima autoría, incluso no humana, de mano de la inteligencia artificial y también mediante el uso de técnicas de ingeniería social a fines de incrementar las probabilidades de su objetivo.

Hasta me atrevo a decir que en su mayoría por lo analizado en el capítulo 2 relativo al ciberespacio, al referirme a la deepweb y darkweb, enlazado con lo visto en el capítulo 4, llego a la conclusión de ¿acaso no califica como **crimen organizado**?, tomando la definición dada por la Convención de las Naciones Unidas contra la Delincuencia Transnacional Organizada en su art. 2 inc. "*grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno más delitos graves (…)"* o delitos tipificados con arreglo a la presente Convención"

Otros de las contingencias reveladas, a pesar del gran aporte legislativo en materia penal en manos de la ley 26.388 (delitos informáticos), sumada la ley 26.904 (*grooming)*, y la ley 27.436 (tenencia de pornografía infantil), sin olvidar mencionar a la ley 11.723 modificada por la ley 25.036 (propiedad intelectual del software) y la ley 25.326 (protección de datos personales), existen parámetros en el derecho comparado dignos de replicar -recordando la tipificación de la explotación económica de las plataformas de contenidos pirata como MegaUpload-, es que no basta legislar ciberdelitos, sino que exige reglamentarse y prever aspectos procesales vinculados con esta nueva forma de delincuencia.

Asimismo, delimitar una nueva teoría penal la del cibercrimen, apartada de actuales dogmas que serán sin dudas enriquecedoras como una de sus fuentes.

También, surge del análisis de trazado sistemático en los primeros tres capítulos (cibercrimen; ciberespacio e IA), la necesidad de resolver el "analfabetismo digital", tanto de los sujetos pasivos de este tipo de delitos, como de quienes deben prevenirlos y reprocharlos, sin desmerecer los esfuerzos que se vienen haciendo jurídicamente, y desde el ámbito institucional y también el privado.

SOLUCIONES

Es por todo lo expuesto a lo largo de la tesina y aquí en mis conclusiones, que planteo el carácter positivo de los siguientes puntos.

En el ámbito legislativo, hacerlo en relación al ciberespacio. Por otra parte será necesario volver a tratar las reservas realizadas por argentina al Convenio de Budapest referidas a la jurisdicción en cuanto a los nacionales que cometan delitos, por ser contrario al principio de territorialidad y a la doble jurisdicción y encontrar una forma de abordar la dimensión transnacional del delito cibernético y mejorar la cooperación internacional a través del desarrollo y estabilizar las que los tratados y leyes que sean conducentes.

También es relevante atender cuestiones procesales probatorias (uno de los temas no abordados por seleccionar enfocarse en intentar aproximar los elementos tecnológicos que están en juego desde una perspectiva jurídica, pero que sin dudas han pasado por mis narices reiteradas veces en mi proceso investigativo, junto a otros como las criptomonedas para lavado de activos en la darkweb que me vi forzada a no seleccionar), evitando caer en pruebas ilícitas, como la conservación de las mismas. Por otra parte "ajustar" ciertos fundamentos que me permito denominar como analógicos, como supe rezar a lo largo del trabajo, e incorporar normas del derecho comparado de relevancia para nuestra sociedad. Por último hacer uso de leyes excepcionales, donde su vigencia depende de la subsistencia de situaciones que por su índole son temporales o transitorias, no aplicadas a mí entender durante el prolongado y actual contexto del Covid-19.

Reforzar la prevención, como pilar fundamental para no sobrecargar al derecho penal, siendo responsabilidad del derecho en su totalidad, como así también de las instituciones públicas y privadas desplegar al máximo herramientas efectivas, que permitan *ex ante* proteger a las víctimas, sujetos pasivos, que parecen ser olvidados en este fenómeno, como si el acto lesivo de estas conductas, al igual que el sujeto activo, se disiparan las consecuencias en el ciberespacio. Teniendo en cuenta que al articularse de manera distinta la exposición de bienes jurídicos pasibles de ser lesionados siendo que en el ciberespacio depende del "ingreso" o facilitación (como se analizó y represento gráficamente en el capítulo 4), por parte del sujeto pasivo, es aquí donde la prevención operaría con éxito.

Por lo antes expuesto, se celebra los avances argentinos en materia de ciberdefensa y la reciente creación del nuevo organismo que forma parte de la Secretaría de Innovación Pública, responsable de la aplicación CuidAR, el cual funcionará como una mesa de ayuda que emitirá alertas a los organismos ante ciertos tipos de vulnerabilidades en aplicaciones o software de uso privado, además de asistir a la resolución de diversos tipos de conflictos digitales, como medidas de seguridad.

También, se elogia la creación de instituciones a nivel nacional como la cibercrimen.org.ar, en el marco del derecho comparado la CCI (centro para la seguridad y la investigación del cibercrimen) en EEUU, Como así también la insistencia de Interpol, EUROPOL y tantos otros abanderados en el tratamiento de algo que urge conocer en detenimiento para receptarlo en las normas de fuente locales como internacional, en busca de unicidad de criterios.

Impedir que se vulneren derechos subjetivos, por falta de conocimiento, fundamentos infundados como el caso de la película argentina "un cuento chino", divulgada en la plataforma YouTube hace casi una década, por falta de expertise en quienes dicen y operan el derecho, como también los peritos en aquel entonces, desconociendo hoy la calidad de estos.

Promover la creación de acuerdos regionales, fornecerá y agilizará avances investigativos. Desterritorializar su estudio permitirá un mejor encuadramiento jurídico.

Aprovechar las asociaciones público-privadas y establecer grupos de expertos multidisciplinarios.

Establecer capacitación obligatoria en esta materia con sus aristas técnicas esenciales en la función pública en todos sus niveles y jerarquías en los poderes Ejecutivo, Legislativo y Judicial de la Nación. como se hizo con la ley 27.499, conocida como Ley Micaela sobre temática de género y violencia contra las mujeres.

Es menester avanzar significativamente en la creación de un Tribunal Penal regional con competencia exclusiva en esta materia.

Por último la hipótesis se sustenta, en la necesidad de esclarecer conceptos, para así no solo mitigar legislativamente algunas conductas dadas en este ámbito, sino también se afirma la necesidad de abordar a este fenómeno desde su propia naturaleza, evitando caer en analogías *in malam partem*, rechazadas por nuestro derecho. Por otra parte se afirma que el derecho penal no resulta suficiente y requiere un pronóstico explorando otras ramas e incluso impensadas áreas de conocimiento, en la búsqueda de respuestas. Emprender soluciones de carácter interdisciplinario favorece atenuar el impacto negativo de la tecnología digital y en ella contemplada la inteligencia artificial.

INTERROGANTES

¿Será acaso que la tecnología, está venciendo a su creador?

¿Qué limitaciones nos corresponde asimilar en las manipulaciones tecnológicas?

Serían las aplicadas a la Ciencia en la manipulación genética…

.. Hoy en manos de pocos.

¿Cómo fue el comienzo del desarrollo tecnológico y digital?

Existen actualmente escenarios análogos de control del ciberespacio..

Este fenómeno,

¿NOS ESTÁ PIDIENDO A GRITOS SU PROPIA TEORÍA DEL CIBERCRIMEN?

Resta sólo recordar las palabras de Luis Jiménez de Asúa:

“Una Teoría que no sirve para la práctica, no es una Teoría;
y una práctica sin Teoría, es mera rutina”.

Inteligencia Artificial [Versión 10.3.2021]

BIBLIOGRAFÍA

- Miró Llinares, Fernando, (2016). "La cibercriminalidad 2.0: falacias y realidades", (pp. 58-59), Madrid, España.

- Righi, Esteban (2016). Derecho Penal. Parte General. Segunda Edición. Buenos Aires, Argentina.

- Enrique Pérez Luño, Antonio, (1996). "Manual de informática y derecho", (p. 75), Barcelona, España.

- Posada Maya, Ricardo (2017). Nuevo Foro Penal No. 88, Universidad EAFIT: El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual, (p. 72 - 78).

- Günther Jackobs, (2002). Los pormenores del tipo objetivo mediante la acción, en Imputación objetiva y antijuridicidad. Estudios de Derecho Penal (p. 107).

- Claus Roxin, (2002). La imputación al tipo objetivo, en Imputación objetiva y antijuridicidad. Estudios de Derecho Penal(p. 122-123)

- Palazzi, Pablo A. (2016). Los delitos informáticos en el código penal. Buenos Aires, Argentina.

- Litvin, Jorge L. (2020). HACKEADOS - Delitos en el mundo 2.0 y medidas para protegernos. (Publicación Digital) Buenos Aires, Argentina.

- Oliveira Rivas, Fabio y otros (2008). CN Crim y Corr. Sala 4.

- Castellini, Alfredo J. y otros (2005). CN Crim y Corr. Sala 7.

- Darahuge, María E. - Arellano González, Luis. Empleo de las direcciones virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad. (p. 183 y 189).

- Parada, Ricardo Antonio; Errecaborde, José Daniel (2018). Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet. Buenos Aires, Argentina.

- #Europol, #UNICRI y #TrendMicro descubren las amenazas actuales y futuras de la #IA y cómo combatirlas | Espacio IA UNESCO, 20 de noviembre de 2020. Consultado el 22 de noviembre de 2020.

- Censura en China: las autoridades bloquearon WhatsApp antes del congreso del Partido Comunista, Infobae.com, 26 de septiembre de 2017. Consultado el 28 de agosto de 2020.

- Definición de inteligencia artificial - Qué es, Significado y Concepto, Definicion.de. Consultado el 22 de noviembre de 2020.

- Delito de piratería por el código penal y sus sanciones, garridodonaque.com, 11 de septiembre de 2020. Consultado el 16 de enero de 2021.

- Ciberdefensa: el desafío de las nuevas generaciones, argentina.gob.ar, 09 de noviembre de 2018. Consultado el 12 de noviembre de 2020.

- Así van a utilizar los cibercriminales la Inteligencia Artificial para atacarte en el futuro, 31 de diciembre de 2020. Consultado el 12 de enero de 2021.

- Revista Electrónica de Ciencia Penal y Criminología, (13-07-2011). Art. SISSN 1695-0194 RECPC RECPC:. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Fernando Miró Llinares, Profesor Titular de Derecho Penal, Universidad Miguel Hernández de Elche.

ANEXOS

ANEXO 1 - SILK ROAD

El 2 de octubre de 2013, fue cerrado por el FBI y su fundador, conocido por su alias «Dread Pirate Roberts», fue identificado como Ross Ulbricht. El 6 de noviembre de 2013 las revistas Forbes y Vice indicaron que el sitio había vuelto a estar en línea.23 En febrero de 2015, Ross Ulbricht fue sentenciado a un mínimo de 30 años de prisión por siete cargos delictivos por un tribunal de Manhattan. Finalmente, en junio de 2015 fue sentenciado a cadena perpetua por una corte Federal de Manhattan, después de haber sido hallado culpable de siete cargos.

Historia: El sitio de Internet fue lanzado en el mes de febrero del año 2011. Los compradores podían registrarse en Silk Road gratuitamente, pero los vendedores debían adquirir nuevas cuentas a través de subastas supuestamente para mitigar la posibilidad de que personas malintencionadas distribuyeran productos contaminados. Las comisiones de dichas ventas en todo el sitio en total eran destinadas al administrador del sitio. Después de mucho tiempo fuera de línea, a principios del mes de octubre de 2013 el sitio de SilkRoad había sido restablecido y funcionaba de igual manera que antes; para registrarse como usuario vendedor se debía pagar cierta cantidad en Bitcoin, pero cualquier persona podía registrarse gratuitamente como usuario comprador.

Es importante destacar que su regreso no había sido muy popular ya que algunos sitios como SheepMarket y The Black Market Reloaded (BMR) habían comenzado a tener un gran auge, no obstante, desde el cierre de estos a finales de noviembre y principios de diciembre de 2013, resucitó la popularidad de SilkRoad. Este último junto con "PANDORA Open Market" son los dos mercados negros más populares en la red TOR en este momento.

Producto[: La mayoría de los productos que eran vendidos en Silk Road, estaban calificados como contrabando en la mayoría de las jurisdicciones. Gran parte de los vendedores tenían su sede en el Reino Unido y los Estados Unidos, y ofrecían productos como Heroína, LSD, Cannabis y otras drogas. Sin embargo, los operadores del sitio prohibían productos o servicios destinados a dañar a otros, tal como números de tarjetas de crédito robadas, falsificación de moneda, información personal, asesinatos y materiales utilizados para fabricar armas.

Referido a transacciones, los compradores y vendedores conducían sus transacciones por medio de la moneda virtual descentralizada llamada Bitcoin, que provee más anonimato

que las tarjetas bancarias. El 99% de todas las transacciones realizadas en el sistema se completaron a satisfacción del comprador y del vendedor, o se hallaba un acuerdo para la resolución de algún conflicto.

En cuanto a la Prensa, el blog de noticias Gawker escribió un artículo completo sobre Silk Road. El National Public Radio se refirió al sitio como «el Amazon.com de las drogas ilegales». El diario británico The Economist, lo describió en un artículo como «Estas e-profundidades no se pueden alcanzar con un navegador común sino con un software llamado Tor. Compradores y vendedores realizan las transacciones bajo pseudónimo y en bitcoins, una moneda cifrada criptográficamente».
Después de esta atención, el tráfico al sitio de internet de Silk Road aumentó drásticamente y la moneda virtual Bitcoin registró un aumento correspondiente en el valor. El sitio también fue utilizado durante la audiencia de la Ley SOPA 2011 como un ejemplo de la evolución de algunos sitios de internet a la creación de redes y sistemas de computación distribuida que por diseño no es posible bloquearlo por filtro de nombre de dominio (DNS) tal como se propone en SOPA.

Por ultimo como referencia de aplicación, y a consecuencia de este caso, la Policía Federal de Australia ha declarado en un comunicado de prensa que «Cualquier persona que ejerza una actividad ilegal a través de los mercados en línea como Silk Road... no siempre va a permanecer en el anonimato y cuando sean capturados, serán procesados»

ANEXO 2 - IA

INTRODUCCION

Una de las pretensiones de la IA es construir réplicas de la compleja red neuronal del cerebro humano e intentar imitar el comportamiento del cerebro humano con una computadora (en sentido amplio), ya que hoy podríamos hablar de dispositivo.

CARACTERÍSTICAS DE LA IA

Una de sus características es que incluye varios campos de desarrollo, como la robótica, la comprensión y traducción de lenguajes, el reconocimiento y aprendizaje de palabras de máquinas o los variados sistemas computacionales expertos, que son los encargados de reproducir el comportamiento humano en una sección del conocimiento.

Tales tareas reducen costos y riesgos en la manipulación humana en áreas peligrosas, mejoran el desempeño del personal inexperto y el control de calidad en el área comercial.

Por otra parte, consideré muy interesante lo que respecta en torno a las REDES NEURONALES DENTRO DE LA AI (se desarrolla a continuación), y otros factores vinculados al tema de alto valor comprensivo. Vislumbrar hacia el futuro de lo que estos sistemas pueden en lograr, en apoyo a anticipar las consecuencias positivas, sin dejar de lado las negativas,

REDES NEURONALES DENTRO DE LA IA

Las redes neuronales son programas de la AI capaces de simular algunas de las funciones de aprendizaje del ser humano. Una red neuronal obtiene experiencia analizando automática y sistemáticamente los datos para determinar reglas de comportamiento; con base en ellas, puede realizar predicciones sobre nuevos casos.

Estas técnicas se aplican a problemas de clasificación y series de tiempo e identifican conexiones con cosas que otras técnicas no pueden, porque utilizan relaciones lineales y no lineales.

Neuronas y conexiones sinápticas. Cada neurona puede tener infinitas entradas llamadas dendritas que condicionan el estado de su única salida existente, el axón; éste se puede conectar a una dendrita de otra neurona mediante la sinapsis correspondiente. En este modelo se considera una neurona que puede ser representada por una unidad binaria; a cada

instante su estado puede ser activo o inactivo. La interacción entre las neuronas se lleva a cabo a través de la sinapsis, la cual define el estado de la neurona.

Por último, las Redes Neuronales son una rama de la IC muy relacionada con el aprendizaje automático.

LA AI EN LA ROBÓTICA

Los robots son dispositivos compuestos de sensores que reciben datos de entrada que manda una computadora, la cual ordena al robot que efectúe una determinada acción.

Hoy en día, una de las finalidades de la construcción de robots es su intervención con rapidez, calidad y precisión en los procesos de fabricación encargados de realizar trabajos repetitivos en la fabricación.

LAS ÁREAS DE INVESTIGACIÓN DE LA IA

Son muchas las áreas de la IA que se investigan hoy día. Entre ellas, tenemos las siguientes:

1. La representación del conocimiento, que busca en el descubrimiento de métodos expresivos y eficientes describir información sobre aspectos del mundo real.
2. Los métodos de aprendizaje automático, que extienden las técnicas estadísticas con el fin de posibilitar la identificación de un amplio rango de tendencias generales a partir de un conjunto de datos de entrenamiento.
3. El campo de la planificación, que enfrenta el desarrollo de algoritmos que construyen y ejecutan automáticamente secuencias de comandos primitivos con el fin de alcanzar ciertas metas de alto nivel.
4. Los trabajos en el área de razonamiento posible, que hacen uso de principios estadísticos para desarrollar codificaciones de información incierta.
5. El estudio de las arquitecturas de agentes, que busca la integración de otras áreas de la I A con el objeto de crear agentes inteligentes, entidades robustas capaces de comportamiento autónomo y en tiempo real.
6. La coordinación y colaboración multiagentes, que ha permitido el desarrollo de técnicas para la representación de las capacidades de otros agentes y la especificación del conocimiento necesario para la colaboración entre ellos.

7. El desarrollo de ontologías, que persigue la creación de catálogos de conocimiento explícito, formal y multipropósito, que puedan ser utilizados por sistemas inteligentes.
8. Los campos de procesamiento de voz y lenguaje, que buscan la creación de sistemas que se comunican con la gente en su lenguaje.
9. La síntesis y comprensión de imágenes, que conduce a la producción de algoritmos para el análisis de fotografías, diagramas y videos, así como también de técnicas para el despliegue visual de información cuantitativa y estructurada.

CATEGORIAS DE IA

Por otra parte, me pareció interesante considerar estos aspectos, se vinculan a nuestra materia penal, en relación al primer pilar de la Teoría del Delito.

1) **Sistemas que piensan como humanos**: Estos sistemas tratan de emular el pensamiento humano; por ejemplo las redes neuronales artificiales. La automatización de actividades que vinculamos con procesos de pensamiento humano, actividades como la toma de decisiones, resolución de problemas y aprendizaje.

2) **Sistemas que actúan como humanos**: Estos sistemas tratan de actuar como humanos; es decir, imitan el comportamiento humano; por ejemplo la robótica. El estudio de cómo lograr que los computadores realicen tareas que, por el momento, los humanos hacen mejor.

3) **Sistemas que piensan racionalmente**: Es decir, con lógica (idealmente), tratan de imitar el pensamiento racional del ser humano; por ejemplo los sistemas expertos. El estudio de los cálculos que hacen posible percibir, razonar y actuar.

4) **Sistemas que actúan racionalmente**: Tratan de emular de forma racional el comportamiento humano; por ejemplo los agentes inteligentes. Está relacionado con conductas inteligentes en artefactos.

ESCUELAS DE PENSAMIENTO

La IA se divide en dos escuelas de pensamiento:

1) INTELIGENCIA ARTIFICIAL CONVENCIONAL: Se conoce también como IA simbólico-deductiva. Está basada en el análisis formal y estadístico del comportamiento humano ante diferentes problemas:

- Razonamiento basado en casos: Ayuda a tomar decisiones mientras se resuelven ciertos problemas concretos y, aparte de que son muy importantes, requieren de un buen funcionamiento.

- Sistemas expertos: Infieren una solución a través del conocimiento previo del contexto en que se aplica y ocupa de ciertas reglas o relaciones.

- Redes bayesianas: Propone soluciones mediante inferencia probabilística.

- Inteligencia artificial basada en comportamientos: Esta inteligencia contiene autonomía y puede auto-regularse y controlarse para mejorar.

- Smart process management: Facilita la toma de decisiones complejas, proponiendo una solución a un determinado problema al igual que lo haría un especialista en dicha actividad.

2) INTELIGENCIA ARTIFICIAL COMPUTACIONAL: La Inteligencia Computacional - IC- (también conocida como IA subsimbólica-inductiva). Es una rama de la IA centrada en el estudio de mecanismos adaptativos para permitir el comportamiento inteligente de sistemas complejos y cambiantes. Se presenta como una alternativa a la GOFAI ("Good Old-Fashioned Artificial Intelligence"), tratando de no confiar en algoritmos heurísticos tan habituales en la Inteligencia Artificial más tradicional. Dentro de la IC, podemos encontrar técnicas como las Redes Neuronales, Computación Evolutiva, Swarm Intelligence, Sistemas Inmunes Artificiales o Sistemas Difusos. También se relaciona con técnicas como los Fractales, Teoría del Caos, Wavelets, Autómata celular, etc.

Asimismo, combina elementos de aprendizaje, adaptación, evolución y Lógica difusa para crear programas que son, en cierta manera, inteligentes. La investigación en IC no rechaza los métodos estadísticos, pero muy a menudo aporta una vista complementaria.

ANEXO 3 - TEST DE TURING Y LA IA

Link:

Prueba de Turing

Se comprende por la prueba de Turing o test de Turing a un examen de la capacidad de una máquina para exhibir un comportamiento inteligente similar al de un ser humano o indistinguible de este.

El nombre está dado por su autor, Alan Turing quien propuso que un humano evaluara conversaciones en lenguaje natural entre un humano y una máquina diseñada para generar respuestas similares a las de un humano.

El evaluador sabría que uno de los participantes de la conversación es una máquina y los intervinientes serían separados unos de otros. La conversación estaría limitada a un medio únicamente textual como un teclado de computadora y un monitor por lo que sería irrelevante la capacidad de la máquina de transformar texto en habla. En el caso de que el evaluador no pueda distinguir entre el humano y la máquina acertadamente (originalmente su autor, sugirió que la máquina debía convencer a un evaluador, después de 5 minutos de conversación, el 70 % del tiempo), la máquina habría pasado la prueba. Esta prueba no evalúa el conocimiento de la máquina en cuanto a su capacidad de responder preguntas correctamente, solo se toma en cuenta la capacidad de ésta de generar respuestas similares a las que daría un humano.

Propuso la prueba en su ensayo "Computing Machinery and Intelligence" de 1950 mientras trabajaba en la Universidad de Mánchester (Turing, 1950; p. 460). Inicia con las palabras: ***"Propongo que se considere la siguiente pregunta, '¿Pueden pensar las máquinas?".***

Como es difícil definir la palabra "pensar", Turing decide "reemplazar la pregunta con otra que está estrechamente relacionada y en palabras no ambiguas.", la nueva pregunta de Turing es*: "¿Existirán computadoras digitales imaginables que tengan un buen desempeño en el juego de imitación?".* Turing creía que esta pregunta sí era posible de responder y en lo que resta de su ensayo se dedica a argumentar en contra de las objeciones principales a la idea de que "las máquinas pueden pensar".

Desde que fue creada por Turing en 1950, la prueba ha demostrado ser altamente influyente y a la vez ampliamente criticada, además de transformarse en un concepto importante en la filosofía de la inteligencia artificial

Muchas personas consideran que el **test de Turing** ha sido superado, citando conversaciones en que al dialogar con un programa de inteligencia artificial para chat, no saben que hablan con un programa. Sin embargo, esta situación no es equivalente a un test de Turing, que requiere que el participante se encuentre sobre aviso de la posibilidad de hablar con una máquina.

Otros experimentos mentales como la Habitación china, de John Searle, **han mostrado cómo una máquina podría simular pensamiento sin realmente poseerlo**, pasando el test de Turing sin siquiera entender lo que hace, tan solo reaccionando de una forma concreta a determinados estímulos (en el sentido más amplio de la palabra). Lo que demuestra que la máquina en realidad no está pensando, ya que actuar de acuerdo con un programa preestablecido sería suficiente. Si para Turing el hecho de engañar a un ser humano que intenta evitar que le engañen es muestra de una mente inteligente, Searle considera posible lograr dicho efecto mediante **reglas definidas a priori.**

ANEXO 4 - CASO YOUTUBE Y LA PELÍCULA UN CUENTO CHINO

Link: Infojus Noticias

Beatriz Busaniche, Magister en Propiedad Intelectual, analiza el fallo que afirmó que subir videos a You Tube no es delito penal. Por qué la normativa vigente está entre las más restrictivas del mundo.

La Sala 5 de la Cámara Nacional de Apelaciones en lo criminal y correccional, con la firma de Gustavo Bruzzone, Rodolfo Pociello Argerich y Mirta López González, confirmó un fallo de primera instancia que había archivado una denuncia penal contra diez usuarios de Youtube acusados de publicar la película "Un Cuento Chino" (de la productora Pampa Films S.A.) en la plataforma de videos de la empresa Google, también acusada por supuesta infracción de la ley de propiedad intelectual.

El fallo traerá polémica. Llega para aclarar un asunto de enorme actualidad: la aplicación de la ley penal a los usuarios finales que cometen infracciones de propiedad intelectual en internet.

El fallo en cuestión no sólo aborda la responsabilidad de la empresa Google, a la que da por sobreseída argumentando que "presta un servicio de intermediación para subir contenidos y su característica esencial para socializar información cultural a nivel mundial le otorgan una condición destacada."

El fallo agrega que, si bien "nos encontramos frente a una actividad riesgosa, por los beneficios mencionados precedentemente en la difusión y promoción de contenidos culturales, es aceptada como un riesgo permitido". El fallo deja en claro que la empresa intermediaria no tiene responsabilidad penal en el caso, aunque reconoce la posibilidad de que la causa avance en el fuero civil y comercial.

La sección más interesante del fallo es el análisis por el cual la Cámara da por sobreseídos a los diversos usuarios que subieron la película a la plataforma. Otros casos de responsabilidad de intermediarios, como el destacado juicio iniciado por la Cámara Argentina del Libro contra Taringa!, no habían dado cuenta de estos actores clave de la historia.

En este caso, lo más destacable es la interpretación que la Cámara hace del artículo 71 de la Ley 11.723, uno de los más polémicos de la normativa. Redactada en 1933, la ley dice claramente que "será reprimido con la pena establecida por el artículo 172 del Código Penal, el

que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta Ley".

El artículo 71 de la Ley de Propiedad Intelectual es amplio e indeterminado, pero homologado a estafa, requeriría necesariamente -como dice el fallo- "un desplazamiento económico en favor del autor o de terceros generado mediante ardid o engaño, y en perjuicio de la víctima".

La querella no dió cuenta de nada de esto. No hubo engaño ni ardid cometido por parte de los usuarios que subieron la película, y si hubo daño en perjuicio de la víctima, entonces correspondería a la figura de lucro cesante a debatir en otra instancia. Lo que hacen los usuarios de Youtube al subir una película no es caracterizable bajo la figura de estafa.

Es suficientemente problemático el hecho de la creación de una figura penal mediante una ley de propósito particular como la de Propiedad Intelectual, que debe recurrir a la referencia del artículo 172 del Código Penal para definir la figura creada en su articulado, que -como bien afirma la Cámara- es indeterminado y amplio.

Ante semejante ambigüedad, asimilar a la estafa cualquier infracción a la ley de propiedad intelectual, es, cuanto menos, problemático. Es por eso que el fallo de la Cámara es trascendente, porque llega a cubrir un hueco importante en materia de interpretación de una norma que requiere urgente revisión.

La Ley de Propiedad Intelectual vigente es una de las normativas más restrictivas del mundo en materia de acceso al conocimiento y la cultura, según diversos análisis de legislación comparada que dan cuenta de la rigidez de la norma. Esta ley, diseñada en un contexto social y tecnológico totalmente diferente del actual, es una de las más infringidas en Argentina. Si tomamos al pie de la letra su texto, descubriremos que cada uno de nosotros infringe la ley de Propiedad Intelectual cotidianamente: cada vez que fotocopiamos unas páginas de un libro para nuestros estudiantes, o cuando descargamos un CD a nuestra computadora, o cuando enviamos una canción que nos gusta a un amigo, cuando un bibliotecario provee copias a investigadores o hace una copia de resguardo o para préstamo, se viola esta ley.

Darle una interpretación justa, equilibrada y atinada al artículo 71 era una tarea indispensable que la Cámara correctamente realizó con este fallo que deja en claro que sólo se puede contemplar el delito penal en caso de que la infracción a la Ley 11.723 constituya efectivamente una estafa.

Con esta interpretación, nosotros, los ciudadanos de a pie que no somos delincuentes ni estafadores, los millones de usuarios de internet y las nuevas tecnologías, los cientos de

bibliotecarios, miles de estudiantes, docentes, en fin, todos los usuarios, consumidores y participantes de la cultura, cuando accedemos, estudiamos, compartimos o divulgamos las obras que admiramos no deberíamos ser alcanzados por la amenaza penal.

ANEXO 5 – EVOLUCIÓN NORMATIVA SOBRE TUTELA DEL SOFTWARE EN MATERIA DE PROPIEDAD INTELECTUAL.

NORMATIVA

DERECHO ARGENTINO

- **Ley 11723 actualizada por ley 25036: dentro de la cual se destacan los siguientes artículos:**

OBJETO DE PROTECCIÓN. ARTÍCULO 1: "*A los efectos de la presente Ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos* ***los programas de computación fuente y objeto;*** *las compilaciones de datos o de otros materiales; las obras dramáticas, composiciones musicales, dramático-musicales; las cinematográficas, coreográficas y pantomímicas; las obras de dibujo, pintura, escultura, arquitectura; modelos y obras de arte o ciencia aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas, en fin, toda producción científica, literaria, artística o didáctica sea cual fuere el procedimiento de reproducción.*

La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí." (Artículo sustituido por art. 1° de la Ley N° 25.036 B.O. 11/11/1998)

TITULARES. ARTÍCULO 4: *"Son titulares del derecho de propiedad intelectual:*
a) El autor de la obra;
b) Sus herederos o derechohabientes;
c) Los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante.
d) Las personas físicas o jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario." Nota: se destaca la incorporación de este inciso

ARTÍCULO 9: "Nadie tiene derecho a publicar, sin permiso de los autores o de sus derechohabientes, una producción científica, literaria, artística o musical que se haya anotado o copiado durante su lectura, ejecución o exposición públicas o privadas.

Quien haya recibido de los autores o de sus derecho-habientes de un programa de computación una licencia para usarlo, podrá reproducir una única copia de salvaguardia de los ejemplares originales del mismo." (Párrafo incorporado por art. 3° de la Ley N° 25.036 B.O. 11/11/1998).

Dicha copia deberá estar debidamente identificada, con indicación del licenciado que realizó la copia y la fecha de la misma. La copia de salvaguardia no podrá ser utilizada para otra finalidad que la de reemplazar el ejemplar original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización. (Párrafo incorporado por art. 3° de la Ley N° 25.036 B.O. 11/11/1998).

DE LA VENTA. ARTÍCULO 55 BIS: *"La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción."*

DEL REGISTRO DE OBRAS. ARTÍCULO 57: *"En el Registro Nacional de Propiedad Intelectual deberá depositar el editor de las obras comprendidas en el artículo 1°, tres ejemplares completos de toda obra publicada, dentro de los tres meses siguientes a su aparición. Si la edición fuera de lujo o no excediera de cien ejemplares, bastará con depositar un ejemplar.*

El mismo término y condiciones regirán para las obras impresas en país extranjero, que tuvieren editor en la República y se contará desde el primer día de ponerse en venta en territorio argentino.

Para las pinturas, arquitecturas, esculturas, etcétera, consistirá el depósito en un croquis o fotografía del original, con las indicaciones suplementarias que permitan identificarlas.

Para las películas cinematográficas, el depósito consistirá en una relación del argumento, diálogos, fotografías y escenarios de sus principales escenas. Para los programas de computación, consistirá el depósito de los elementos y documentos que determine la reglamentación" (Última parte incorporada por art. 5° de la Ley N° 25.036 B.O. 11/11/1998).

DE LAS PENAS. ARTICULO 71: *"Será reprimido con la pena establecida por el* ***artículo 172 del Código Penal****, el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta Ley."* **(CASO PELÍCULA UN CUENTO CHINO)**

DE LAS PENAS. ARTÍCULO 72*: "Sin perjuicio de la disposición general del artículo precedente, se consideran casos especiales de defraudación y sufrirán la pena que él establece, además del secuestro de la edición ilícita:*
a) El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derechohabientes; **CASO PELÍCULA UN CUENTO CHINO)**

b) El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto;
c) El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto;
d) El que edite o reproduzca mayor número de los ejemplares debidamente autorizados."

DE LAS PENAS. ARTICULO 72 BIS: *"Será reprimido con prisión de un mes a seis años:*
a) El que con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del productor;
b) El que con el mismo fin facilite la reproducción ilícita mediante el alquiler de discos fonográficos u otros soportes materiales;
c) El que reproduzca copias no autorizadas por encargo de terceros mediante un precio;
d) El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura que lo vincule comercialmente con un productor legítimo; **(CASO PELÍCULA UN CUENTO CHINO)**

e) El que importe las copias ilegales con miras a su distribución al público.

El damnificado podrá solicitar en jurisdicción comercial o penal el secuestro de las copias de fonogramas reproducidas ilícitamente y de los elementos de reproducción.

El juez podrá ordenar esta medida de oficio, así como requerir caución suficiente al peticionario cuando estime que éste carezca de responsabilidad patrimonial. Cuando la medida precautoria haya sido solicitada por una sociedad autoral o de productores, cuya representatividad haya sido reconocida legalmente, no se requerirá caución.

Si no se dedujera acción, denuncia o querella, dentro de los 15 días de haberse practicado el secuestro, la medida podrá dejarse sin efecto a petición del titular de las copias secuestradas, sin perjuicio de la responsabilidad que recaiga sobre el peticionante.

A pedido del damnificado el juez ordenará el comiso de las copias que materialicen el ilícito, así como los elementos de reproducción. Las copias ilícitas serán destruidas y los equipos de reproducción subastados. A fin de acreditar que no utilizará los aparatos de reproducción para fines ilícitos, el comprador deberá acreditar su carácter de productor fonográfico o de licenciado de un productor. El producto de la subasta se destinará a acrecentar el "fondo de fomento a las artes" del Fondo Nacional de Derechos de Autor a que se refiere el artículo 6° del decreto-ley 1224/58." (Artículo incorporado por art. 2° de la Ley N° 23.741 B.O. 25/10/1989).

- **DECRETO 165/94.**

ARTÍCULO 1: *"A los efectos de la aplicación del presente decreto y de la demás normativa vigente en la materia:*
a) Se entenderá por obras de software, incluidas entre las obras del artículo 1º de la ley 11.723, a las producciones constituidas por una o varias de las siguientes expresiones:
I. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación;
II. Los programas de computación, tanto en su versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por el computador;
III. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.

b) Se entenderá por obras de base de datos, incluidas en la categoría de obras literarias, a las producciones constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos.
c) Se considerarán procedimientos idóneos para reproducir obras de software o de base de datos a los escritos o diagramas directa o indirectamente perceptibles por los sentidos humanos, así como a los registros realizados mediante cualquier técnica, directa o indirectamente procesables por equipos de procesamiento de información.
d) Se considerará que una ***obra de software*** *o de base de datos tiene el carácter de publicada cuando ha sido puesta a disposición del público en general, ya sea mediante su reproducción sobre múltiples ejemplares distribuidos comercialmente o mediante la oferta generalizada de su transmisión a distancia con fines de explotación.*
e) Se considerará que una ***obra de software*** *o de base de datos tiene el carácter de inédita, cuando su autor, titular o derechohabiente la mantiene en reserva o negocia la cesión de sus derechos de propiedad intelectual contratando particularmente con los interesados"*

- **CONVENIO DE BERNA:** Ley 25.140 para la Protección de las Obras Literarias y Artísticas, el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Interpretación o Ejecución y Fonogramas y el Tratado de la Organización Mundial de la Propiedad Intelectual.

PROGRAMAS DE ORDENADOR. ARTÍCULO 4*:"Los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2 del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión (3).*

(3) Declaración concertada respecto del Artículo 4: El ámbito de la protección de los programas de ordenador en virtud del Artículo 4 del presente Tratado, leído junto con el Artículo 2, está en conformidad con el Artículo 2 del Convenio de Berna y a la par con las disposiciones pertinentes del Acuerdo sobre los ADPIC

- ***CONVENIO ADPIC (TRIPS en inglés).*** **CONVENIO SOBRE PROPIEDAD INTELECTUAL. RELACIONADOS CON EL COMERCIO**

ARTÍCULO 2*:*
1. "En lo que respecta a las Partes II, III y IV del presente Acuerdo, los Miembros cumplirán los artículos 1 a 12 y el artículo 19 del Convenio de París (1967).

2. Ninguna disposición de las Partes I a IV del presente Acuerdo irá en detrimento de las obligaciones que los Miembros puedan tener entre sí en virtud del Convenio de París, el Convenio de Berna, la Convención de Roma y el Tratado sobre la Propiedad Intelectual respecto de los Circuitos Integrados."

SÍNTESIS DE LA EVOLUCIÓN DE LA PROTECCIÓN JURÍDICA DEL SOFTWARE.

DERECHO COMPARADO. EEUU

A continuación enumero los momentos que delimitaron su protección:

- 1960: El hardware (ordenador) era comercializado junto con el software, por tanto su protección estaba en manos de la Propiedad Industrial. Los programas aun no tenían carácter de "autoría".
- 1966: EEUU admite registros de programas para su patentamiento de forma individual al hardware.
- 1988: Surge la Ley Federal de protección de programas bajo derechos de autor, y posteriormente varios países dictaron leyes similares.

7.3. ARGENTINA. ETAPAS. CASOS EMBLEMÁTICOS DE NUESTRA JURISPRUDENCIA LOTUS Y DESK

Nuestro derecho positivo paso por varias etapas que sucintamente describo.

PRIMERA ETAPA:

- 1933: se sanciona la Ley 11.723 de Propiedad Intelectual, la cual alcanzaba la protección de obras científicas, literarias y artísticas, junto con disposiciones penales.
- A posteriori y hasta 1994, es decir en ese lapso, más aún con los antecedentes del derecho comparado, surge el interrogante ¿los programas de computación (hasta ese entonces no abundaba la IA, como sucede hoy) son una creación del intelecto? Existiendo diferencias de percepción entre el derecho penal y el derecho civil.
- 1994: FALLO LOTUS, la cámara por mayoría establece por analogía que sí constituye una idea, es decir un acto intelectual.

SEGUNDA ETAPA:

- 1994: decreto 165/94 - Por la presión de los EEUU, por las duplicaciones de medicamentos, de software, de música, etc., el Poder Ejecutivo Nacional dicta el 3 de febrero de 1994, el decreto, bajo el título Propiedad Intelectual, por el cual redefine el concepto de obra, introduciendo por ende en el mismo conductas que antes no abarcaba, e incorporando a las mismas la tutela penal que la ley prevé en sus artículos 71 y 72. O sea que modifica la definición contenida en el artículo primero de la ley. Otro aspecto importante es que el Poder Ejecutivo Nacional, no estaba facultado por el Congreso, ni por delegación de la ley, para redefinir el concepto de obra intelectual, por ende es inconstitucional, inclusive aunque hubiera sido un decreto de necesidad y urgencia, en el aspecto penal sería inconstitucional, pues el Presidente tiene expresamente prohibido en la Constitución Nacional legislar en materia penal, conforme el art. 99 inc. 3 de la CN.

  Asimismo se introduce un procedimiento de registro, inédito en DNDA.
- 1995: FALLO AUTODESK, declara válido el decreto del 94', pero deja sin efecto la tutela penal.

TERCERA ETAPA:

- 1995: Argentina firma el tratado ADPIC/TRIPS ratificado por ley, el cual protege programas y compilación de datos.
- 1995: Se cuestiona en el fallo AUTODESK, que al no haber una definición de software, no se puede perseguir penalmente la copia sin un tipo penal, por prohibirse la analogía *in malam partem*. Motivo desencadenante de la ley de software 25.036.

- 1998: Se modifica la ley 11.723 por medio de la sanción de la 25.036, incorporando a los programas de computación y se establece que la acción penal alcanza al software en virtud del tratado ADPIC/TRIPS.

ANEXO 6 - CASO SHADOWCREW

A LA CAZA DEL MAYOR CIBERLADRÓN

de James Verini

28 NOV 2010 - 03:00 ART

Una noche de julio de 2003, cerca de la medianoche, un agente del departamento de policía de Nueva York que investigaba una serie de robos de coches en un distrito de Manhattan siguió a un hombre joven con aspecto sospechoso hasta un cajero situado a la entrada de un banco. El agente observó cómo el hombre sacaba una tarjeta de crédito de su bolsillo y retiraba cientos de dólares en efectivo. Después sacó otra tarjeta y realizó la misma operación. Y otra vez. Y una vez más. El tipo no estaba robando coches, pero el policía se imaginó que estaba robando algo.

El joven estaba en efecto realizando una operación de "retirada de efectivo", tal como más tarde admitiría. Había programado un montón de tarjetas de crédito sin datos con números de tarjetas robados y estaba sacando todo el dinero que podía de cada cuenta. Lo había hecho unos minutos antes de las 12 de la noche, hora límite diaria para retirar dinero y el momento en que el cajero puede dar el doble de dinero con otra retirada en efectivo unos minutos más tarde. El policía le preguntó su nombre y aunque el hombre tenía varios alias en Internet, le dio el suyo verdadero. "Albert Gonzalez", contestó.

Albert Gonzalez fue detenido y rápidamente conducido hasta la oficina del fiscal de Nueva Jersey en Newark, quien, junto con agentes del destacamento oficial de delitos informáticos del FBI, estaba investigando sin mucho éxito el fraude de tarjetas de crédito y débito en los cajeros automáticos de la zona. Gonzalez fue interrogado y pronto se descubrió que era un tipo peculiar. No solamente poseía los datos de millones de cuentas de tarjetas almacenados en el ordenador de su apartamento en Nueva Jersey, sino que además tenía un truco para explicar online su experiencia como defraudador de tarjetas de crédito.

Tal como descubrirían los agentes del orden público, Gonzalez era un prometedor intermediario de shadowcrew.com, un ciberbazar de programas piratas que se expandió a principios del año 2000 durante el boom del comercio en Internet. Shadowcrew tenía cientos de miembros en Estados Unidos, Europa y Asia. Según me explicó un fiscal federal, era "una especie de eBay, monster.com y MySpace, pero dedicada al delito informático".

Tras un par de interrogatorios, Gonzalez aceptó ayudar al Gobierno y así evitar un proceso judicial. "Tenía 22 años y estaba asustado", me comentó más tarde. Gonzalez se convirtió en el confidente de delitos informáticos más valioso que el Gobierno de EE UU haya tenido jamás. Su ayuda permitió a la policía acusar a más de una docena de miembros de Shadowcrew, por lo que los agentes asignados a Gonzalez, empleados del FBI, le convencieron para que por su propia seguridad se trasladara a vivir a Miami, su ciudad natal. Después de prestar su ayuda en otra investigación, a principios de 2006 se convirtió en un confidente a sueldo del FBI en Miami. El hombre del FBI que mejor llegó a conocer a Gonzalez, el agente Michael (apodo de su verdadero nombre), fue trasladado a Miami y trabajó con Gonzalez en una serie de investigaciones en las que realizaron un trabajo tan extraordinario que la agencia le pidió que participara en seminarios y conferencias. "Parecía que estaba intentando hacer lo correcto", comentaba Michael.

Y sin embargo no era así. Durante los muchos años que trabajó para el Gobierno, Gonzalez, su banda de hackers y otros seguidores tuvieron acceso aproximadamente a 180 millones de cuentas de tarjetas de pago que estaban guardadas en la base de datos de clientes de algunas de las empresas norteamericanas más conocidas.

En la sentencia dictada el pasado marzo en la que fue condenado a dos penas simultáneas de 20 años, la mayor sentencia jamás dictada a un norteamericano por un delito informático, el juez dijo: "Lo que me pareció terrible fue que usted engañó a la agencia del Gobierno con la que al mismo tiempo estaba colaborando, por lo que usted era un agente doble".

Gonzalez compró su primer ordenador cuando tenía 12 años. A los 14 entró ilegalmente en los ordenadores de la NASA, con lo que consiguió que los agentes del FBI fueran a visitarlo a su colegio en Miami. Pero Gonzalez no se amilanó. Organizó un grupo de black hats -un tipo de hackers con tendencia a ir contra la autoridad- y consiguió cierta fama. Entonces abandonó sus estudios universitarios en la Universidad del Condado de Miami en el primer curso. Él mismo había aprendido, leyendo manuales de software, cómo atacar los ordenadores de los proveedores de servicios de Internet para conseguir banda ancha gratis. Se dio cuenta de que aún podía ir más lejos y obtuvo los nombres y claves de acceso de directores y ejecutivos.

El mejor amigo de Gonzalez, Stephen Watt, que se encuentra en estos momentos en la cárcel cumpliendo una condena de dos años por descifrar un programa de software que permitió a Gonzalez robar datos de tarjetas, describe a Gonzalez como "poseedor de una cualidad al estilo de Sherlock Holmes, producto de su buena educación".

Fue en 2003, justo después de haber aceptado convertirse en confidente, cuando Gonzalez ayudó al Departamento de Justicia y al FBI a preparar, en el transcurso de un año, una trampa ingeniosa para destapar Shadowcrew. Gonzalez era el cerebro de la Operación Firewall. Gracias a él, el Gobierno consiguió "poseer", según la jerga de los hackers, Shadowcrew. Compradores secretos se infiltraron en la red y siguieron el rastro de sus usuarios por todo el mundo; con el tiempo, los funcionarios incluso consiguieron transferir el sitio a un servidor seguro controlado por el FBI. Gonzalez convenció a los usuarios de Shadowcrew para que se comunicaran a través de una red privada virtual, un canal seguro que comunicaba a los ordenadores entre sí enviando mensajes codificados que él mismo introducía en el sitio. Esta red privada virtual tenía una característica especial: estaba intervenida por orden judicial.

Gnzalez trabajó con los agentes durante varios meses. La mayoría de ellos le llamaban Albert. Otros le conocían como Soup, por el nombre que había dado a su antigua pantalla, Soupnazi. "Haber pasado tanto tiempo con un confidente que estaba profundamente metido en una trama de delito informático fue una experiencia totalmente nueva para nosotros", explica un fiscal del Departamento de Justicia. "Fue una experiencia de las que dejan huella".

El 26 de octubre de 2004, Gonzalez fue trasladado a Washington, donde se estableció el centro de control de la Operación Firewall en las oficinas centrales del FBI. Consiguió sus objetivos en una sesión de chat. A las nueve de la noche, los agentes comenzaron a derribar puertas. Hacia la medianoche, 28 personas habían sido detenidas en ocho Estados norteamericanos y en seis países, la mayoría de ellas a escasos metros de sus ordenadores. Con el tiempo, otras 19 fueron acusadas. Según algunas informaciones, el Gobierno nunca antes había logrado llevar a cabo un caso tan importante y con tanto éxito contra el delito informático.

Un día después del asalto, los funcionarios del FBI pusieron en la página de inicio de Shadowcrew una fotografía de un matón jorobado, sin camisa, en la celda de una cárcel, con un tatuaje en el que se podía leer: "¡Póngase en contacto con su agente local del FBI de Estados Unidos… antes de que nosotros contactemos con usted!".

"La investigación resultó apasionante", me comentó un día Gonzalez mientras hablábamos sobre Shadowcrew. "Desenmascararlos, conocer sus identidades. Sin embargo, cuando pienso en ello, me parece que fue bastante fácil. Cuando alguien confía en uno, puedes bajar la guardia".

Sin embargo, "tenía mala conciencia por todo lo que había pasado". "A diferencia de otros confidentes, tuve un dilema moral", me confesó también. En otra ocasión, cuando estaba

hablando sobre el tema, Gonzalez me escribió una carta: "Me gustaría dejar una cosa bien clara… siempre he sido leal a la comunidad de los black hats".

Tras la Operación Firewall, Gonzalez volvió a Miami a finales de 2004. Por entonces estaba investigando sobre la vulnerabilidad de las redes inalámbricas en las empresas. Gonzalez estaba especialmente interesado en las posibilidades de una técnica conocida como wardriving. Los hackers, provistos de portátiles y antenas de radio de gran alcance, aparcan sus coches o furgonetas en los parkings de las grandes tiendas de ordenadores para detectar las redes wifi de las empresas más vulnerables.

Gonzalez contactó de nuevo con Christopher Scott -un viejo amigo de una red social en Internet, EFnet, frecuentada por black hats-, que estaba dispuesto a hacer un trabajo especial. Scott comenzó a intercambiar datos comerciales de la autopista 1 de Miami para buscar objetivos wardriving. Sus experimentos en BJ's Wholesole Club en Miami y en DSW tuvieron éxito. Robó cerca de 400.000 cuentas de tarjetas del primero y un millón del segundo. Le explicó a Gonzalez cómo lo había hecho y le pasó los números de tarjetas.

El verano siguiente, Scott aparcó su coche delante de una de las tiendas Marshall. Consiguió la ayuda de Jonathan James, un menor muy conocido entre los black hats de Miami por haber sido el primer joven norteamericano encarcelado por delitos informáticos. Scott pirateó la red wifi de Marshalls y, junto a James, comenzó a navegar dentro del sistema: capturaron nombres de usuario y claves de acceso, lo que permitió a Gonzalez entrar en la red; atacaron los servidores de la central de Marshalls en Framingham, Massachusetts y en TJX, una filial de la empresa, y localizaron los servidores que alojaban las operaciones con antiguas tarjetas de las tiendas.

A finales de 2006, Gonzalez, Scott y James tenían información de más de 40 millones de tarjetas. Utilizaron los mismos métodos para piratear los ordenadores de OfficeMax, Barnes & Noble, Target, Sports Authority y Boston Market, y probablemente de muchas otras empresas que nunca detectaron que sus equipos hubieran sido pirateados, o al menos no lo notificaron a las autoridades.

Al mismo tiempo que robaba datos de tarjetas bancarias, Gonzalez participaba en una organización internacional. Tomó contacto con un ucranio, Maksym Yastremskiy, que le vendió un conjunto de números de tarjetas de consumidores de Estados Unidos, América del Sur, Europa y Asia, y compartió las ganancias con él. Gonzalez contrató a otro amigo de EFnet, Jonathan Williams, para sacar dinero de todos los cajeros del país. Un amigo de Watt en Nueva York recogía los envíos de dinero en efectivo que Williams y Yastremskiy habían enviado. Entonces, el amigo de Watt enviaba el dinero a Miami o a un apartado de correos que James había creado con la colaboración de un intermediario. Gonzalez creó sociedades ficticias en

Europa. Para cobrar y lavar el dinero abrió una cuenta e-gold y cuentas WebMoney difícilmente controlables. Por último, contactó con dos hackers del este de Europa a quienes solamente conocía por los nombres que mostraban en su pantalla, Annex y Grig, y que estaban dispuestos a entrar en los procesadores de datos de las tarjetas de crédito americanas, el centro neurálgico de las ventas al por menor. "Muchas veces me he preguntado por qué hice todo esto", me dijo recientemente Gonzalez desde la cárcel un día mientras hablábamos por teléfono. "Sobre todo lo hice por dinero. El dinero que ganaba en el FBI no era suficiente y yo lo necesitaba. Cuando me di cuenta, la bola de nieve ya se había formado y era difícil detenerla. Intenté dejarlo, pero no pude". Afirma que sus intenciones eran en parte buenas. Lo que realmente él quería era ayudar a Patrick Toey, un amigo íntimo y hacker que más tarde le ayudaría en otro trabajo.

A diferencia de Gonzalez y de Watt, Toey, de 25 años, tuvo una educación complicada. Tras abandonar sus estudios, tuvo que ayudar a su madre, a su hermano pequeño y a su hermana pirateando ordenadores. Gonzalez prestó su apartamento de Miami a Toey sin cobrarle ni un céntimo. La casa era de su propiedad, pero él prefería vivir en casa de sus padres. Dice que le encantaba cómo cocinaba su madre y jugar con su sobrino. Además, de esa forma tenía más facilidad para lavar el dinero.

A Gonzalez le entusiasmaba también los retos que le proporcionaba el delito informático. No es un programador que destaque por su talento, sino por la forma especial que tiene para introducirse en los sistemas y en las cuentas. A menudo tengo la impresión de que para Gonzalez el delito informático era como un recurso de apelación.

Pero lo cierto es que le gustaba robar. "La emoción siempre conseguía vencer cualquier sentimiento moral que pudiera sentir", me dijo. Y también le gustaba gastar. En parte, aunque no del todo, se puso a explicarme su plan en la operación "hazte rico o muere en el intento". No quiso decirme cuánto dinero había conseguido, pero está claro que está obteniendo beneficios de los millones de dólares que robó. Parte de ese dinero fue a parar a Toey, pero probablemente nada fue para Watt.

En la primavera de 2007, Gonzalez estaba cansado de trabajar para el FBI. "Siempre llegaba tarde", según la opinión del agente Michael, que habló con otros agentes sobre la posibilidad de controlar a Gonzalez. "No quería estar aquí". Además estaba cansado del wardriving. Buscaba nuevos desafíos.

González puso toda su atención en TJX, en parte porque almacenaban antiguas transacciones, pero se dio cuenta de que muchas de las tarjetas estaban caducadas. Necesitaba encontrar una manera de conseguir los números de tarjetas justo después de que los clientes las hubieran utilizado. Era posible. Consiguió averiguar cómo meterse en los

terminales punto de venta de las tiendas y en los datáfonos de los supermercados, de las gasolineras, de los almacenes o de cualquier otro comercio donde se pudiera comprar algo.

Gonzalez y Toey recorrieron las tiendas de Miami para ver las marcas de los terminales con los que trabajaban. Gonzalez descargó manuales y esquemas de software. Antes de esto, Williams había visitado una tienda de OfficeMax cerca de Los Ángeles donde desenchufó un terminal y salió de la tienda con él. Algunos hackers que trabajaban con un contacto de Gonzalez en Estonia atacaron los ordenadores de la central de Micro Systems en Maryland, el mayor fabricante de sistemas de puntos de venta, y robaron software y una lista con los nombres y claves de acceso de los empleados y se la enviaron a Gonzalez.

Entonces, una vez que Toey le introdujo en el sistema, Gonzalez ya no tuvo que rastrear en las bases de datos para conseguir información valiosa. Podía acceder directamente a los servidores donde llegaban los datos de las tarjetas recién utilizadas, milésimas de segundos antes de que la información fuera enviada al banco para su aprobación. Realizó esta operación en JC Penney, en las tiendas de ropa Wet Seal y en Hannaford Brothers, una cadena de tiendas de alimentación. Su contacto en Estonia utilizó la misma técnica en Dave & Buster's. "Cada vez que un comercio pasaba una tarjeta, los datos quedaban registrados en nuestros ficheros", explica Toey. "Nadie podía hacer nada".

Unos días antes de la Navidad de 2006, los abogados de TJX llamaron alarmados al Departamento de Justicia y a Stephen Heymann, ayudante del fiscal de Estados Unidos en Massachusetts. Una empresa de tarjetas de crédito había contactado con la compañía, ya que, al parecer, habían descubierto el robo de un gran número de tarjetas que se habían utilizado en Marshalls y en T. J. Maxx. TJX había examinado sus servidores en Framingham y lo que habían descubierto era una catástrofe. Creían que durante casi un año y medio, "los datos de aproximadamente la mitad de las transacciones realizadas con tarjetas en comercios de Estados Unidos, Puerto Rico y Canadá" habían sido robados. Fue el mayor robo de datos de tarjetas en la historia de Estados Unidos y no había ninguna prueba de ello.

En 2007, los abogados de Dave & Buster's llamaron al FBI. Esta empresa también había sufrido ataques, pero su caso era diferente. Los ladrones se las habían ingeniado para acceder al sistema de puntos de venta. En verano, Heymann y Kim Peretti, fiscal jefe de delitos informáticos del Departamento de Justicia, tenían sobre su mesa una gran cantidad de datos, montones de posibles pruebas y ningún rastro sobre a quién tenían que perseguir. Desesperados, necesitaban encontrar una pista como fuera.

Y les llegó de la mano de los viejos amigos de Peretti en el destacamento oficial de delitos informáticos del FBI. Resultó que, durante dos años, un agente secreto de la oficina de San Diego había estado comprando a Yastremskiy tarjetas de memoria. El agente viajó a

Tailandia y a Dubai para encontrarse con el ucranio y en Dubai copió el disco duro del portátil de Yastremskiy sin que este se diera cuenta. Especialistas en informática del FBI peinaron la copia del disco duro y descubrieron que Yastremskiy guardaba meticulosamente los documentos. Desde hacía años, había salvado y catalogado todas las listas de sus clientes y los mensajes que había recibido. En los registros encontraron a un compañero de chat que parecía ser su mayor proveedor de datos de tarjetas robadas. Sin embargo, todo lo que pudieron conseguir de esta persona fue un número de registro de mensajería instantánea, pero ninguna información personal.

Yastremskiy fue detenido en julio de 2007 en un club nocturno en Turquía. El FBI consiguió de él una prueba muy útil. Su proveedor anónimo le había pedido que le consiguiera un pasaporte falso. Según le había comentado, uno de sus proveedores había sido detenido y quería ayudarle sacándolo de EE UU. El problema: no sabía dónde había sido detenido.

Así que los agentes llamaron a cada una de las comisarías de policía y del fiscal del distrito de todo el país en las que hubieran realizado una detención similar o estuvieran trabajando en un caso parecido. La investigación les condujo a una cárcel de Carolina del Norte donde se encontraba Williams. Había sido detenido llevando encima 200.000 dólares en efectivo. Los agentes del FBI conectaron un pendrive que Williams llevaba en el momento de su detención y encontraron un fichero que contenía una fotografía de Gonzalez, un historial de crédito y la dirección de su hermana María en Miami. "El archivo era una medida de seguridad en caso de que Gonzalez intentara contactar conmigo", me comentó Williams desde la cárcel el pasado mes de junio. Entonces, los funcionarios siguieron la pista de los paquetes que Williams había enviado al apartado de correos de Miami. Esto condujo al FBI hasta James. Registraron los archivos de la policía y descubrieron que en 2005 un oficial de policía le había detenido de madrugada en Palmetto Bay (Florida), junto a Scott, en el parking de una tienda.

El momento culminante llegó cuando los funcionarios del FBI finalmente consiguieron la información del número de registro de mensajería instantánea de quien estaba suministrando a Yastremskiy los datos de tarjetas bancarias. No había una dirección ni un nombre, pero sí una dirección de correo electrónico: soupnazi@efnet.ru. Era la prueba evidente para quien conociera a Gonzalez.

Enseguida, la operación "hazte rico o muere en el intento" se puso en marcha. La policía registró los domicilios de Scott y de Gonzalez. Los agentes detuvieron a Scott y se llevaron nueve ordenadores y 78 plantas de marihuana. En la casa de Gonzalez encontraron varias drogas de diseño y a un medio dormido Toey. Este fue conducido a Boston para prestar declaración ante un jurado de acusación. Les dijo a Heymann y a Peretti dónde localizar las cuentas e-gold y WebMoney y los servidores que estaban alojados fuera del país. Gracias a estos servidores pudieron localizar a Watt, que había vuelto a su apartamento de Greenwich

Village, donde se encontró a un grupo de policías esperándolo. También registraron la casa de Gonzalez, pero Albert no estaba allí.

Finalmente la policía le localizó el 7 de mayo de 2008 a las siete de la mañana en la suite del hotel National en Miami Beach. Junto a él había una mujer croata, dos portátiles y 22.000 dólares. Comenzó a hablar rápidamente. Meses después condujo a los agentes del FBI hasta un contenedor enterrado en el jardín de la casa de sus padres en el que había 1,2 millones de dólares. El abogado de Gonzalez le aseguró que para el Gobierno era un caso que no tenía mucha consistencia. Las pruebas electrónicas a menudo no se sostienen, afirmó.

Esto fue antes de que los abogados de Heartland Payment Systems en Princeton (Nueva Jersey) hubieran llamado a Peretti a principios de enero de 2009. Heartland, una de las empresas más importantes del país de datáfonos, había sido atacada. Pronto Gonzalez le confesó a Peretti que había ayudado a Annex y a Grig a entrar en Heartland a través de una técnica conocida como inyección SQL. Por entonces, en Heartland ya se habían dado cuenta de que algo no funcionaba bien. Este robo había sido demasiado importante: habían desprotegido los datos de 130 millones de transacciones. Gonzalez fue acusado en Nueva Jersey, Nueva York y Massachusetts (donde había pruebas más contundentes del caso).

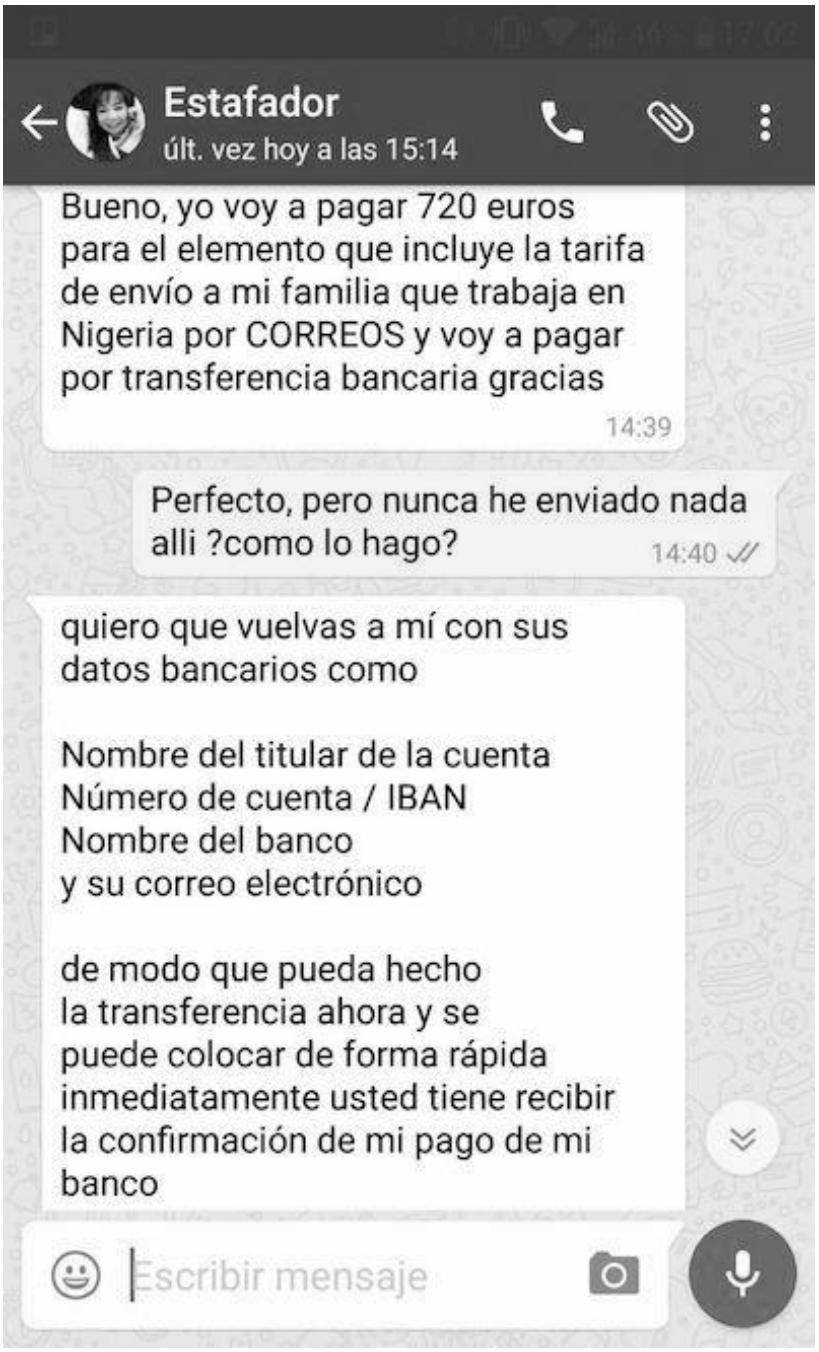
En la sentencia dictaminada en marzo, Gonzalez fue declarado culpable de todos los cargos. Teniendo en cuenta el tiempo que pasó en prisión antes de la condena y el buen comportamiento, probablemente saldrá de la cárcel en 2025.

En mayo, Toey ingresó en prisión para cumplir una condena de cinco años, y Scott, una de siete. A Yastremskiy le cayeron 30 años en una cárcel de Turquía. Watt, que afirmó que nunca supo muy bien para qué quería utilizar González su software y no quiso dar información sobre Gonzalez al jurado o al fiscal, ha sido condenado a dos años.

Según el fiscal general Eric Holder, TJX, Heartland y otras empresas víctimas de los ataques de Gonzalez tuvieron que hacer frente a más de 400 millones de dólares en reembolsos y honorarios de abogados y forenses. Al menos 500 bancos se vieron afectados por el ataque a Heartland. En Estados Unidos, el fraude online continúa en auge, aunque las estadísticas muestran una caída importante en 2009 respecto a años anteriores, cuando Gonzalez estaba en activo.

Tras la sentencia, González fue trasladado al Metropolitan Detention Center (MDC) en Brooklyn (anteriormente había estado en una prisión de Michigan). Situado entre un tramo de la autopista de Brooklyn a Queens y Gowanus Bay, el MDC es un sitio horrible incluso para ser un centro penitenciario. "Este lugar es terrible", dijo el agente Michael. "Pero ¿quiere que le diga una cosa? Cuando se juega con fuego, esto es lo que se consigue".

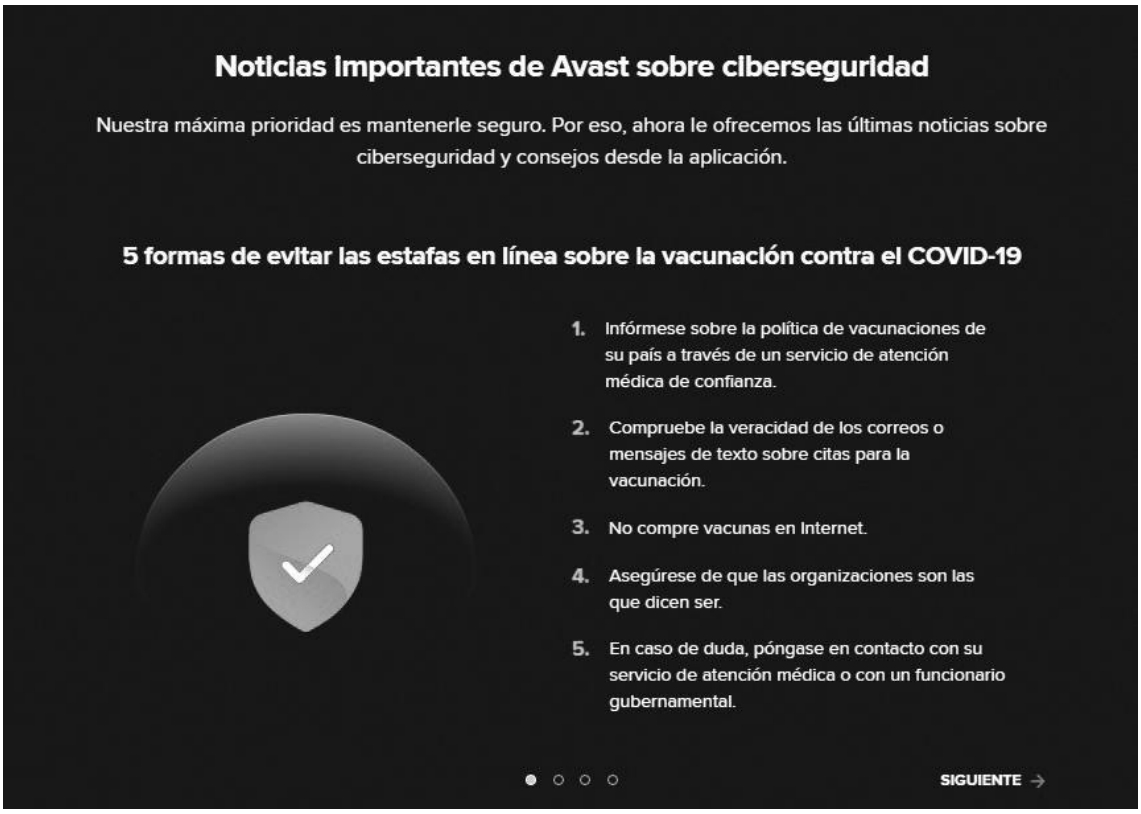
ANEXO 7 - ESTAFA NIGERIANA



Fuente: **Cuidado con la nueva estafa nigeriana**

Link: https://www.elgrupoinformatico.com/cuidado-con-nueva-estafa-nigeriana-t32387.html

ANEXO 8 - PHISHING. PREVENCIÓN




¿Se pregunta si alguien intenta estafarle? Siga este razonamiento:
1 ¿Parece demasiado bueno para ser verdad?
2 ¿Se han puesto en contacto con usted sin permiso?
3 ¿Le piden información personal y privada?
4 ¿Le piden dinero para hacer algo?
Si responde afirmativamente a alguna de estas preguntas, podría tratarse de una estafa.
ATRÁS
SIGUIENTE


Esperamos que esta información le resulte útil
Su antivirus Avast le protege frente a las estafas de ransomware y phishing, pero es importante que siga atento a las nuevas amenazas y sepa cómo evitarlas. Desde Avast, le deseamos que siga seguro, esté conectado o no.
Desde Avast, le deseamos que siga seguro, esté conectado o no.
EXPLORE SU APLICACIÓN
ATRÁS

page not found