EDI

REVISTA DIGITAL NRO 30 - DICIEMBRE 2018

2019...

Continuamos

ELDERECHOINFORMATICO.COM

"Los **datos** no son el **petróleo** de la época, lo **supera** en valor e **implicaciones** sociales: es **renovable**, permite **perfilar** nuestro **comportamiento**, contiene datos de nuestra **intimidad**."

Mabel Cueto en su conferencia en Pta Cana

LEGALTechFORUM GUATEMALA

EL FUTURO TECNOLOGICO DEL SECTOR JURIDICO

EDI Capítulo GUATEMALA
Red Iberoamericana El Derecho Informático

17 de Noviembre del 2018
Club Centro Español, Calzada Roosevelt | Guatemala, Centroamérica
www.infogtm.com | www.ogdi.org | www.elderechoinformatico.com

"La **Seguridad** de tu **información digital** no es un **juego**...el futbol si!
Cuida tu **información** electrónica."

EDI Capítulo GUATEMALA

Red Iberoamericana el Derecho Informático
www.elderechoinformatico.com
El centro de información más grande de Iberoamérica

INDICE


(EDI)
ELDERECHOINFORMATICO.COM
ESTAMOS
DONDE QUERÉS VOS
• SOMOS, LA RED •

Hemos llegado al N° 30 de nuestra Revista Digital, como desde hace ya unos años, les ponemos a disposición excelentes artículos, con gente de distintos paises de latinoamerica.
También van a encontrar 30 (entre personas y entidades) que hemos considerado que se han destacado dentro de diferentes categorias en cuestiones que hacen al Derecho Informático. Ya razones y demás cuestiones de los porque ellos y no otros, están explicados dentro de la revista, por lo que me remito a lo allí expuesto.-

"Las buenas costumbres, y no la fuerza, son las columnas de las leyes; y el ejercicio de la justicia es el ejercicio de la libertad."
Simón Bolivar

EDITORIAL

Un 2018 bastante apagado para el gusto nuestro, esperábamos poder ser más activos en cuanto a congresos, una revista más periódica, cursos más seguidos, en fin, nos hubiera gustado estar más presentes, poder crecer a otro ritmo, no se dio, y no fue por falta de ganas, sino por limitaciones propias de quien escribe probablemente.

En defensa propia puedo decir que fue un año de repensar La RED, de procurar entender por donde es que tenemos que reinventarnos para mejorar, para seguir siendo apoyo y soporte de quienes incursionan en esta apasionante rama del Derecho, (que por cierto creo amerita en forma urgente un replanteo de su enfoque).

Al igual que otros años, organizamos congresos propios, colaboramos en la organización de otros, publicamos material inédito y apoyamos campañas de difusión de temas especialmente sensibles a la sociedad. Nos falto más, siempre falta más, no nos quedamos en que lo hecho es suficiente, por eso, para este 2019, no adelantamos nada, solo la promesa de buscar acercarnos a todos Uds, desvirtualizarnos, ser más abrazos y menos pantallas, la tecnología es maravillosa, pero no se cambia por una charla frente a frente en un break ni una sonrisa prometiendo volver a encontrarnos.
Que tengan un año fantástico

Director Guillermo M Zamora

SOMOS EDI LA RED

EL CENTRO DE INFORMACIÓN

y contenidos
más grande iberoamerica

TWITTER: ELDERECHOINF

Por: Emanuel Ortiz, bloguero de Huella Forense. Perito experto en informática forense. Analista -Malware - IOC - APT - Seguridad de la Información - Seguridad digital y Auditoría Forense.

La evidencia digital, definida a secas, provee ciertas características de importancia que demandan un estudio general de la informática forense como disciplina, desde el ámbito técnico-científico. Actualmente esta sirve como apoyo indispensable en la administración de la justicia y el derecho, por tanto, se deben tener en cuenta su desarrollo y criterios para poder adoptar un procedimiento adecuado.

Para solucionar estas ambigüedades, en lo que respecta a su aplicación o ejecución en la vida práctica, vale la pena mencionar los principales lineamientos que en virtud de la comisión de una conducta criminal o punible se puede derivar un tratamiento de evidencia digital ante un fraude o la examinación de información almacenada en cualquier tipo de dispositivo de almacenamiento digital.

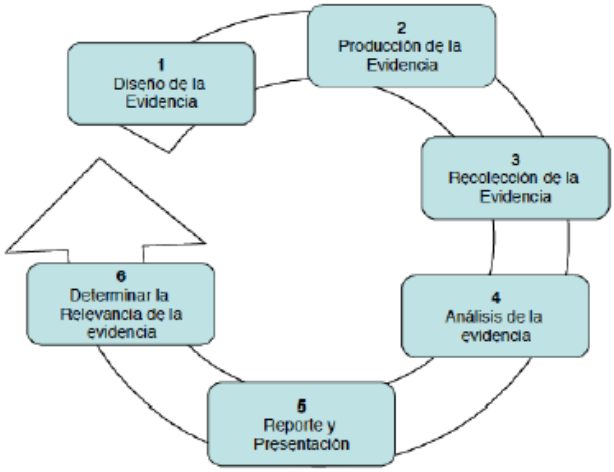
En ese sentido radica la importancia que tiene la creación de criterios y procedimientos para el tratamiento y análisis de la evidencia digital, los cuales permitan fortalecer toda la actividad del examinador, perito o especialista en informática forense, dentro de cada una de las conductas que se

presentan en los procesos investigativos. De tal forma que se diseñe un 'paso a paso' para recolectar, preservar y dar un tratamiento adecuado a la *Información Electrónicamente Almacenada*.

Esta aproximación permite enfocar los esfuerzos para unificar conceptos que orienten el resultado para garantizar los principios de confidencialidad, integridad y disponibilidad.

Existen actualmente distintas guías o parámetros que permiten abordar el procedimiento para la recolección de dispositivos de almacenamiento y/o electrónico estandarizadas bajo la orientación del Instituto Nacional de Estándares de Tecnología (sus siglas en inglés NIST[1]). Por ejemplo, hoy en día, el Departamento de Justicia de los Estados Unidos permite evaluar de manera continua los procedimientos unificados hacia el correcto aseguramiento, adquisición, examinación, análisis, documentación y entrega del reporte digital forense; de manera que estas actividades tienen observancia de un fiel manejo de la evidencia digital o electrónica.

Ilustración 1. Esquema del ciclo de vida de la evidencia digital.



Fuente: HB171:2003 Handbook Guidelines for the managment of IT Evidence

Otros aspectos de importancia que rodean el tratamiento de la evidencia digital tienen que ver con el estándar universal acoplado a las reglas americanas (Committee IT/012, Information. Systems, Security and Identification Technology o Australia) de clasificación y autenticidad de la data recolectada y para ello se deben consolidar unos aspectos incorporables en el tratamiento de la información electrónicamente almacenada, como:

> *- Determinar los tiempos de retención de documentos electrónicos, la transformación de estos (cambios de formato) y la disposición final de los mismos. [HB171]*

- Diseñar los registros de auditoría de las aplicaciones, como parte fundamental de la fase de diseño de la aplicación. Este diseño debe considerar la completitud y el nivel de detalle (granularidad) de los registros. [HB171]

- Utilizar medidas tecnológicas de seguridad informática para validar la autenticidad e integridad de los registros electrónicos. Tecnologías como certificados digitales, token criptográficos, entre otras podrían ser candidatas en esta práctica. [HB171]

- La infraestructura tecnológica debe asegurar la sincronización de las máquinas o dispositivos que generen la información, de tal manera que se pueda identificar con claridad la fecha y hora de los registros electrónicos. [HB171]

Desde el 2005, el Instituto SANS Internacional creó el manual de mejores practicas para la recolección de evidencia digital a partir de un estándar para enmarcar el procedimiento de recolección y tratamiento de la evidencia digital, el cual complementa la actividad del experto en materia del análisis de la evidencia digital y la información electrónicamente almacenada.

En este sentido, dicha organización ha promulgado la innovación frente a las tecnologías, promoviendo las mejores prácticas dentro de los esfuerzos para satisfacer las necesidades de la industria.

Uno de los cambios más recientes en el manejo de la evidencia ha sido el concepto 'Retirar el conector' (conector de energía) como un primer paso en la recopilación de pruebas para la adopción de metodologías dirigidas a adquirir evidencia cuando el computador del sospechoso se encuentra encendido.

Estos aspectos se han incorporado en las guías de recolección de evidencia digital y los retos propuestos respecto de la recolección de información en dispositivos físicos o en sistemas de información virtual.

Para SANS existe un orden específico en la toma de muestras o recolección de los datos volátiles de aplicaciones teniendo en cuenta un orden de prioridad o volatilidad primaria, así:

- *[2]CPU, memoria caché y registro de contenido.*
- *Tabla de enrutamiento , caché [3]ARP , tabla de procesos , las estadísticas del kernel y memoria [4]RAM.*
- *Sistema de archivos temporales / espacio de intercambio [5]SWAP, [6]hiberfil.sys y [7]Pagefile.sys*

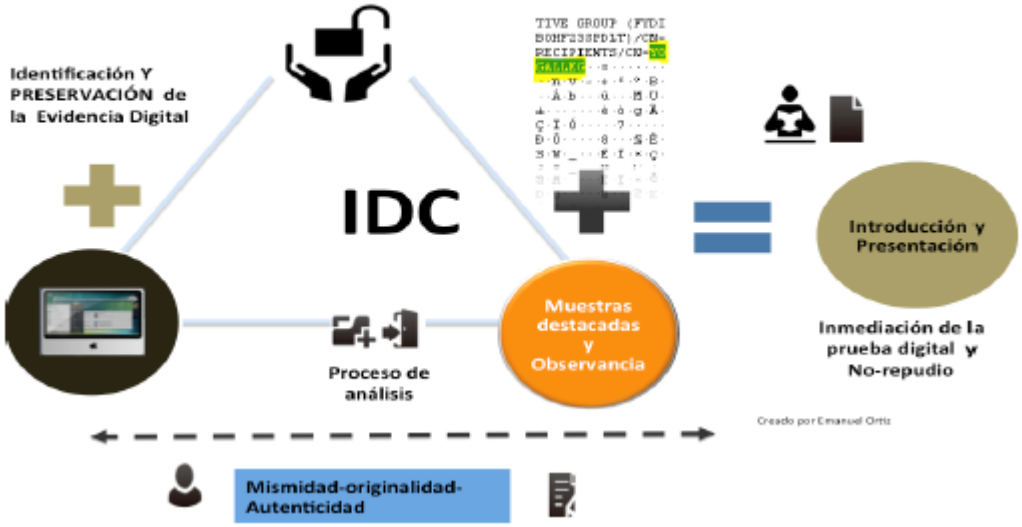
❍*Los datos contenidos en el disco duro.*

❍Datos remotos que estén registrados.

❍Los datos contenidos en los medios de archivo o unidades externas.

Aseguramiento de la evidencia digital

Ilustración 3 Principios Evidencia Digital



Uno de los aspectos incorporados de acuerdo a los estándares técnicos científicos ha sido la tendencia positiva a nunca manipular el dispositivo del sospechoso, por tanto es muy importante para el perito en informática forense tener en cuenta los siguientes aspectos:

- Por medio de fotografía, descriptiva y narrativamente documente el lugar de los hechos.

- Antes de tener contacto con el lugar utilice pulsera antiestática y guantes.

❍*Si el ordenador está apagado no lo encienda.*

- Si el equipo está encendido fotografíe la pantalla.

- Recopile datos en vivo - inicia imagen RAM con (Respuesta en vivo de forma local o remota a través de una herramienta forense) y luego recoja otros datos en vivo "como lo requiera", tales como el estado de conexión de red, usuarios conectados actualmente, la ejecución de procesos, etc.

- Si se detecta cifrado de disco duro recoja "la imagen lógica" del disco duro utilizando dd.exe, Helix, de forma local o remota a través de herramientas forenses *y tenga en cuenta la memoria RAM recolectada.*

- Desconecte el cable de alimentación de la parte posterior de la torre. Si el equipo es un portátil y no se cierra cuando se retira el cable, retire la batería.

- Diagrame y etiquete todos los cables.

- Documente todos los números de modelo de dispositivo y números de serie.

- Desconecte todos los cables y dispositivos.

- Compruebe HPA luego de imagen unidades de disco duro utilizando un bloqueador de escritura.

- Paquete de todos los componentes (usando bolsas de pruebas anti-estáticas).

- Aproveche todos los medios de almacenamiento adicional (adquisición de imágenes respectivas y coloque LSO dispositivos originales en bolsas de pruebas anti-estáticas) “Proteja siempre la evidencia original”.

- Mantenga todos los medios de comunicación fuera de los imanes, transmisores de radio y otros elementos potencialmente dañinos.

- Recoja instrucciones, manuales, documentación y notas.

- Documente todos los pasos utilizados en la recolección de datos volátiles y aseguramiento de los dispositivos de almacenamiento.

Principales guías para recolección y tratamiento de evidencia digital

1. Examen Forense de Evidencia Digital DOJ EEUU

Es el conjunto de características que reúne la Evidencia Digital.

(Forensic Examination of Digital Evidence: A Guide for Law Enforcement) [FoEx04].

- *Desarrollar políticas y procedimientos de la Evidencia Digital.*
- *Determinar el curso de la evidencia a partir del alcance del caso.*
- *Adquirir la evidencia.*
- *Examinar la evidencia.*
- *Documentación y reportes.*
- *Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).*

2. Guía de la IOCE

La IOCE [IOCE0], publicó la “Guía para las mejores prácticas en el examen forense de tecnología digital”. (Guidelines for the best practices in the forensic examination of digital technology) [IOCE0].

- Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal,

documentación, herramientas y validación de las mismas y espacio de trabajo).

- Determinación de los requisitos de examen del caso.

- Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).

3. Investigación en la escena del crimen electrónico

El Departamento de Justicia de los Estados Unidos de América (DoJ EEUU), publicó la "Investigación en la Escena del Crimen Electrónico" (Electronic Crime Scene Investigation: A Guide for First Responders) [ElCr01].

- Dispositivos electrónicos (tipos de dispositivos se pueden encontrar y cuál puede ser la posible evidencia).

- Herramientas para investigar y equipo.

- Asegurar y evaluar la escena.

- Documentar la escena.

- Recolección de evidencia.

- Empaque, transporte y almacenamiento de la evidencia.

- Examen forense y clasificación de delitos.

- Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

4. Guía RFC 3227

El "RFC 3227: Guía Para Recolectar y Archivar Evidencia", (Guidelines for Evidence Collection and Archiving) [GuEvCo02], escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group.

- Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.

- El proceso de recolección: transparencia y pasos de recolección.

- El proceso de archivo: la cadena de custodia y donde y como archivar.

5. El ISFS

Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense), creada en Hong Kong, publicó: "Computación Forense - Parte 2: Mejores Prácticas". (Computer Forensics – Part 2: Best Practices) [CoFor04].

- Introducción a la computación forense. Calidad en la computación forense.

❍*Evidencia digital.*

❍*Recolección de Evidencia.*

❍*Consideraciones legales (orientado a la legislación de Hong Kong). f) Anexos.*

❍*5.2.6 Guía de Buenas Prácticas para Evidencia Basada en Computadores.*

❍*La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido mediante su departamento de crimen por computador, publico "Guía de Buenas Prácticas para Evidencia Basada en Computadores" (Good Practice Guide For Computer Based Evidence) [GoPra99].*

❍*Los principios de la evidencia basada en computadores. Oficiales atendiendo a la escena.*

❍*Oficiales investigadores.*

❍*Personal para la recuperación de evidencia basada en computadores.*

❍*Testigos de consulta externos.*

❍*Anexos (legislación relevante, glosario y formatos).*

❍*5.2.7 Guía Para el Manejo de Evidencia Digital.*

❍*Standards Australia (Estándares de Australia) publicó "Guía para el Manejo de Evidencia en IT" (HB171:2003 Handbook Guidelines for the management of IT evidence) [HBIT03]. Esta guía no está disponible para su libre distribución, por esto para su investigación se consultaron los artículos "Buenas Prácticas en la Administración de la Evidencia Digital" [BueAdm06] y "New Guidelines to Combat ECrime" [NeGu03].*

❍*Diseño de la evidencia.*

❍*Producción de la evidencia.*

❍*Recolección de la evidencia.*

❍*Análisis de la evidencia.*

❍*Reporte y presentación.*

❍*Determinación de la relevancia de la evidencia.*

6. **Guía para el análisis forense a dispositivos creada por la Policía Nacional de Colombia.** *El cual no está publicado o aceptado todavía.*

Relevancia del Dictamen Pericial en el Procedimiento y su admisibilidad y contexto legal de validez probatoria

La evidencia digital obtenida debe ser clara y eficaz, para que los elementos que se desean aportar en el proceso y en el juicio soporten debidamente la actividad y el procedimiento efectuado. Por tanto, el fin del análisis y los aportes a los objetos de prueba deben ser los más relevantes para el esclarecimiento de los hechos en la comisión de la conducta.

En este sentido el estándar sugiere dos criterios para tener en cuenta: [*STANDARDS AUSTRALIA INTERNATIONAL 2003*]

- **Valor probatorio:** establece que el registro electrónico tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación y confiabilidad del sistema.
- **Reglas de la evidencia:** establece que se han seguido los procedimientos y reglas establecidas para la adecuada recolección y manejo de la evidencia.

Principios equivalentes al mensaje de datos como esencia jurídica de la evidencia digital en cualquier contexto forense

Primero se debe considerar el argumento bajo el derecho fundamental de la legalidad, el debido proceso y su valoración como evidencia, tal cual como se expone en el argumento de la Corte Constitucional de Colombia, en el cual refiere lo siguiente: "valorar una prueba no necesariamente implica admitir su contenido".

La valoración de la prueba es, precisamente, el procedimiento previo que permite establecer si el contenido de lo que se prueba puede ser admitido como elemento de convicción y sustento de la consecuencia jurídica.

Por ello, en el caso sub judice, no es cierto que las autoridades competentes hubieran dejado de valorar las pruebas allegadas al expediente. (Sentencia T-233/07); en ese orden de ideas ha sido clara en lo relacionado con la convicción y su consecuencia de su resultado o finalidad jurídica, entendida como la consecuencia jurídica de la obtención de la evidencia de carácter digital.

En precisión, la Corte referencia en la necesidad y conducencia de la prueba, comprender cada uno de los elementos esenciales de los derechos fundamentales para que estos se examinen bajo su expresión práctica en la actividad procesal y como fundamento, y evitar así la afectación

de contenidos en otros aspectos del debido proceso.

Si bien es cierto que la ley 527 de 1999 determina que los mensajes de datos transmitidos en o a través de internet pueden tener vocación probatoria en el proceso judicial, el código general del proceso (L. 1564/12), a través del artículo 175, también es admisible para algunas de las características esenciales de este mensaje de datos, como un elemento de discusión ante una evidencia demostrativa en etapa de juicio oral.

La [8] equivalencia funcional se presenta en total armonía con la argumentación o discusión de la existencia de un dato, respecto de la obtención y aseguramiento digital. Luego es fundamental pensar que los argumentos no distan o se separan por simple analogía o hipotética gramatical, empero guardan estructuras de similar comparación en aspectos técnicos y fundamentales para la aprehensión de manera integral u holística en la conducencia de la evidencia, para que tenga como fin último observarse la garantía procesal expuesta en toda su expresión técnica.

De acuerdo a lo anterior, es falso considerar que se subordina la titulación del mensaje de datos a un todo relacionado con la Información Electrónicamente Almacenada (IEA); luego dista de su calidad heterogénea y su convergencia en otras tecnologías. Por eso es distinto pensar que la evidencia digital o electrónicamente almacenada hace parte únicamente de la informática forense como ciencia auxiliar de la administración de justicia, porque corresponde a un sin número de ventajas en todos los aspectos de correlación e importancia y también comparte atributos de validez probatoria en materia del ejercicio y cumplimiento en una auditoría forense.

En conclusión, y señalando la importancia de la evidencia digital en la informática forense y otras áreas relacionadas con las disciplinas forenses, vale la pena exhortar que, independientemente de la guía de obtención de esta información, -que hizo o hace parte de una investigación digital- se debe comportar aspectos claros de independencia y autonomía, sin desligarlos del carácter técnico científico. En donde la persona idónea para hacerlo debe saber demostrar su validez probatoria, jurídica y procedimental para absolver la confiabilidad ante la naturaleza de esa evidencia digital. Luego responder a las necesidades de cualquier área profesional donde se obtenga data de obligatorio aseguramiento y tratamiento. Esto, bajo los estándares legales y análogos de cada país.

[1] Instituto Nacional de Estándares de Tecnología de los EE.UU

[2] Unidad Central de Procesamiento

[3] Protocolo De Redireccionamiento de direcciones

[4] Memoria de Acceso Aleatorio

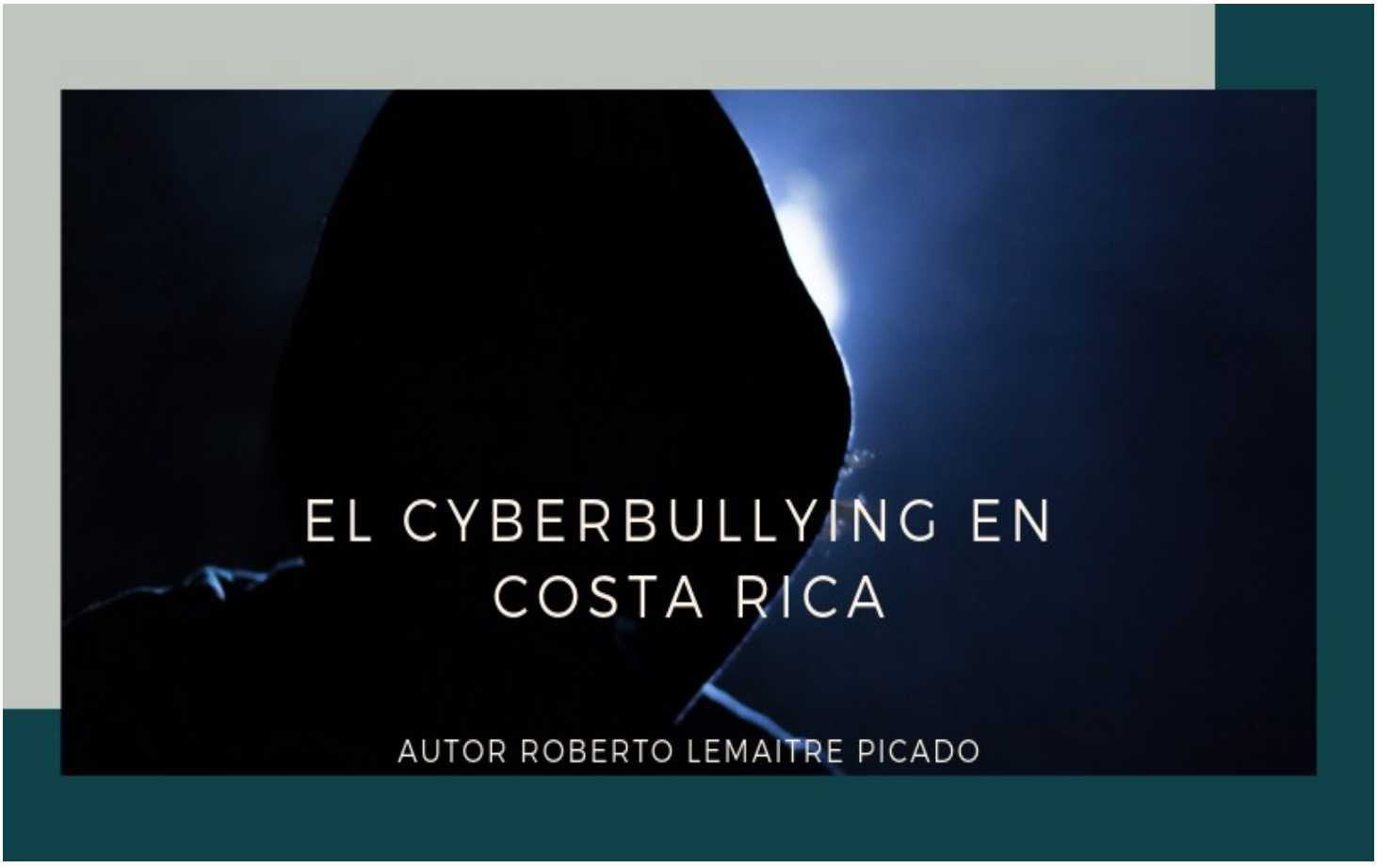
[5] Memoria de Intercambio en sistemas operativos Linux/Unix

[6] Archivo de hibernación

[7] Archivo de Paginación de Windows

[8] Son aquellos atributos de analogía con los principios fundamentales del mensaje de datos electrónico a la información contenida, en resultados obtenidos a través de la evidencia digital presentada como elemento material probatorio de una conducta punible o criminal.

Primeramente, debemos definir el término “cyberbullying”; este concepto proviene del inglés conformado por los términos “cyber” y “bullyng”, los cuales analizaremos a continuación: “Cyber” se refiere “al área virtual”, es decir, aquello que conocemos como “ciberespacio”, y que es generado por medio de tecnologías de la información; y por otra parte, el término “bullying”, que se divide en dos partes: “bull” del inglés que se traduce como “toro” en español, y luego “ying” que es la terminación “ando o endo” en español, y que implica la acción de estar llevando a cabo algo en ese momento, es decir, impregna de acción a la palabra; pero en este caso el contexto lo debemos entender como una acción de intimidación o matonismo.



Willard, N. en su guía “An Educator’s Guide to Cyberbullying and Cyberthreats” distingue siete formas de cyberbullying:

1. Flaming: Envío de mensajes vulgares o que muestran enfado sobre una persona a un grupo online o a esa persona vía email o servicio de mensajes cortos [SMS].

2. Acoso online: Envío repetido de mensajes ofensivos vía email o SMS a una persona.

3. Cyberstalking: Acoso online que incluye amenazas de daño o intimidación excesiva.

4. Denigración: Envíos perjudiciales, falsas y crueles afirmaciones sobre una persona a otras o comentarios en lugares online.

5. Suplantación de la persona: Hacerse pasarse por la víctima y enviar o colgar archivos de texto, video o imagen que hagan quedar mal al agredido. 36

6. Outing: Enviar o colgar material sobre una persona que contenga información sensible, privada o embarazosa, incluido respuestas de mensajes privados o imágenes.

7. Exclusión: Cruel expulsión de alguien de un grupo online.

Todas estas acciones, que afectan a los menores de edad, amenazan, y tienen un impacto, en el desarrollo adecuado de la vida de los niños, niñas y adolescentes; asimismo, los medios tecnológicos amplían este tipo de matonismo y acoso, extendiendo su alcance e impacto de forma tal que el daño es amplio y de largo alcance.

Los menores que sufren estas acciones pueden generar sentimientos de ansiedad, depresión, ideación suicida, estrés, miedo, baja autoestima, sentimientos de ira y frustración, sentimientos de indefensión, nerviosismo, irritabilidad, somatizaciones, trastornos del sueño y dificultades para concentrarse que afectan al rendimiento escolar; mientras que los ciber-agresores muestran falta de empatía, conducta agresiva y delictiva, superior consumo de alcohol y drogas, dependencia de las tecnologías y absentismo escolar. Garaigordobil (2011).

Estas acciones, que deben tener una atención inmediata, tanto para la víctima como para el victimario, y donde muchas de ellas ocurren en los centros educativos y son realizados por “compañeros” del mismo centro de enseñanza, implican que debe existir un abordaje normativo por medio del que la víctima pueda defenderse. Para atender estas acciones se creó la Ley N° 9404, llamada “Ley para la prevención y el establecimiento de medidas correctivas y formativas frente al acoso escolar o "bullying"”, y que indica en su artículo 1, que busca la prevención y el establecimiento de medidas correctivas y formativas ante conductas de acoso escolar o "bullying", con el fin de lograr que los niños, las niñas, los adolescentes y las personas jóvenes matriculadas en un centro educativo, en todos los ciclos y modalidades educativas previstas dentro del sistema educativo costarricense, puedan exigir que protejan su integridad física, moral, psicológica y social

de cualquier acción u omisión que vulnere derechos en el ámbito de la convivencia estudiantil. Esta normativa aplica para centros de enseñanza públicos y privados, y establece que las medidas correctivas y formativas que se establezcan ante un caso de acoso escolar deben ser, en primer término, aplicadas desde una perspectiva psicoeducativa que aborde integralmente la situación que se presenta y sobre todo que los centros educativos deben tener protocolos de abordaje para estos casos.

De igual forma, es importante indicar que esta normativa establece una obligación de los padres, las madres, las personas encargadas o de quien ejerza la guarda, crianza y educación de quienes hayan sido víctimas de violencia, hostigamiento, intimidación o de cualquier conducta que sea considerada como acoso escolar o "bullying", por parte de otro estudiante, y deben denunciar el hecho ante el personal del centro educativo; de igual forma establece que en casos en que exista un incumplimiento del personal de los centros educativos públicos, ante las previsiones de esta ley, habilita la aplicación del régimen disciplinario, esto en razón de no responder a tiempo o que no se tomen las medidas para prevenir e intervenir en los casos de acoso escolar

Asimismo, dependiendo del contexto de la situación que genere el cyberbullying, podríamos tener que aplicar el marco normativo de nuestro código penal en materia de delitos informáticos, por ejemplo, en figuras como la definida en el Artículo 230, que habla de la “Suplantación de identidad”, o el Artículo 196 sobre Violación de correspondencia o comunicaciones y el Artículo 196 bis de Violación de datos personales, o alguna otra figura que pueda configurar una acción penal, como por ejemplo delitos contra el honor, esto siempre pensando en sede penal juvenil, al estarnos refiriendo a menores de edad, mientras estos cumplan el rango de edad para ser procesados en dicha sede. Además, podría recurrirse también a la vía civil en busca del resarcimiento de daños.

Es importante que, en los casos de acoso, matonismo, tanto en el ámbito presencial como virtual, los padres, los docentes y los centros educativos no lo deben tomar a la ligera; debemos estar atentos a lo que le sucede a nuestros menores de edad, tanto en el ambiente físico como virtual. Es necesario romper la brecha digital que separa a nuestras generaciones, para poder aconsejar y atender efectivamente los problemas que se presenten con sus hijos con el uso de las tecnologías de la información. Los docentes, junto al centro educativo, deben tener un protocolo y un plan de acción efectivo para prevenir y atender las acciones de bullying como cyberbullying; de esta forma podremos evitar que estos casos avancen a situaciones aún más lamentables.

Roberto Lemaître Picado

Abogado e Ingeniero Informático

Profesor Universitario

Premio al Mérito Informático Categoría Pionero 2017 y

Abogado Destacado 2017 por la Red Iberoamericana de Derecho Informático

LA RED EDI

INFORMACIÓN QUE SUENA BIEN

WWW.ELDERECHOINFORMATICO.COM

En ocasión del IV ENCUENTRO DE DERECHO INFORMÁTICO, organizado en Agosto 2018 por la Red EDI, en Montevideo, Uruguay (Colegio de Escribanos) a cargo de la corresponsal de la RED en ese país, escribana Elisabeth Bouvier y que se lo pudo seguir tanto en modo presencial como online, se planteó la temática sobre “Tecnología y empoderamiento de la mujer”.

El encuentro reunió panelistas y auditorio de diferentes especialidades que abordaron el rol de la mujer en el desarrollo de la sociedad en relación a las TICs.

En el presente articulo se expone sobre lo presentado por la autora en el panel “Educando para la paz. Acceso y uso de las herramientas tecnológicas”, mesa compartida con la Dra. Lorena Naranjo de Ecuador y moderada por el Dr. Guillermo Zamora de Argentina.

INTRODUCCIÓN:
En términos generales referido al campo de las TIC y según UNESCO, las mujeres ocupan el 35% de personas graduadas y 21% de personas en puestos ejecutivos, y en lo que hace a puestos de liderazgo la falta de mujeres se constata aún más.

Intervienen estereotipos y role models que ya de los años 80 con el boom de los videojuegos y con la imagen a quienes iba dirigidos en las publicidades, mundo enteramente masculino, contribuyó a alejar a la mujer de la tecnología.

Esto se ve reflejado en la actualidad donde la inscripción en centros educativos de aspirantes femeninas a profesiones relacionadas con las TIC es notoriamente menor, según datos de la ONG argentina

Chicas en Tecnología, es de 15% contra un casi 85% de hombres. Es decir existe una desproporción de género en las áreas de CTIM (disciplinas académicas de Ciencia, Tecnología, Ingeniería y Matemáticas).

Porqué será que notables ejemplos femeninos en las ciencias exactas, no trascienden como sí lo hacen investigadores varones con descubrimientos similares. Tal es el caso de quien trabajara en un sistema de salto de frecuencias de comunicación o sistema de comunicaciones denominado "técnica de transmisión en el espectro ensanchado" en el que se basan todas las tecnologías inalámbricas actuales, la austríaca ingeniera en telecomunicaciones e inventora, Hedwig Eva Marie Kiesler. Fue más conocida por su nombre artístico como estrella de Hollywood Hedy Lamarr, que como artífice del sistema precursor del wifi y del Bluetooth actual.

A su vez en el área temática de la "educación", considerando la importancia de capacitar a la sociedad es imprescindible concientizar en la importancia del derecho de autodeterminación informativa y la prevalencia del derecho a la intimidad, campo no ajeno a la mujer, a quien el acceso a la tecnología en estadísticas indica la necesidad de darle un mayor apoyo por su vulnerabilidad en la falta de acceso a las mismas.

Es frecuente encontrar la inquietud en los círculos educativos planteando la pregunta, ¿Cómo promover las carreras tecnológica entre las jóvenes?.

Se estima que en el mundo hay un 12% menos de mujeres que de varones que acceden a Internet, ya sea porque viven en zonas sin conectividad, porque no pueden pagar el servicio o porque culturalmente no está habilitado que hagan uso de Internet. Se hace así una clara referencia a lo que denominamos "inclusión digital".

En la inclusión digital se pone a disposición las herramientas competentes, que permiten el acceso pleno a las aplicaciones que existen relacionado a los ámbitos bancarios, financieros, de marketing y en cuanto a la social media o plataformas de comunicación social en redes. Actualmente se cuentan numerosas herramientas disponibles a nivel digital, numerosas de ellas son gratuitas, por lo que es importante la capacitación para su uso y disposición.

Es de resaltar la importancia de la inclusión digital que le dan las agencias de Naciones Unidas como ONU Mujeres, quien propone utilizar las TIC en el empoderamiento femenino.
ONU Mujeres, aconsejó usarlas para ofrecer servicios a las víctimas de violencia de género y así fue propuesto en la Tercera Comisión de la Asamblea General de la ONU, en su 71º encuentro, por el Representante de Estonia como Estrategia 2015-2020 aplicada en su país, para mejorar los servicios en línea para víctimas de violencia.

Tan relevante es la igualdad mediante la inclusión digital de las mujeres que conforma uno de los cuatro objetivos estratégicos del Women20. El W20 es uno de los grupos de afinidad del G20, que abarca temas sobre el empoderamiento económico de la mujer. Nuclea a una red transnacional de organizaciones de mujeres, asociaciones de empresarias y think tanks cuyo objetivo es realizar un proceso de debate y votación para realizar un foro anual del que surgirán las propuestas que la sociedad civil le realice a los líderes del G20 para considerar una agenda de género sustentable.

La inclusión digital se toma en cuenta junto con la inclusión laboral, la inclusión financiera y el desarrollo rural. Esta consideración es el resultado en que se han convertido las tecnologías digitales como fuente de desarrollo económico y social.

Como la modalidad planteada en el Encuentro realizado en el Colegio de Escribanos por la Red EDI se desarrolló por sistema de preguntas, se tratará de sintetizar con sus correspondientes respuestas, como se expone en adelante:

Qué consenso subyace para focalizar sobre un tópico tan específico como el “empoderamiento de la mujer y las Tic”?

Tener en agenda y tratar este tema en los diferentes encuentros de la ONU y ser adoptado por numerosas ONG demuestran a claramente su importancia.

Justamente se refleja en los Objetivos del Milenio (ODM) y en los Objetivos de Desarrollo Sustentable (ODS) especialmente el ODS 5, en referencia a la Igualdad de Género, ODM 3, en referencia a la promoción de la igualdad de género y el empoderamiento de la mujer, ODM 8F en cuanto que el acceso a internet es un derecho del ser humano.

De qué hablamos con “brecha digital”?

Las nuevas tecnologías y especialmente internet, cual luces y sombras para un desafío, ha traído tanto ventajas como otro tipo de exclusión social, a saber: desigualdad, discriminación y analfabetismo digital.

Esto se engloba en lo que se llama la brecha digital. Por lo que si queremos acortar diferencias en la sociedad se debe tener en cuenta la vulnerabilidad en que se podría caer al no considerar la inclusión de las TIC en los grupos vulnerables de la misma (niños, ancianos, mujeres, personas con capacidades diferentes, etc.)

Porqué se dice que la digitalización está cambiando las modalidades laborales?
Con la digitalización, las formas de trabajar sin lugar a dudas están cambiando. No se puede negar el impacto de las TIC en el campo laboral donde la capacitación y acceso a ellas es fundamental. Se dejarán de usar ciertos tipo de puestos de empleos y surgirán nuevos que requerirán capacitaciones y habilidades especiales.

Valores como la cooperación, cobran mayor relevancia frente a otros tradicionalmente asociados al género masculino como la competición. Valores sociales como la fidelidad y un “fair play” toma cada vez mayor relevancia.

Es sólo una percepción que las posiciones laborables dominantes están en manos masculinas?

Una vez más las estadísticas nos muestran que la alta dirección empresarial es un mundo predominantemente masculino.
Las mujeres ocupan el 15% de los puestos en los Consejos de Administración de las empresas, según datos recopilados por Deloitte. En el 2017 según la citada empresa, en España el porcentaje llegó al 16%, y en Europa en general al 22%.

Se puede aseverar que las mujeres tienen menos accesos a las TIC?
Si tomamos en cuenta la tecnología móvil, por ejemplo los “celulares”, las mujeres tienen un menor acceso en los países de bajos y medianos ingresos, solo un 41 % tiene teléfono móvil propio, mientras que en el caso masculino el 46 % posee uno.

Según la agencia de Naciones Unidas para la Alimentación y la Agricultura, FAO, “… alrededor de dos tercios de las mujeres que viven en las subregiones de Asia Meridional, Asia Oriental y el Pacífico no tienen teléfono móvil. …”

A menudo, las mujeres del medio rural no acceden a la sanidad, la educación, trabajos dignos ni garantías sociales, por lo que tienen mayores probabilidades de caer en la pobreza y son más vulnerables a las crisis económicas y las perturbaciones climáticas.

La FAO y el PMA (Programa Mundial de Alimentos) se reunieron en marzo 2018 y pusieron énfasis en la importancia de este punto a la hora de ampliar las oportunidades de las mujeres rurales en las cadenas de valor y la creación de empresas y aumentar su acceso a la educación y la información, por lo tanto involucra la educación en el presente que se ve reflejada en las TIC.

El Director General de la FAO ha dicho "..las TIC tienen muchas posibilidades de impulsar la igualdad de género y mejorar los medios de vida rurales.." Y el Director Ejecutivo del PMA: "..Cada vez que una de esas mujeres agricultoras utiliza una aplicación del PMA para vender sus cultivos, mejora la prosperidad de su familia y de su comunidad..."

En Mozambique y Tanzania, por poner ejemplos de diferentes paises, el Fondo Internacional de Desarrollo Agrícola, el FIDA, respalda un proyecto en el que se imparte capacitación financiera y formación sobre herramientas tecnológicas a grupos de agricultores más de un 50 % de los cuales dirigidos por mujeres con el fin de ayudarles a empezar a utilizar sistemas de gestión de pagos electrónicos en lugar de efectivo.

De esta forma, los agricultores, muchos de ellos son mujeres, no solo entran a formar parte del sector financiero formal, sino que también están mejor informados de los precios de mercado con miras a mejorar su posición socio económica.

Porqué podría ser útiles las TIC en el desarrollo económico de las mujeres en específico?

Las TIC pueden ser sumamente útiles para colaborar con las oportunidades económicas de las mujeres en general pero es notorio realmente en el medio rural.

Los teléfonos móviles y los teléfonos inteligentes por ejemplo, permiten acceder a información en tiempo real sobre los precios en distintos mercados y elegir con mayor fundamento dónde y cuándo comprar y vender.

Según los estudios, cuando ganan dinero, las mujeres son más propensas que los hombres a gastarlo en alimentos para sus familias y en la educación de sus hijos, por eso la importancia de su empoderamiento.

La plataforma digital del PMA para la gestión de los beneficiarios, que cuenta con 26 millones de beneficiarios, apunta a que se haga efectivo la asistencia a la persona indicada.

Valga como ejemplo lo que ocurre en Bangladesh, entre los refugiados de Myanmar, es la mujer más mayor de cada hogar la que recibe una prestación mensual para comprar arroz, lentejas y hortalizas a los comerciantes minoristas próximos que han suscrito un contrato con el PMA. Así, las mujeres y las niñas están más seguras y tienen menos cargas en el hogar.

Una investigación del Banco Mundial reveló que las mujeres ahorran un promedio de entre el 10% y el 15% de sus ganancias, sin importar lo bajo o impredecibles que sean sus ingresos.

Las mujeres son ahorradoras responsables por naturaleza. Esto significa que, si aumentamos el acceso de las mujeres a la tecnología móvil digital, sus vidas y las de sus familias y comunidades muy probablemente mejorarán.

Es viable alguna relación entre “educación” y “seguridad de los datos”?

Además de la conectividad y la participación en el mercado laboral de las TIC, existen otras barreras más sutiles que podrían impedir que las mujeres se beneficien del acceso y el uso de Internet.
Las mujeres pueden enfrentar dificultades para acceder a las instalaciones públicas donde se encuentran los recursos de TIC (podrían tener que ver con normas sociales y culturales o con dificultades objetivas, por ejemplo, relacionadas con razones de seguridad o culturales).
Además sin la suficiente educación y capacitación en su uso, la navegación on line podría implicar para las mujeres amenazas de acoso, intimidación, vigilancia, retención ilegal de datos o delito cibernético.

Tales amenazas a menudo reflejarán los arreglos fuera de línea, incluidas las fuerzas patriarcales que se sienten incómodas con el uso de las TIC y el acceso a Internet, grupos represivos dirigidos especialmente a mujeres, ya sea por intimidación o campañas negativas, autoridades estatales que podrían retener datos de usuarios legal o ilegalmente o agresivos y discurso de odio sexista que se alimenta de los estereotipos de género tradicionales.
De acuerdo con los datos de la ONU mencionados por la Asociación para el Progreso de las Comunicaciones (APC), algunas plataformas incluso permiten la explotación sexual de mujeres y niñas y la mercantilización de los cuerpos de las mujeres, así como la trata de mujeres y menores.
En la Unión Europea, se estima que alrededor del 18% de las mujeres han sufrido alguna forma de acoso desde la adolescencia. Estas situaciones a menudo actúan como un mecanismo de disuasión para que las mujeres usen Internet.
Un estudio reciente de APC examinó las políticas de tres plataformas principales de Internet, Facebook, YouTube y Twitter con respecto a la violencia contra las mujeres en línea.
El estudio mostró algunas características comunes entre los tres casos: renuencia observada a involucrarse en cuestiones de violencia relacionadas con la tecnología antes de que se convirtieran en un asunto de relaciones públicas; falta de claridad con respecto a los procedimientos de presentación de informes y reparación; ausencia de un compromiso público con las normas de derechos humanos aparte de la libertad de expresión.
Estas plataformas de redes sociales han tomado medidas recientemente, como la interacción con grupos de partes interesadas

o la provisión de mecanismos de denuncia más sencillos.
Pero también han demostrado una postura poco clara y una falta de conciencia sobre su responsabilidad de proteger a las mujeres de la violencia en línea, mientras que han protegido sistemáticamente la libertad de expresión, a menudo a expensas de la propia ofensa de las mujeres.

¿Qué ejemplos concretos de modelos puede mencionar que estén siendo aplicables en este momento?
Como iniciativas argentinas se puede mencionar diversos ejemplos. Existe una escuela de programación dirigida a mujeres y que otorgan préstamos. Recibe apoyo de empresas como Mercado Libre , IBM, etc.

Otra ONG que promueve la programación entre adolescentes en escuelas de todo el país, es “Chicas en Tecnología”. Trabajan identificando problemas en la comunidad y con orientación de profesionales proponen soluciones. Al concluir sus estudios sigue el apoyo a través de pasantías.
Recomiendo a quien esté interesado en identificar otras organizaciones dedicadas a la inclusión digital de las mujeres, en el caso de Argentina, un articulo publicado por el periódico La Nación que habla sobre la brecha tecnológica, del dia 6 de julio del 2018.

Conclusión:

El impacto de la tecnología ya es una realidad en nuestra sociedad, donde el rol de la mujer tiene un significado especial por cuanto está comprobado que empoderar a la misma, posibilita el desarrollo.

El empoderamiento se debe dar a través de la educación y capacitación en las mismas condiciones de igualdad que se le da a los hombres.

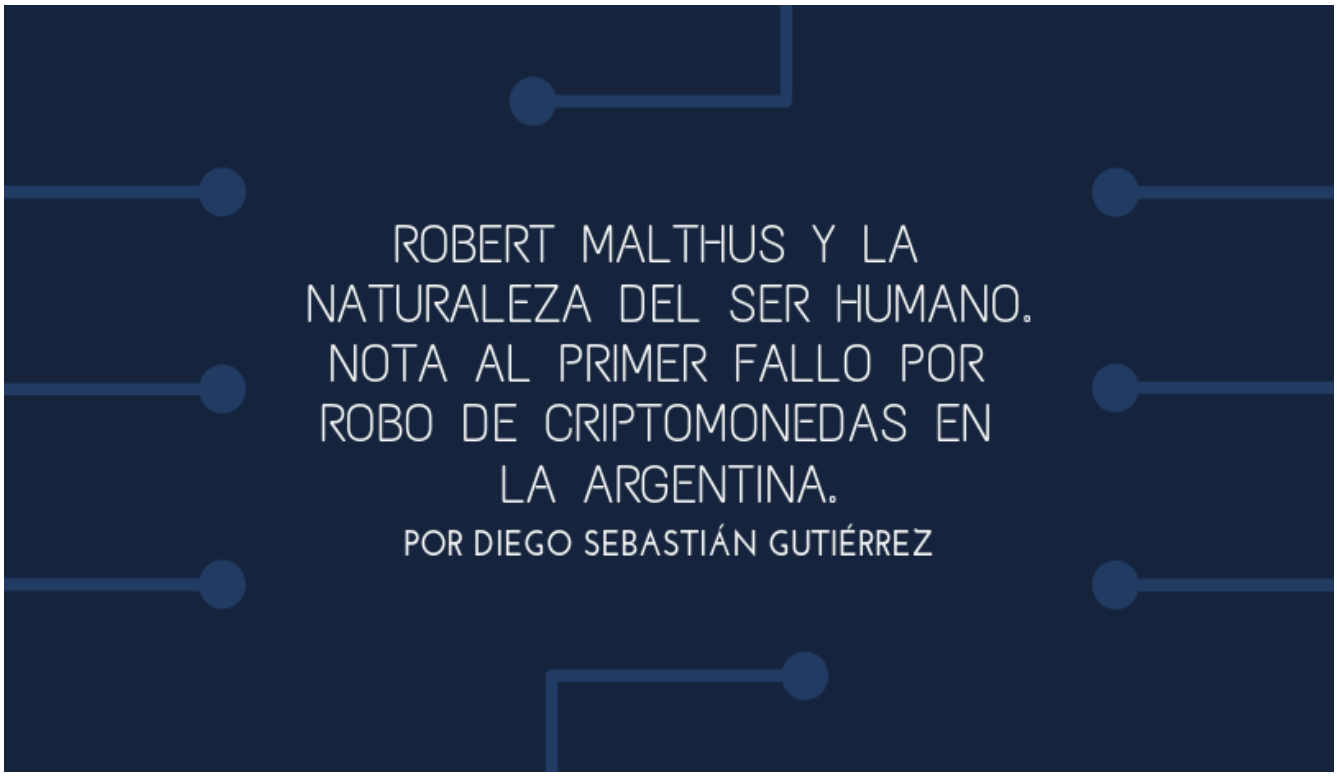
Más que un blog.
Toda la actualidad jurídica

información jurídica ágil, eficiente y relevan

aldiaargentina.microjuris.com

Llámenos (5411) 5031-9300

microjuris.co
inteligencia jurídica



Thomas Robert Malthus postuló en el siglo XVI2 que mientras el crecimiento de la población en el mundo se daba en forma geométrica, la producción de alimentos aumentaba en progresión aritmética, lo que llevaría necesariamente a una crisis alimentaria.
Parafraseando a Malthus, me gusta utilizar la metáfora de que mientras el derecho evoluciona en forma aritmética (ej.: 2,4,6,8,10,12,14,16) los avances tecnológicos se desarrollan en forma geométrica (2,4,8,16,32,64,128,264). Este desfasaje produce una brecha no solo entre el Derecho y la tecnología, sino además, entre ésta, y nuestra capacidad para comprenderla, un trípode que consideramos esencial comprender en los tiempos que corren. Esta brecha se refleja, por supuesto, en lo atinente al juzgamiento y detección de delitos informáticos.

En vistas de la referida asimetría o brecha, resulta necesario encontrar un elemento que compense las referidas asimetrías, un nivelador de diferencias. Volveremos sobre este punto mas adelante.

Dicha brecha genera el hecho de que cuando el Derecho se encuentra en un estado de avance que podríamos medir hipotéticamente en 12, la tecnología ya se encuentra en estado 512. Esta circunstancia ha dado lugar a una ya trillada dicotomía de nativos digitales y colonos o inmigrantes digitales, reservando la primera designación para aquellas personas que han nacido en medio de la tecnología, de los teléfonos celulares inteligentes y computadoras, y la última, para aquellas personas que la hemos precedido, y que nos vemos en la obligación de migrar hacia ella, al menos si no deseamos quedar excluidos.

Esa metáfora, en principio resulta cómoda, porque permite englobar y explicar en ella, una serie de capacidades y aptitudes referidas al manejo de la informática -al decir de la gente mayor- todo aquello que “los chicos hacen en la computadora”, pero al mismo tiempo, invisibiliza las diferencias que se crean entre nativos y colonos, y obviamente, entre grandes y chicos.

Walter Benjamín, cuando analizaba en los años treinta la aparición del cine y de los cambios que había producido en la sociedad, refería que una generación que nace cuando ya se encuentra implementada determinada tecnología, adquiere una forma de ver las cosas, una forma de reproducir cultura, una forma -agregaría yo- de litigar, tan distinta a los inmigrantes digitales que hace que el derecho se acompleje tanto, se contorsione tanto, que propicia la lamentable consecuencia de que la forma de litigar de quien maneja tecnología y quien no la maneja, hoy asuma contornos de dimensiones abismales.

En los tiempos que sobrevendrán a los nuestros, a nivel de procesos judiciales, los consensos necesarios entre las partes fundamentales del mismo (fiscalía-querella-fuerzas de investigación, policía científica) asumirán roles determinantes en función del éxito que busquen, y ello en línea directa con la efectividad que implementen, no solo en el fortalecimiento de su propio rol, sino de la capacidad de trabajo colaborativo y trasversal, en un mundo donde la especialidad juega su propio partido competencial en relación a las propias funciones, pero en paralelo juega otro partido, esta vez de naturaleza complementaria con otras profesiones y ramas, en la cual el conocimiento (la mirada) clínica@ se erige en la llave del mañana.

Es en este punto exacto donde la referida dicotomía (nativos digitales-colonos digitales) se vuelve paradojal, por que por un lado sirve para explicar algo, y por el otro establece una clara exclusión entre quienes asimilan el rol de la tecnología y quienes no. No pretendo con ello llegar a la conclusión de que se es -hoy en día- mejor abogado o juez asimilando conceptos elementales de tecnología y su imbricación en la sociedad, sino que hoy por hoy no se puede ejercer el derecho ni la magistratura sin conocer tales aspectos.

En la provincia del Chaco, con la reciente sanción del Código Procesal Civil y Comercial que entró en vigencia el 1/8/2017 (siendo la primer provincia en adecuarlo al código de fondo nacional) hemos tomado debida nota de esta evolución. Si bien es necesario decirlo, nuestro poder judicial ya hace años viene, a través de la dirección de tecnologías, implementando el expediente en línea, la notificación electrónica, la firma digital, pero la circunstancia de que el Derecho recién incorpore normativamente algo conocido y probado exitosamente hace tiempo, demuestra a las claras las consecuencias de la brecha de la cual hablaba mas arriba.

Es además importante mencionar que entre derecho y tecnología existe una relación que no es directa, que se encuentra mediada por el desarrollo. Todos los países que se han desarrollado, manifiestan instituciones en Derecho fuerte, como el derecho de propiedad, libertad, nivel de desarrollo constitucional, entre otros. Por su parte, la tecnología ha aportado lo suyo en este triunvirato que conforma junto al derecho y al desarrollo.

Si observamos que desde el año cero hasta el año 1800 la mayoría de las mediciones

indican que la humanidad tal cual la conocemos, se ha desarrollado un cincuenta porciento, y en casi los últimos doscientos veinte años de vida, hemos crecido mas del mil porciento, con lo cual, la vertiginosidad del desarrollo queda en clara evidencia.
Creo que las fronteras en el mundo, con la intervención de la tecnología se están desdibujando y en el derecho mucho mas aún.

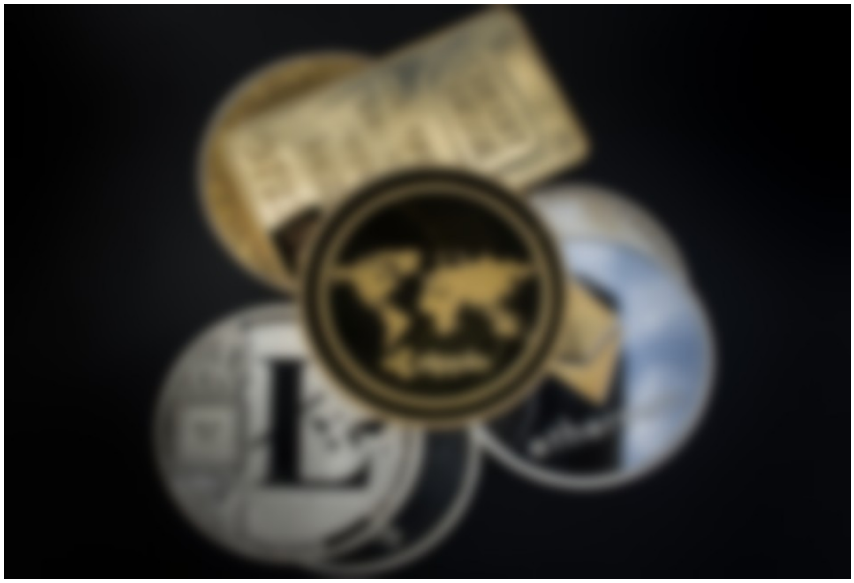
En cuanto a la relación entre derecho y tecnología, alguna vez leí a Rohan Silva, afirmar que mientras la revolución industrial sustituyó al músculo del ser humano, la revolución tecnológica -en la cual estamos inmersos- sustituirá al cerebro del hombre. Como consecuencia directa de ello, muchas personas perdieron su trabajo, perteneciendo a estratos menos capacitados de la sociedad.

En los días que corren, afirma Silva, paralelamente estamos viviendo una revolución tecnológica, que de manera similar a la industrial va a generar la pérdida de trabajo a muchas personas; pero esta vez comprometerá a quienes pongan, al servicio del trabajo, no al esfuerzo físico, sino la materia gris. Y en eso, la justicia, y los operadores del derecho estamos mas expuestos, mas involucrados.

Creo que es nuestro deber ir disminuyendo cada vez más las diferencias, con apoyo en las herramientas tecnológicas. Dicen que el derecho actúa como un gran lienzo, elaborado (por lo holístico de su contenido) con el mejor género que podamos imaginar. Pero ese mismo mantel o lienzo, cuanto mas noble, colocado sobre una superficie irregular, copia necesariamente las irregularidades que solapa.

Entonces, es nuestro deber ir disminuyendo las mencionadas irregularidades o diferencias, afianzando el Derecho, para ser cada vez mas iguales en relación al mismo, o mas bien, para ir creando cada vez mayor nivel de igualdad de oportunidades, premisa sin la cual, el Derecho carece de sustento, al menos si pretende asumir las características del estado social, constitucional y democrático de Derecho.

Direccionándonos hacia el fallo bajo comentario, diremos resumidamente que se trató de una investigación iniciada por la Oficina de la Fiscalía del Distrito Medio de Florida -Orlando- de los Estados Unidos, y de la cual tomó participación Interpol, en el cual la Sala Tercera de la Cámara Criminal y

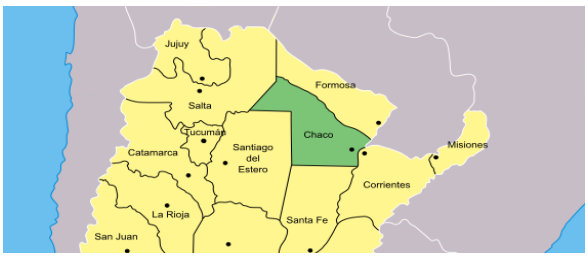


Correccional de Resistencia -Chaco- ha dictado una sentencia que se erige en la primera de todo el país sobre robo de criptomonedas o monedas virtuales, en este caso, denominadas Ethereums.

La empresa damnificada, de capitales radicados en Orlando, sufrió la sustracción de su billetera maestra, de mas de 619 Ethereums (ETH), bajo perfiles encubiertos y hackeo de su privacidad. Al momento del hecho, la referida moneda cotizaba en alrededor de 650 dólares, con lo cual podemos calcular que no se trataba de una suma de menor cuantía. A pesar de haber encubierto todas las conexiones, alguna IP (internet Protocol) argentina quedó al descubierto, lo que justificó la toma de razón y la radicación de competencia.3

Lo novedoso del fallo no es solamente el haber sido pionera a nivel país, sino además que en la misma no se realizó plenario o debate, sino que la sentencia ha sido dictada como consecuencia directa de un proceso de juicio abreviado. Siendo ello así, se nos plantea el interrogante respecto que, mas allá de la ausencia de debate y producción elaborada de pruebas, debieron haber existido elementos objetivos suficientemente acreditados para que subjetivamente el imputado de autos decidiera firmar el proceso de juicio abreviado. Explicaremos esto.

En materia política criminal, la provincia del Chaco, suele aplicar penas que se acercan a los umbrales mínimos de la escala establecida para el delito bajo tratamiento. Ello se repite en el concierto nacional.



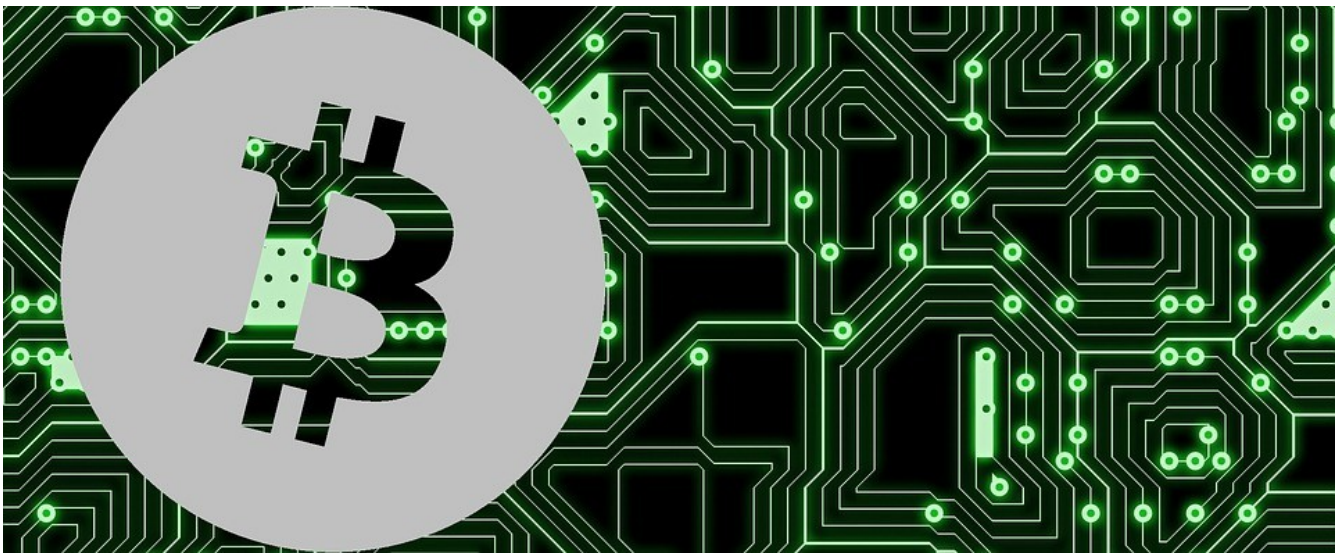
El instituto del juicio abreviado, regulado en el Código procesal penal provincial, establece un procedimiento en el cual el Fiscal de Investigaciones, al momento de dictar la requisitoria de elevación a Juicio, puede solicitar al juez de la causa su aplicación con la conformidad (como requisito de procedencia) del imputado y los abogados defensores. Se erige como un acuerdo entre acusado y fiscal, en virtud del cual el primero acepta la comisión del delito, y el segundo acepta imponer el mínimo de la pena, renunciando a la realización del proceso. El acuerdo debe contener la conformidad respecto a los hechos por los que se acusa, la calificación legal propuesta y la pena pactada. De todo ello, el Tribunal debe correr vista a la querella, cuya opinión solo resulta vinculante en el caso que la pena establecida para el delito supere los ocho años de prisión en abstracto.

Ergo, teniendo en cuenta los bajos montos de pena aplicados en concreto (al dictarse sentencia, y después de un largo proceso) los imputados raramente aceptan acudir al instituto de referencia, pues de aprobarse el acuerdo de juicio abreviado, el mismo seria de cumplimiento efectivo, lo que se acercaría bastante a una sentencia condenatoria, renunciando a la posibilidad estratégica de que no se logre acreditar suficientemente el delito imputado, o se detecten algunas nulidades en el procedimiento que permitan solicitar prescripción o insubsistencia de la acción penal.

La falta de plenario en el caso que nos ocupa, impide inicialmente poder dar respuestas empíricas de lo ocurrido para orientar a la defensa y al imputado a firmar un juicio abreviado (aún considerando su inconveniencia)

Sin embargo, ello no nos impide afirmar que desde la óptica del imputado (hoy

condenado), debieron existir ciertas condiciones objetivas que determinaron que el mismo recurra al instituto del juicio abreviado, aún sabiendo que en nuestra provincia, realizado el plenario y con una sentencia condenatoria, las sentencias suelen acercarse bastante a los mínimos legales.



En efecto, la base probatoria de cargo colectada en la investigación penal preparatoria (IPP), debe haber sido muy contundente para que el imputado acepte suscribir el proceso abreviado.

Es por ello que, siendo la primer condena a nivel nacional por robo de criptomonedas, se presente éste como un espacio interesante para analizar la prueba y los hechos ocurridos hasta el auto de requerimiento de elevación a juicio, que nos permitan arribar a alguna conclusión en torno al tema de la presente nota.

La damnificada, es una empresa radicada en Orlando, EUA, que funciona para el trading (intercambio) de monedas sean éstas convencionales, de uso legal, o virtuales.
El Ethereum, como otras monedas virtuales, funcionan bajo es sistema blockchain (cadena de bloques) el cual funciona -dicho de modo figurado- como un libro contable, permitiendo a quienes tengan acceso, auditar el camino que ha recorrido la transferencia de dichas monedas, y determinar a cual billetera virtual han sido enviadas.

La empresa damnificada en el hecho bajo comentario, posee servicio externo de fiscalización y monitoreo, que mediante un canon, permite obtener en tiempo real o mediante filmación, todos los movimientos de los usuarios en la plataforma de la empresa.
Una de las características principales del blockchain es que puede ser consultado por cualquier persona con acceso a internet, pudiendo auditar las billeteras virtuales, y determinar cuándo una persona -poseedora de una determinada billetera- envía las monedas a otra persona, y si quien las recibe realiza alguna acción con ellas.

Sin embargo, uno de los pilares para determinar la autoría de la acción delictiva en el caso bajo exámen, ha sido el de los indicios y presunciones probatorios.
Veamos.

Existe un procedimiento que las regulaciones financieras de numerosa cantidad de países -fundamentalmente Estados Unidos- exigen a empresas, para evitar el lavado de activos financieros de procedencia ilegítima o similares. Esta práctica se denomina "know your customer" (KYC) -conoce a tu cliente-. práctica que incluso los bancos oficiales de todos los países que funcionan con monedas físicas utilizan. Esta práctica permite tanto el control como la auditoría de clientes y de terceros que pretenden serlo.

Al crear una nueva cuenta, una persona humana (según la expresión adoptada por el nuevo Código Civil y Comercial de la Nación) utiliza su nombre, correo electrónico y una contraseña de su selección. Iniciado el proceso de logueo, el usuario recibe un correo electrónico mediante el cual debe validar su cuenta de email o correo electrónico. El cliente no puede acceder a comprar, vender ni transferir criptomonedas sin completar ese paso.

Allí se accede a la sección Mi Perfil o Configuración, donde la persona completa los datos personales, y, a modo de resabio de tiempos pretéritos que precedieron a la digitalización de las operaciones financieras, para validar físicamente al solicitante, se requiere el escaneo de su pasaporte y una selfie, sosteniendo su pasaporte en una mano y en la otra un papel donde el usuario debe escribir con su propia letra "Para el Uso exclusivo de -nombre de la empresa-" en inglés: "Only for trading in xxxxx" u "Only for use by xxxxxx".

Esos datos se los cruza con la lista OFAC "Office of Foreign Assets Control" (Oficina de Control de Activos Extranjeros), que permite verificar si el usuario ha actuado ilícitamente con lavado de activos o financiando terrorismo. Estas medidas permiten al oficial de cumplimiento determinar -al igual que cualquier entidad crediticia- si el perfil examinado cumple con los estándares requeridos.

Una vez que el usuario está validado por el sistema, puede obtener criptomonedas recibiendo una transferencia de terceros, realizar una transferencia bancaria desde su propio banco en cualquier lugar del mundo que le permita realizar una "transferencia por cable" (de internet o de datos) -wire transfer- a la cuenta de la empresa seleccionada, o efectuar la compra mediante alguna tarjeta de crédito.

Contando con criptomonedas en su billetera digital, puede negociarlas libremente. Ahora bien, para transferir monedas hacia algún comercio o persona, a fin de adquirir un servicio o producto, debe inscribir -en su propia billetera- como “favorito” dentro del sistema de la empresa, la dirección o número de cuenta de esta persona o entidad con la cual haya conveniado la transacción; es un procedimiento similar a aquel en el cual se agrega una cuenta beneficiaria para realizar transferencias por el sistema home banking. Una vez registrado el beneficiario, le llegará un mail que el usuario debe validar, aceptando la incorporación como beneficiario. A partir de allí puede enviarle las criptomonedas que desee.

El mundo hoy transacciona con habitualidad de esta manera, y de forma legítima, debiendo incluso facturar de acuerdo a la normativa local, los servicios o productos vendidos, como si lo hubieran sido bajo moneda de curso legal.

Veremos seguidamente, de las investigaciones realizadas por la querella, éste ha sido un punto de quiebre para

determinar la ligazón entre varias cuentas operadas por el mismo imputado.

En diciembre del año 2017, el imputado se conectó con la plataforma de la empresa bajo cuenta falsa que denominaremos “D”. Este perfil o cuenta principal, mediante técnicas de hackeo y violación del sistema referido, logró extraer monedas del saldo operativo de la empresa y enviarlas a billeteras externas la plataforma de la misma. Esta cuenta se conectó desde un acceso VPN (virtual private network) con la dirección IP xxx.xx.99.20, proveniente del Reino Unido.

Toda IP (Internet Protocol -Protocolo de Internet-) se compone de cuatro combinaciones de números, separadas por puntos. Por ejemplo 187.25.14.190. Este número es un identificador único en el mundo, en conjunto con la hora y con la fecha puede ser utilizado para determinar el lugar de origen de una conexión, o al menos, una aproximación.

En la causa, existió una primer billetera beneficiaria, que denominaremos Nº 1, terminada en "b9fD" donde hizo múltiples transferencias hasta completar un monto de 470 monedas aproximadamente.

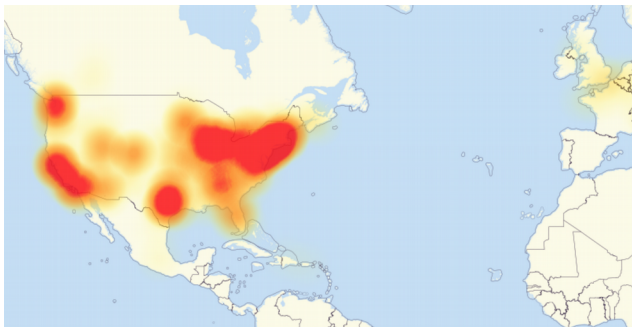
Posteriormente transfirió 26 monedas desde la billetera 1 a la billetera número 5 terminada en "97b3". Lo llamativo es que la primera de estas billeteras, se encontraba registrada dentro de los favoritos de la cuenta oficial del imputado en autos, al que referiremos como HMP, por las siglas de su nombre real.

Cabe aquí la pregunta. Porqué el imputado en autos poseía oficial y legalmente una billetera digital entre sus favoritos, que recibía monedas de lo que denominamos billetera número 1, la cual recibió 470 monedas el día del ataque, y la billetera número 5 recibió de la billetera 1, 26 monedas un día después del ataque?.

Es allí donde la investigación procedió a vincular los múltiples inicios de sesión con la misma IP que la cuenta que utilizó el atacante. Aquí ya no analizaremos las billeteras, sino mas bien los perfiles y las IP utilizadas.
El mismo día del ataque, y luego de la extracción de las 470 criptomonedas de la plataforma de la empresa, un usuario con nombre que estipularemos en “A” se registró en la plataforma de la empresa utilizando la misma dirección IP del Reino Unido la cual identificamos anteriormente con la numeración xxx.xx.99.20. Como se puede percibir, ese usuario “A” inició sesión el día del ataque informático desde la misma dirección IP del usuario “D”, desde Reino Unido.

Al día siguiente, la cuenta A inició sesión con una IP de Suiza, identificada como xx.xx.138.66., pretendiendo replicar el ataque realizado el día anterior, utilizando los mismos mecanismos. Al no poder realizarlo satisfactoriamente, intentó probar una variante, utilizando una funcionalidad legal dentro de la empresa, denominada Solicitud o Request, consistente en que una billetera solicita a otra que le envíe monedas. El request o requerimiento por 500 Ethereums fue realizado desde la cuenta A, hacia la cuenta que había recibido las 470 monedas.

Al finalizar el Request el usuario cerró sesión de la cuenta de A, para luego iniciar sesión en la cuenta oficial del imputado, pero con la dirección IP de Suiza. Efectivamente, la misma que utilizó la cuenta A para solicitar (a la cuenta D) la transferencia de 500 monedas ilícitamente sustraídas con antelación.



Como podemos ver, el usuario detrás de la cuenta “D” atacó desde la IP de Reino Unido y transfirió 470 ETH a la Billetera terminada en "b9fD" (billetera 1). Luego esta última billetera envió 25 ETH a la billetera o cartera digital "97b3" (billetera 5) que fue validada por el imputado vía email el día siguiente al del ataque. La cuenta de A inició sesión el día anterior con la IP de Reino Unido (la misma que usó el perfil D) y al día siguiente el perfil A y el perfil oficial del imputado iniciaron sesión con la IP de Suiza, vinculándose así las tres cuentas, dado que físicamente resulta imposible que una persona esté en tres lugares distintos, por lo que se presume que utilizó una VPN para así engañar la ubicación real desde donde se encontraba conectado.

Independientemente de que el presente ha sido escrito para una revista especializada, debemos aquí, en lenguaje coloquial, explicar que una VPN (Virtual Private Network) funciona como un túnel que disfraza la identidad desde la cual proviene la comunicación (IP) y que la red TOR (The Onion Router) es un sistema que enmascara la IP, utilizando para ello varios servidores activos en el mundo, que funcionaría -figurativamente- como red de encubrimiento.

También debemos poner de relieve que ello no hubiera ocurrido si entre el cierre de un perfil y la apertura de otro, hubiera el imputado interrumpido la conexión, dado que (sea por TOR o por VPN) la IP hubiera cambiado.
Aquí se torna evidente lo que referíamos respecto de la brecha malthusiana entre el avance de la tecnología y nuestra capacidad de comprender el desarrollo de la misma. Evidentemente, no existe TOR ni VPN que le quite al ser humano su condición de tal.

Podemos, en fin, afirmar que los roles de cada uno de los actores vinculados en el descubrimiento y condena de la causa, han actuado fortaleciendo el rol que a cada uno les tocaba cumplir: la fiscalía actuante, la División de Delitos Tecnológicos de la policía de la provincia del Chaco, con la apoyatura técnica de la querella hemos puesto en juegos los elementos necesarios para lograr esta primera condena nacional.
Cada una de las potestades, funciones o roles de los actores involucrados -per se- podrían claramente ser considerados

insuficientes para determinar el resultado final.
Léase: una adecuada detección del delito, jamás habría rendido frutos sin una preocupación fuerte de la justicia en la persecución penal, como tampoco si no se hubiera librado la orden de allanamiento y detención con la inmediatez que ello requería, u ordenado las periciales en los elementos secuestrados.

Ello ha generado que todas las funciones comprometidas en la causa hayan trenzado sus fuerzas, generando así una nueva composición de capacidades, que nos permite postular el principio de que ante el inminente avance de la tecnología de modos nunca antes vistos, solo logrando un trabajo coordinado y fortalecido entre todas las partes vinculadas con la investigación y el juzgamiento del delito informático, podremos obtener resultados eficientes.

Este quizás sea el elemento que referíamos inicialmente, el que nos permita equilibrar la brecha existente entre el delito informático y su investigación: en un futuro no muy lejano, solo el trabajo colaborativo podrá compensar una brecha cada vez mas evidente.

AUTOR: DR DIEGO SEBASTIAN GUTIERREZ
El autor es abogado, egresado de la UNNE. Ha dirigido la querella en la primer causa en el país por robo de criptomonedas con fallo firme. Es profesor en la UTN-FRRe, donde imparte clases de Derecho e informática desde el año 2011. Ha sido creador de la plataforma y jornadas LegalByte. Es presidente del Colegio de Abogados y Procuradores de Resistencia, presidente y fundador de la Federación de Colegios de Abogados del Chaco (FeCACh). Fue Secretario Legal y Técnico de la Municipalidad de Resistencia. Es maestrando en Derecho Administrativo de la Universidad Austral de Buenos Aires

Estamos donde estas vos

ElDerechoInformatico

Centro de Información y Formación

La proliferación de la Internet se condice con el reconocimiento -de gran parte- de la Comunidad Internacional del derecho a "acceder" a ella, pero ya no como una simple prerrogativa, sino como Derecho Humano. Que vendría a ser el derecho que posee toda persona de acceder a la Internet con el fin de ejercer la libertad de expresión, de opinión y otros Derechos Humanos fundamentales que conforman la democracia.

La "Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información"1 (Ginebra, 2003) ya establecía como objetivo para las naciones aprovechar el potencial de las tecnologías de la información para promover los objetivos de desarrollo, en particular, erradicar la pobreza extrema y lograr la educación primaria universal, bajo el criterio de comprender a las tecnologías de la comunicación como base necesaria para cualquier democracia,

al ser propicias para fomentar la participación y el libre desarrollo de la personalidad.
En este sentido, el Consejo de Derechos Humanos de la Organización de las Naciones Unidades adoptó, siguiendo al informe (del 16 de Mayo de 2011) relativo a la libertad de expresión en Internet del Relator Especial de la Comisión de Derechos Humanos, Frank La Rue, la resolución A/HRC/20/L.13 (del 29 de junio de 2012) con la que se "Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos", además se "Exhorta a los Estados a que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países" y "Decide seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos ".
Así también existen diversos precedentes internacionales que reconocen el derecho al acceso a las tecnologías de la información -y a la banda ancha-, ya sea a nivel constitucional, como es el caso de Ecuador2; a nivel legal, como en Brasil3; o jurisprudencial, como en Costa Rica4.
Incluso en nuestro país, la reciente ley "Argentina Digital" (N° 27.078) declara "de interés público el desarrollo de las Tecnologías de la Información y las Comunicaciones, las Telecomunicaciones, y sus recursos asociados, estableciendo y garantizando la completa neutralidad de las redes. Su objeto es posibilitar el acceso de la totalidad de los habitantes de la República (...). Esta norma es de orden público (...). Las disposiciones de la presente ley tienen como finalidad garantizar el derecho humano a las comunicaciones y a las telecomunicaciones, reconocer a las Tecnologías de la Información y las Comunicaciones (TIC) como un factor preponderante en la independencia tecnológica y productiva (...)".
Así, el reconocimiento generalizado del acceso a Internet como Derecho Humano pareciera ser un beneficio para el hombre común, ahora más libre, ahora más democrático. Sin embargo, luego de diversas experiencias, resulta lógico preguntarnos si realmente somos los benefactores del acceso “garantizado" a la Web. Porque si bien la libertad de expresión es la piedra fundamental de la democracia, como se sostiene en cada uno de los documentos citados, también lo son las demás libertades individuales, sin las cuales tampoco habría expresión, prensa, ni nada parecido. Es que, si el fundamento de la libertad de expresión -y el derecho a la información- es la dignidad de la persona, no se puede aceptar que esa dignidad se vea

perjudicada por el mismo ejercicio de dichas libertades.
En la actualidad, Google (casi exclusivamente5) facilita el ejercicio de estos derechos fundamentales al recibir 2.4 millones de consultas por minuto6. De hecho, la Web se divide prácticamente entre lo que el “buscador” ve y lo que no7. En apenas un par de décadas, la compañía -renombrada Alphabet en 2015- ha logrado que su producto estrella se convierta en el ojo de Internet, en la puerta de entrada. “Googlear” se ha vuelto sinónimo de buscar en la Red, y no lo vimos venir.
Los países en general no han podido -o sabido- protegerse a tiempo, y muchos de ellos ahora se encuentran en la disyuntiva de tener que elegir entre ceder soberanía ante la posición dominante de Google y el riesgo de limitar las libertades de sus ciudadanos en Internet. Y es en este embrollo, que la Unión Europea (evidentemente contraria a los intereses estadounidenses) pareciera ser el caballero blanco de la contienda al tomar una postura crítica respecto del statu quo de Internet y posicionarse abiertamente en contra de las tecnológicas, sus políticas de uso y la recolección indiscriminada de datos, impulsando medidas como el reciente Reglamento General de Protección de Datos Personales.
Es que, con cada búsqueda, con cada click, la gran “G” nos conoce un poco más, nos estudia y nos procesa. Y no le dábamos importancia porque -en muchos ámbitos- se hizo imprescindible y hasta simplificó en cierta manera nuestra vida. Pero ahora, que tomamos conciencia, puede que ya sepa demasiado acerca de nuestros hábitos, gustos y costumbres, de nuestras familias, lugares y relaciones. De hecho, puede que ya sea tarde para reaccionar.
Evgeny Morozov, reconocido tecnólogo, analiza a los asistentes virtuales que poseemos actualmente en los teléfonos "inteligentes" y refuta la "Regla de Varian"8 diciendo que "Cuando uno contrata a alguien como asistente personal, uno paga a esa persona por los servicios prestados y ahí se acaba la cosa (...) con los asistentes virtuales: uno hace entrega de sus datos -igual que haría entrega de su dinero en efectivo- para que Google le provea de ese servicio (...) [Pero no] esperamos que nuestros asistentes personales se marchen con una copia de todas nuestras cartas y archivos para hacer dinero con ellos (...) [Sin embargo] esa es la única razón de que ellos existan. De hecho, se nos está engañando (...) cuando esos datos son después utilizados para personalizar y estructurar nuestro mundo de una manera que no es ni transparente ni deseable. Esta segunda característica de los datos, capaz de moldear la vida, como una mera unidad de intercambio (...) convierte a los datos en un instrumento de dominación (...) Nada por el estilo les sucede a los ricos [que pagan por los servicios] (...) el amo está dominando a quien le sirve, y no al revés, como es el caso con Google Now y los pobres (...) son los pobres los verdaderos “asistentes virtuales” de Google, al ayudarle a amasar los datos"9.
Y aquí continuamos, ¿acaso no podemos resistir la tacaña tentación de un servicio "gratuito"? Porque el costo no importa, y la estrategia de Google es evidente: estar en todos lados. Hace tiempo que dejó de ser sólo un buscador de Internet. Debemos mirar ya a la empresa como una conglomeración de diversos productos10 que, individualmente, son impactantes. AdWords (publicidad), Android (software), Gmail (e-mails), YouTube (video streaming) y Blogger (blogs) son apenas los más visibles. Pero también encontramos los mapas, el traductor y Google+, la red social, entre tantos otros. El éxito de Google estiva justamente en llegar a los más profundos rincones de la vida humana, mediante

servicios -en su mayoría gratuitos- que prometen comodidad y productividad, con la libertad de acceso a la información como bandera.
Así, luego de Search y AdWords, llegaron Trends y Analitycs (estadísticas de búsqueda y publicidad), luego de Android llegaron Google Play (consumo a través del teléfono móvil), Drive (almacenamiento en "la nube"), Chrome (explorador de Internet) y Reader (lector de RSS). Google nos propone hacer todo a través de su plataforma, y para ella además vende hardware, como teléfonos móviles (Nexus), televisores inteligentes (Chomecast) y computadoras personales (Chromebooks), cargado con sistemas operativos propios y específicos. Incluso ofrece Android "libre" a diversos fabricantes, como Samsung, LG y Motorola, para así abarcar diversos gustos y bolsillos. Google lo ha logrado: es omnipresente.
Es más, a futuro la empresa pretende participar en el negocio de las telecomunicaciones mediante Google Fiber (fibra óptica y telefonía móvil) y llevar Internet a las zonas más alejadas con SpaceX (satélites de bajo costo) y Loon (globos meteorológicos). Prevé participar a su vez en medicina a través de proyectos como Calicó (investiga cómo retrasar el envejecimiento) y Liftware (ayuda a enfermos con el Mal de Parkinson) e impulsa el desarrollo de su propio vehículo autónomo (Google Car). Incluso colabora con la NASA (Xprize, exploración espacial) y apoya el acceso a energía limpia mediante drones o cometas (Makani Power).
Y hay mucho más. Porque Google incluso se imagina gobernador de una ciudad inteligente. Con el proyecto "Sidewalk Labs" promete ciudades gestionadas por algoritmos que, en tiempo real y tomando como referencia al ciudadano y sus datos -aunque sin su participación activa-, decide "lo mejor para todos". Vendría a ser algo así como la ejecución del Big Data mediante la concreción algorítmica de una supuesta administración gubernamental perfecta. Tan solo imaginar una plataforma que gestione desde el tráfico y el transporte hasta el consumo energético y el precio de los alquileres suena a utopía, pero si el medio será la información que "aporte" el ciudadano de a pie volvemos al origen: privacidad y datos personales a cambio de servicios gratuitos y acceso irrestricto a la Red.
Porque al final del día todo se reduce a los datos, a lo que Google sabe de nosotros según lo que le hicimos saber. Porque por este camino llegará el día en que efectivamente nos ayude a bajar costos, optimizar consumos y aumentar productividad, pero a costa de la libertad del usuario, quien gastará lo que le dejen, consumirá lo que le muestren y producirá lo que le requieran. Un mundo hiper-automatizado, y dominado -como dice Morozov-, en el que sólo nos quede rogarle a Google: "Don´t be evil"11.

EL AUTOR: Abogado (UCA). Socio en MCI Abogados. Asesor Jurídico en la Administración Gubernamental de Ingresos Públicos (AGIP) de la Ciudad de Buenos Aires. Dedicado, en el ejercicio libre de la profesión, a las nuevas tecnologías. Redactor en iOSMac.es. Investigador adscripto del CONICET en cuestiones de derecho informático. Especialista en Derecho de la Alta Tecnología (UCA), y en Abogacía Estatal, Local y Federal (PGCABA).

Dra Bárbara Peñaloza

En los tiempos que corren, en los que las Redes Sociales se han convertido en un medio de comunicación fundamental para el ejercicio de la libertad de expresión y el derecho a la información, pero también y como contrapartida, en una herramienta para canalizar el odio y la violencia, en un abierto e impune avasallamiento a derechos personalísimos como la intimidad, la reputación, el honor, la imagen y la identidad digital y, por consiguiente, al derecho humano a la dignidad de las personas humanas, se hace indispensable articular mecanismos que propendan a la protección de la dignidad digital. Es en este contexto que adquiere relevancia un artículo de nuestro Código Civil y Comercial, que puede llegar a pasar desapercibido, pero que hoy en día es una herramienta fundamental para la protección de la dignidad digital de las personas que son partes en un expediente de familia, ya sea por sí mismas o por formar parte de una familia que ha debido acudir a los tribunales para dirimir algún conflicto, como por ejemplo, los hijos de un matrimonio en proceso de divorcio o en proceso de alimentos.

Es que en los tiempos que corren muchos padres, en el afán de hacer justicia por mano

propia desde lo que ellos piensan que es "justo", utilizan las constancias de los expedientes de familia en los que son partes para difamar a la contraparte, que otrora fuera su pareja. Esta práctica implica un avasallamiento no sólo a la dignidad digital de adultos, sino
también de niños, niñas y adolescentes que se ven en el medio de una disputa judicial y ahora también digital.

Por ello el artículo 708 del Código Civil y Comercial de la Nación es de una importancia mayúscula en la era de las redes sociales, al determinar el acceso limitado al expediente en los procesos de familia, es decir que sólo las partes, sus representantes y letrados y los auxiliares designados en el proceso pueden acceder al mismo.

Sin embargo, para una aplicación eficaz de este artículo de fondo sería necesario que las leyes de forma reglamenten esta norma.

Atento que nos encontramos en un proceso de reforma de la Ley Procesal de Familia en la provincia de Mendoza, es interesante analizar cómo aplica el Proyecto de Ley este artículo.

Así, el artículo 11 del mismo, fija el acceso limitado al expediente, reproduciendo el artículo 708 del CCyCom sin añadir mucho más. Ello, como la realidad social y digital lo demuestran, no es suficiente para persuadir a las partes del proceso a no difundir las constancias de los expedientes de familia.

De hecho hoy en día pueden leerse las fojas de un expediente en el perfil de Facebook de una mamá de una nena de 8 años, que decide compartir habitualmente y de manera pública partes del expediente en el que se ventilan los alimentos que le reclama a su padre, sin cubrir el nombre y documento de identidad de la nena, junto a las denuncias que ha realizado por supuesta violencia de género.

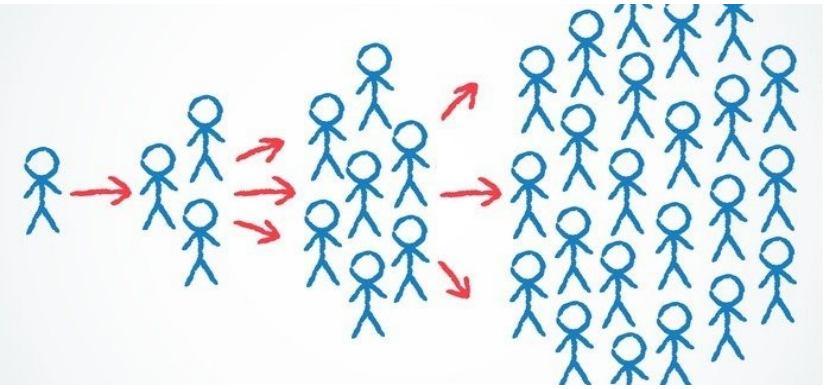
Con ese accionar no sólo perjudica la intimidad y el honor del padre de la nena y de los otros hijos adolescentes de este, si no que también viola la dignidad digital de su propia hija de 8 años, puesto que al no ocultar la identidad de la misma, la expone en la red social y expone la problemática por la que pasa ella y su familia.

El daño provocado a la dignidad digital se potencia por la posibilidad de "viralización" que permite el uso de redes sociales, por la cual una publicación sin filtro de 1 privacidad puede llegar a un número indeterminado de usuarios, quienes a su vez pueden compartir y comentar esta publicación en la misma u otras redes sociales, multiplicando así los destinatarios. Cuando se produce la viralización de una publicación, y esta sale de la esfera íntima de las personas involucradas en la misma, se pierde la empatía por estas.

Quienes comentan la publicación viralizada desconocen la historia de la familia y no saben quiénes son los involucrados en el conflicto, por lo que los insultos y mensajes difamatorios y violentos se recrudecen, provocando un daño incalculable.

Por ello, y desde una perspectiva de prevención más que de resarcimiento, una manera de proteger la intimidad de la familia y la dignidad digital de los miembros que la componen, es la efectivización, a través de la norma de forma del procedimiento de familia, del mencionado artículo 708 del CCyCom.

1 La viralización o “Efecto viral“ es inherente a las redes sociales, que permiten, dada la cantidad de usuarios que cada una de ellas tiene, que un contenido compartido por un usuario pueda propagarse en la Red rápidamente y de modo exponencial, pudiendo ese contenido llegar a un sinnúmero de personas en muy poco tiempo.



Para ello, se hace necesario que el legislador aprehenda que en la realidad digital que nos circunde, el hecho de restringir el acceso al expediente a las partes, sus letrados y peritos no es suficiente, pues en ocasiones son las mismas partes, con acceso permitido, las que facilitan a través de sus redes sociales el acceso ilimitado al expediente que se ha intentado resguardar mediante el Art. 708.

Si a ello le sumamos que muchos de esos expedientes se ven abultados de denuncias falsas e intentos de entorpecer la tutela judicial efectiva de los derechos e intereses en juego, no puede admitirse que alguna de las partes utilice las actuaciones judiciales para mortificar a la contraparte, infligir una presión social en pos de sus intereses y colateralmente provocar la exposición de personas menores de edad, colocándolas en una situación de vulnerabilidad mayor que la que de por sí padecen.

Por todo lo expuesto, es que humildemente quien escribe estas líneas propone que el legislador advierta esta problemática, que ha llegado para quedarse de la mano del uso de las TIC´S y que implica el uso de un expediente judicial de familia para hostigar y

2 difamar a una de las partes del mismo, provocando colateralmente la exposición de las personas menores de edad que necesariamente se ven enredadas en el conflicto familiar. Tales conductas, completamente reñidas con todo el andamiaje normativo protectorio de la dignidad humana, no pueden ser toleradas.

Por ello se hace necesario un aggiornamento procesal, acorde a los tiempos que vivimos. Así las cosas y aprovechando la reforma, la futura ley procesal de familia mendocina debería prevenir estas conductas ilícitas y, asimismo, prever un mecanismo de tutela preventiva expedita para evitar el daño incalculable que una “viralización” de un expediente de

familia puede provocar en la contraparte y en los niños, niñas y adolescentes que forman parte del conflicto.

Así las cosas, es esta una buena oportunidad de prever una sanción para quienes extraigan del ámbito privado las actuaciones en los procesos de familia, consignando expresamente la prohibición de difundir las mismas mediante cualquier medio tecnológico, ya sea mediante mensajería privada, redes sociales, blogs, grupos, foros o cualquier otro medio de comunicación on line, de manera de persuadir efectivamente estas prácticas

2 Tecnologías de la Información y Comunicación digitales ilícitas que comenzamos a advertir algunos operadores del Derecho.

Asimismo, se hace necesario articular un mecanismo de protección inmediata a la intimidad de las personas que se hayan visto afectadas por la transgresión a esta prohibición. Es decir, un mecanismo que permita, mediante una simple presentación en el mismo expediente difundido, la denuncia de la difusión y la solicitud de dar de baja las publicaciones, con una consiguiente multa por día de incumplimiento.

Finalmente, también debería preverse la exigencia, para el tribunal, de informar, en un lenguaje sencillo, en el primer decreto que se notifique a las partes el carácter privado de las actuaciones y las consecuencias que provoca su publicidad por el medio que sea. Es que hoy en día, cualquier reforma normativa, ya sea de fondo o de forma, no puede dejar de lado los comportamientos digitales que comienzan a generalizarse. puede dejar de lado los comportamientos digitales que comienzan a generalizarse.

Han transcurrido 21 años desde que decidí entrar a la facultad de Derecho, no fue fácil ni mi primera opción, pero ser astronauta o antropólogo en este país (Ecuador) no eran alternativas viables, así que tomé la decisión de aventurarme en uno de los viajes más enriquecedores de mi vida, el mundo jurídico.

A lo largo de esta aventura, probé distintas áreas, civil, penal, laboral, menores, familia, mercantil, societario, pero no creí que la rama que más me apasionaría sería la informática o como la conocemos hoy en día derecho

informático, y que a través de ella encontraría temas relacionados con otras carreras que me hizo comprender que ser abogado es una profesión inmensamente noble que nos abre el camino en cualquier otra y nos permite desenvolvernos sin ningún problema.

Sin embargo, hace 2 años, tomé la decisión de alejarme un poco del derecho y embarcarme en una nueva aventura, estudiar peluquería, y cosmetología, y no llegué nunca a imaginar cómo esta nueva aventura se convertiría en un reto de curiosidad para mí desde el campo legal, jamás pensé que estas profesiones tan distintas y tan alejadas, podrían converger de una manera tan cercana.

Quizás ahora están confundidos, y no dan con el punto de encuentro de estas profesiones, ambas tan bonitas pero tan distantes una de la otra, a simple vista no podría existir una relación tan grande, sin embargo vamos a analizar algunos aspectos dentro del ejercicio del campo de la belleza hablando en términos generales que sin duda nos demostrarán que no se encuentran tan alejadas una de la otra como imaginábamos.

Y es que hablar de belleza se remonta hasta la época de Platón quien decía que la belleza hace referencia a que “gusta, que atrae, que despierta admiración, agrado, fascinación”1, definición que no se encuentra muy lejos de la planteada por la RAE2: “Cualidad de bello” o “persona o cosa

notable por su hermosura”, y es debido a esto que hablar de belleza es algo muy subjetivo, ya que lo que es bonito o bello para una persona no necesariamente lo es para otra, sin embargo, la sociedad ha establecido un canon de belleza y que no es más que un conjunto de características según las cuales la sociedad en general considera como atractivas, bonitas o deseables a las personas, es por esto que decimos que la belleza de las cosas dependen de los ojos o el cristal con que se la mira.

Hoy en día escuchar hablar de estética tampoco es raro, la oferta de tratamientos estéticos es inmensa (reduzca medias, obtenga cintura de avispa, elimine los brazos de murciélago, rejuvenezca 100 años, entre otros), y es que, su relación directa y estrecha con la belleza ha hecho que de cierta manera belleza y estética se conviertan en una especie de sinónimo.

De acuerdo con la RAE3 se considera a la estética como: “disciplina que estudia la belleza”; sin embargo para Kant, la estética es como la doctrina de la filosofía del arte, concibiendo lo bello como una forma particular del ser, sin embargo la estética antigua no ha podido explicar el por qué lo bello es apreciado por diversos hombres de distinta manera, esto de acuerdo a los cánones que se han establecido en cada época, las clases sociales, el nivel económico e incluso el social.

Y es sin lugar a dudas que todos estos cánones ha hecho que nosotras las cosmetólogas tengamos un hermoso y gran campo de trabajo, pero no fue hasta que obtuve mi titulación y que mi curiosidad fue más grande que me di cuenta que el campo de la belleza es hermoso pero también un nicho donde la información de las personas rueda sin ningún tipo de cuidado o precaución.

Muchos se preguntarán a que me refiero y para eso utilizaré algunos ejemplos.

Cuando vamos a la peluquería en el caso de las mujeres nos sometemos a varios servicios, entre ellos arreglo de manos y pies, peinados, depilación. Sin embargo ninguno de nosotros se ha puesto a pensar que todos estos servicios dejan a la deriva muestras biológicas que contienen valiosa información personal genética como el ADN.

Es así que, si hablamos de las uñas, estas en sí mismas no sirven para extraer ADN, pero sí las células de la piel que se quedan adheridas a ellas. Las uñas de los pies son más fiables, porque es más probable que no estén contaminadas con el ADN de otras personas. Las uñas de las manos pueden tener residuos o células de otras personas, y provocar una mezcla de perfiles y, con ella, la anulación del análisis. Sin embargo, la tasa de éxito para obtener ADN de uñas de los pies es del 85%, algo que jamás en la

vida se me hubiera imaginado ya que llevo más de 20 años haciéndome un pedicure.
Y qué decir del cepillado y peinado, alguna vez se han puesto a pensar en cuantos cabellos nos arrancan de raíz cada vez que vamos al salón? O que pensar de la depilación donde nos arrancan hasta el último suspiro?.
Pues en este caso para hacer una prueba de paternidad o de maternidad se necesitan, al menos, 3 ó 4 pelos con raíz. La tasa de éxito para obtener ADN es del 85%. Ya saben cuántos nos arrancan de un jalón en una depilada e incluso de zonas donde ni el sol se atreve a llegar y por tanto la tasa de contaminación de los mismos es bajísima.
Pero el tema no termina ahí en los últimos tiempos han vuelto de moda las barberías, a las cuales los caballeros asisten para el arreglo de sus barbas, sin embargo sabían que en el depósito de la maquinilla de afeitar eléctrica, junto con los pelos, quedan células cutáneas que también pueden ser utilizadas para obtener ADN. Su tasa de fiabilidad es del 80%.

Todo este análisis me puso los pelos de punta debido a que jamás he visto políticas de manejo adecuado de muestras biológicas (uñas, cabellos, paños de depilación) o protocolos de deshecho de este tipo de deshechos (biológicos) en los salones.

Todo lo desechan en mismo lugar sin el menor reparo y es ahí cuando mi cabeza empieza a dar vueltas como novela de terror, y si toman un pedazo de mi uña y la implantan en la escena de un delito? Y si ponen un cabello mío en un lugar inapropiado solo para causar daño a mi imagen?

La menta empieza a volar y después te acuerdas que una vez fuiste a una estética para hacerte un tratamiento y llenaste una ficha con millón de información entre ella información médica y te preguntas, que tratamiento le dan a mi información, tienen sistemas de protección de datos, como manejan mi información dentro de la estética, quien tiene acceso a ella? Realizan procesos de anonimización de datos cuando comparten información de evaluación de tratamientos realizados.

En fin los cuestionamientos en relación al uso y manejo de nuestros datos si bien pueden en este caso sonar o parecer muy sacados de película o ciencia ficción los dejo con la inquietud para que puedan revisar si en sus países existen medidas específicas para estíticas, centros de belleza y otros para el manejo adecuado de desechos de muestras biológicas como se lo exige en consultorios médicos, veterinarios, hospitales y centros de salud, así como si en sus países los centros de estética desde el más grande hasta el más pequeño cuenta con algún sistema de protección de información de sus clientes.

No busco que dejemos de ir a estos lugares o nos creemos una paranoia solo busco despertar un poquito la curiosidad de ustedes y que así como yo puedan buscar espacios donde pensaban que no había posibilidad de converger y que se pueden sorprender.

DESTACADOS

2018

LA RED

BREVES CONCEPTOS

Estimados amigos, presentamos una nueva edición de nuestro reconocimientos a los que hemos considerado como "LOS DESTACADOS DEL 2018" en materia de derecho informático,

Con seguridad hemos olvidado algunos, y quizás hayan otros/as con más méritos, pero bueno, estamos para aprender como siempre y esperamos poder mejorar.-

Buscamos hacer un pequeño mimo a los que trabajan día a día por esto que tanto nos apasiona, quizás, el año que viene, le toque a alguno de Ustedes.-

Tengan un gran año!

DESTACADOS EDI 2018

CATEGORIA: TRAYECTORIA

DRA MYRNA ELIA GARCÍA BARRERA

DR EDUARDO MOLINA QUIROGA

DR DEMÓCRITO RAMOS REINALDO FILHO

DESTACADOS EDI 2018

CATEGORIA: ABOGADO/AS

DRA BARBARA PEÑALOZA (ARGENTINA)

DRA SARA IBAÑEZ (COLOMBIA)

DR DAVID BRAVO (ESPAÑA)

DESTACADOS EDI 2018

CATEGORIA: ABOGADO/AS

DRA KATIUSKA HULL HURTADO (PANAMÁ)

DR WILSON FURTADO (BRASIL)

DR DIEGO GUTIERREZ (ARGENTINA)

DESTACADOS EDI 2018

CATEGORIA: INFORMATICAS/OS

JEIMY JOSÉ CANON (COLOMBIA)

JOÃO KEPLER BRAGA (BRASIL)

SHEILA A BERTA (ARGENTINA)

DESTACADOS EDI 2018

CATEGORIA: INFORMATICO/AS

ANDRÉS VELAZUEZ (MÉXICO)

MARCELO ROMERO (ARGENTINA)

JOSÉ LEONETT (GUATEMALA)

DESTACADOS EDI 2018

CATEGORIA: SITIO WEB

TERMINOSYCONDICIONES.ES
(ESPAÑA)

ABOGADODIGITAL.TV
(MÉXICO)

JURISTAS
CERTIFICAÇÃO DIGITAL

JURISTAS.COM.BR
(BRASIL)

DESTACADOS EDI 2018

CATEGORA: APORTE ACADÉMICO

DR PABLO PALAZZI
(ARGENTINA)

DR CARLOS REUSSER
MONSALVEZ
(CHILE)

DRA PATRICIA REYES
(CHILE)

DESTACADOS EDI 2018

CATEGORA: INSTITUCIÓN/CAMPAÑA

IQT
IDEAS QUE TRANSFORMAN

IDEAS QUE TRANSFORMAN (ARGENTINA)

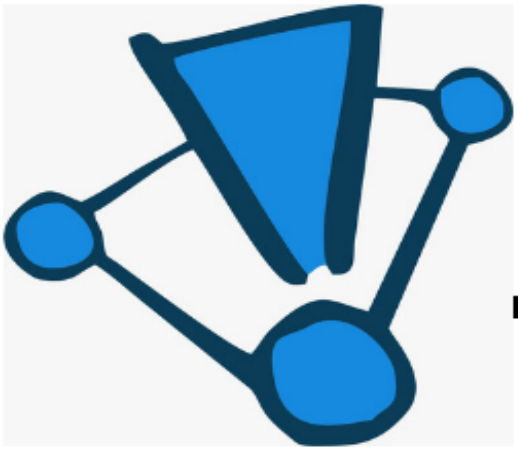
INSTITUTO BRASILERO DE DIREITO INFORMATICO (IBDI) (BRASIL)

IBDI
INSTITUTO BRASILEIRO DE DIREITO DA INFORMÁTICA

ACTIVISMO FEMINISTA DIGITAL (ARGENTINA)

DESTACADOS EDI 2018

CATEGORA: INSTITUCIÓN/CAMPAÑA



CONCIENCIA EN RED
(ARGENTINA)

ASOCIACIÓN PANAMEÑA DE
DERECHO Y NUEVAS
TECNOLOGÍAS
(PANAMÁ)

APANDETEC
DERECHO Y NUEVAS TECNOLOGIAS

ASOCIACIÓN DE
ESCRIBANOS DE URUGUAY
(URUGUAY)

DESTACADOS EDI 2018

CATEGORA: INSTITUCIÓN/CAMPAÑA

DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PUBLICOS (ECUADOR)

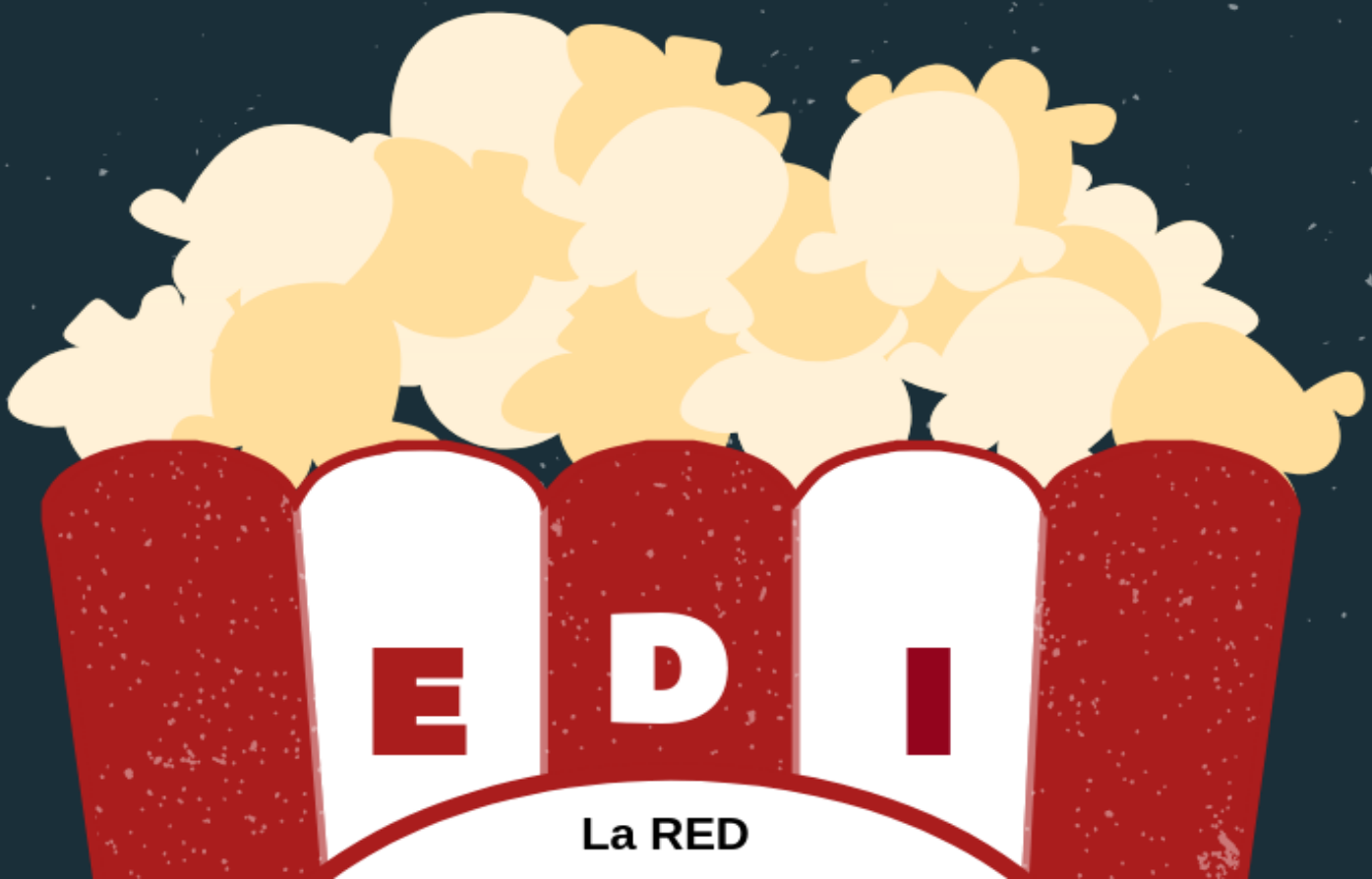
ASOCIACIÓN INTERNACIONAL DE INFORMÁTICA FORENSE (COLOMBIA)

LABORATORIO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA EN INFORMÁTICA FORENSE (INFO-LAB) (ARGENTINA)

ELDERECHOINFORMATICO.COM

LOS DESTACADOS DEL AÑO 2018

Abogado/a - Sitio Web - Trayectoria - Aporte académico - Informatico/a - Institución



\\EL CENTRO DE FORMACIÓN E INFORMACIÓN MÁS GRANDE DE IBEROAMERICA\\

LA RED

somos

ELDERECHOINFORMATICO.COM