EDI

Revista Digital Nro 29
Junio 2018

CAMILO ESCOBAR MORA -
PABLO RODRIGUEZ -
ISIDRO MORGANTI
HERNANDEZ

CAROLINA MARÍN
- CHRISTIAN H. MILLER -
SEBASTIÁN GAMEN

EMANUEL ORTIZ -
ADRIAN SANDLER -
FABIÁN DESCALZO -

MUJERES COLOMBIANAS EN EL CIBERDERECHO

CUARTO ENCUENTRO ELDERECHOINFORMATICO.COM URUGUAY

Tecnología y empoderamiento de la mujer

Jueves 2 de agosto de 2018 ▪ 9:00 hs.

Espacio Prof. Esc. Eugenio B. Cafaro de la Asociación de Escribanos del Uruguay
(Av. 18 de Julio 1730, piso 11, Montevideo)

MODALIDADES DE TRABAJO

Paneles | Charlas | Conferencias

ORGANIZA:

La Red ElDerechoInformatico.com
El Centro de Información más grande de Iberoamérica

APOYA:

Asociación de Escribanos del Uruguay

Editorial

Siempre es una satisfacción lograr la salida de una nueva edición de nuestra revista, siempre pienso que tengo para contarles de novedades o propuestas.

Hoy quiero dedicarle esta Editorial a un amigo que se fue.

El 12 de abril de 2011 recibo un correo de un estudiante avanzado del ultimo semestre de Derecho me escribía para ver la posibilidad de incluirlo entre los profesionales de la Red, me contaba que era informático, y, aunque no me lo dijo, vi que era distinto, Carlos Tudares, se recibió de abogado, fundó ReVeDerIn la Red Venezolana de Derecho Informático, y estudió y creció y se convirtió en el tipo de amigo que la distancia de nuestros paises nos permitieron, me consta que el cariño era mutuo y asi nos lo hicomos saber los últimos tiempos.

Hace unas semanas, su enfermedad y el gobierno de su pais, se lo llevó.-

No se sinceramente si este espacio es el adecuado para estas despedidas, pero siento que no tengo otros para hacerlos. Carlos era parte de la Red y como siempre decimos, buscamos la forma de no ser solo un sitio web, con noticias, sino desvirtualizarnos, conocernos, apoyarnos, ser mucho más que una foto en el whatsapp, o un Me Gusta en Face...

Hace unos días se nos fue Carlos Tudares, un amigo, buen tipo, solo queria contarles que su recuerdo quedará en mi y espero en todos Ustedes.-

Guillermo M Zamora
DIRECTOR EDI

ORGANIZA:
ELDERECHOINFORMATICO.COM

(EDI)

CONGRESO ONLINE IBEROAMERICANO DE DERECHO INFORMÁTICO

ESPAÑA - PORTUGAL - MÉXICO - GUATEMALA - PANAMÁ - COSTA RICA - DOMINICANA - VENEZUELA - COLOMBIA - ECUADOR - BRASIL - PARAGUAY - URUGUAY - CHILE - ARGENTINA

VISIÓN ACTUAL DEL DERECHO INFORMÁTICO

Agosto, 2018 | 28 - 29 - 30
plataforma virtual de la Red EDI

INFORMACIÓN POR PONENCIAS A:
ONLINE@ELDERECHOINFORMATICO.COM
INFO@ELDERECHOINFORMATICO.COM

Contenido

www.issuu.com/elderechoinformatico.com
info@elderechoinformatico.com

EDI

"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

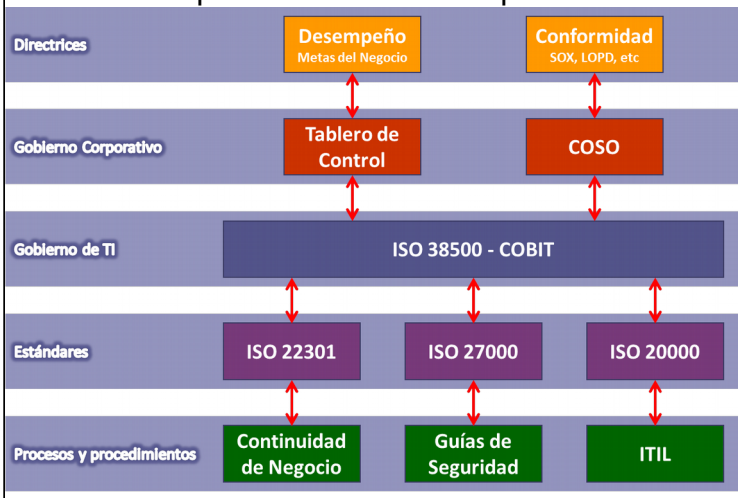
INTEGRACION DE RIESGOS DE IT Y RIESGOS OPERACIONALES

Cuando la operación de nuestro negocio depende de cómo gestionamos la tecnología

Por definición, riesgo operacional es la suma de fallas o errores en los procesos, de las personas que los ejecutan o de las tecnologías que los soportan, las que pueden presentarse tanto desde un entorno externo como interno y estar ocasionadas por actividades intencionales, procedimientos inadecuados o defectuosos o por agentes contingentes como desastres naturales.

Entre estos escenarios pueden presentarse tanto **amenazas**, como un potencial de riesgo, como **vulnerabilidades,** que son brechas que quedan como puertas abiertas esperando a ser explotadas en forma programada o fortuita. Lo que sí tienen en común es un escudo metodológico para mitigar los riesgos a la operación: **LA GESTIÓN**. Entonces, evitar pérdidas financieras e incumplimiento legal requiere establecer un entorno metodológico en nuestra operación, mediante la gestión relacionada con la seguridad física y lógica, normativa interna para alinear las TI con el cumplimiento, proyectos de TI, usuarios de la organización, y amenazas externas.

En la búsqueda de cómo resolver nuestra problemática sobre los riesgos operativos, podemos ver que existe una relación lógica entre la definición del alcance del riesgo operacional y los factores de producción determinados para el gobierno de la información (Procesos – tecnologías – personas), afirmando la necesidad de establecer procesos adecuados para el



cumplimiento de los objetivos de negocio, operados por personal con las capacidades y conocimientos necesarios y acorde a sus funciones dentro de los servicios y el soporte de recursos tecnológicos e infraestructura de servicios a la medida de las necesidades del negocio.

Por ello, es natural el empleo de estándares relacionados con el Gobierno de TI y Gobierno Corporativo (como las Normas ISO 20.000 y 27001, ITIL, COBIT5, Normas NIST, etc.) para normalizar nuestros procesos y ayudar a ordenar todas las actividades asociadas a la Continuidad Operativa, así como a la Integridad y Disponibilidad de la información.

Minimizar el riesgo operativo requiere de un conocimiento ***"relacionalista"*** de la Organización. Pensar que los procesos internos y los servicios de TI están disociados entre sí o que no hay nada más allá de la

Organización que pueda afectarla, es acotarse a una sola dimensión de riesgos y perder la visión global y multidisciplinaria que se requiere para la subsistencia de la operación de nuestro negocio. Las necesidades de Gobierno deben surgir a nivel Corporativo, desde todas las áreas de la Organización, y apoyarse piramidalmente teniendo en cuenta que no se pueden establecer directrices que no se sustenten inicialmente en procesos y procedimientos que vayan enmarcándola hacia un camino de madurez que le permita establecer un Gobierno adecuado a su entorno, a su industria y principalmente a su cultura. Este entendimiento nos brindará la objetividad necesaria para la adopción de los estándares adecuados.

¿Cómo determino objetivamente cual es el marco metodológico adecuado?

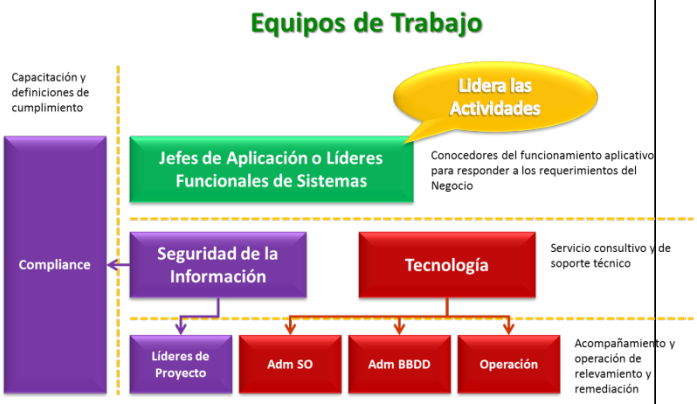
Inicialmente debo conocer "el negocio", a través de las definiciones de sus procesos y de su marco legal y regulatorio. Esto nos aporta el hecho de conocer cuáles son los límites del entorno de su industria y define los primeros parámetros de alto nivel o necesidades primarias de cumplimiento. Como sabemos, las leyes o regulaciones nos dicen lo que se debe cumplir pero no como implementar el cumplimiento, por lo que es muy importante basarnos en nuestro conocimiento inicial para verificar internamente en la organización cuál es su "adherencia" al cumplimiento y la cultura de las personas en su participación en los procesos. Esto nos ayudará a la elección del estándar adecuado para nuestra Organización y determinará cual es la forma más correcta de abordar su implementación.

Una vez seleccionado el estándar e identificados los puntos de necesidad de cumplimiento, podremos definir los planes de implementación o remediación necesarios, que deben alcanzar tanto a procesos, como a personas y tecnología. El resultado final nos debe aportar lo que llamamos "línea base de cumplimiento", con definiciones funcionales y técnicas que se verán representadas en nuestro marco normativo.

Como dijimos, debemos tener una visión global y multidisciplinaria, por lo que cada área de la organización va a participar en forma completa y desde sus funciones, tanto de actividades consultivas como operativas según corresponda, y de acuerdo a sus alcances funcionales relacionados con el Gobierno, Riesgo y Cumplimiento. Uno de los mejores ejemplos para visualizar esta interacción, es la de reconocer en un proyecto de negocio cuales son los diferentes hitos relacionados con la necesidad que tiene la Organización en el inter-relacionamiento de sus áreas para la obtención de sus objetivos.

Imaginemos que un área de negocio de nuestra organización está desarrollando un nuevo servicio, el cual requiere del uso de la tecnología. Como indicamos, ya contamos con una línea base de cumplimiento que abarca tanto a procesos funcionales como tecnológicos, y esta base de cumplimiento requiere que el análisis de los riesgos

asociados a este proyecto sea realizado en conjunto entre el área de negocios y las áreas tecnológicas, con el soporte consultivo de áreas legales y de riesgo, porque este análisis no solo debe estar enfocado a los riesgos sobre las ganancias del negocio, sino también a las pérdidas económicas por la falta de previsión en la operación, continuidad y cumplimiento que requiera tanto el servicio de negocio como el servicio de TI.



Esto nos lleva a conformar un equipo de trabajo para cada proyecto dentro del cual podamos sumar el conocimiento y las experiencias de las personas en la construcción de este servicio de negocio apoyado en la tecnología, teniendo en cuenta que el representante del negocio debe liderar el proyecto (como dueño del proceso, de datos y riesgos que es) apoyado por las áreas de cumplimiento y legales, y contando con los servicios de soporte y operación de Tecnología y Seguridad de la Información.

Para comprender los alcances que debemos tener en cuenta al iniciar el diseño de proceso o servicio de TI y seguridad de la información para dar soporte a los procesos de negocio nuevos o existentes, desarrollé el siguiente mapa en donde identifiqué los diferentes componentes que construyen los recursos necesarios para la operación de la tecnología, y sobre los cuales deben identificarse aquellos riesgos asociados y objetivos que pueda tener nuestra Organización basados principalmente en los resultados de nuestra gestión de incidentes, gestión de riesgos y en el análisis del entorno geográfico, físico y operativo en el que se suceden los servicios de TI.

Esto abarca tanto aspectos técnicos como lo relacionado con los ambientes de aplicación e infraestructura como al gobierno y control sobre la tecnología, que son componentes clave a los cuales necesito ponerles una gestión adecuada a la cultura interna y madurez del negocio, y a su entorno e industria, para minimizar las probabilidades de impacto negativo a nuestra operación y proteger la información de la organización.

Pensando en riesgos operacionales, no podemos dejar de lado la participación de terceros en nuestros procesos de negocio o de servicios tecnológicos, ya que es habitual la subcontratación para potenciar nuestros procesos o servicios valiéndonos de la experiencia y conocimientos de un socio de negocio o un proveedor. Ahora bien, si no nos proponemos una adecuada gestión sobre nuestras terceras partes, aumentan mis riesgos en la contratación, por ejemplo, sobre los recursos humanos, legales por incumplimientos contractuales con nuestros clientes o relacionados con la tecnología en cuanto a sus vulnerabilidades y amenazas propias de cada plataforma.

La gestión y aplicación de la tecnología y las crisis externas a la organización, son los principales focos de amenazas que conforman los principales riesgos de TI, que asociados ponen en grave peligro a la operación si no los evaluamos en forma correcta identificando su mapeo relacional con los procesos de negocio y su entorno operativo. Basados en este análisis, podremos obtener para cada uno el plan de mitigación adecuado a la operación real, siendo así seguros y óptimos respecto de las necesidades operativas de la compañía.

Hay cuatro dominios en los cuales deben agruparse las principales actividades de mitigación de estos riesgos de TI:

- ***El gobierno de la tecnología***, que debe ser compartido con nuestro proveedor de servicios
- ***La gestión de riesgos sobre los servicios***, tanto internos como externos, y en el caso de terceros, reclamando y auditando a nuestro proveedor en su gestión implementada
- ***La educación y actualización para la mejora del conocimiento y capacidades***, no solo relacionadas con la infraestructura técnica sino también en los procesos de servicio de TI, tanto de los contratados como de los internos, sobre los cuales el proveedor también debe capacitarse
- ***El cumplimiento***, sobre la base de ser conscientes que puede delegarse la operación en un tercero, pero no puedo delegar la responsabilidad en el cumplimiento, por lo que debo establecer los controles y auditorías necesarias para verificar este cumplimiento por parte de nuestro proveedor

Esto determina que, tanto los riesgos asociados al proceso de negocios y a los servicios de TI como las necesidades de continuidad operativa de los mismos, debe ser pensada desde su diseño. Conocer el modelo de negocio y diseñar los servicios de TI entorno a sus necesidades basándonos en una gestión implementada como resultado de la adopción de estándares metodológicos, nos va a brindar la oportunidad de construir servicios de TI que estén alineados a los procesos de negocio, y por ende a los objetivos de la organización dando una respuesta efectiva a su ***plan de negocio.***

Además de cumplir con las etapas lógicas y prestablecidas por cualquier normativa asociada a la gestión de proyectos, seguridad de la información o gestión de los servicios de TI, es recomendable que cada vez que decida iniciar un proyecto identifique una fase de capacitación para el entendimiento de la operación, integre el equipo de trabajo documentando e informándoles sobre sus alcances y roles dentro del proyecto, necesidades de cumplimiento legal y de negocio y, fundamentalmente, las necesidades de servicio por parte de las áreas tecnológicas (IT, redes, comunicaciones) y de seguridad

(seguridad de la información, o bien seguridad física y seguridad informática).

En el inicio de este camino, lo que primero deberíamos de establecer es un conjunto de actividades tendientes a proteger y controlar los principales componentes de los servicios de TI al negocio. Este blindaje podremos obtenerlo mediante actividades iniciales asociadas a Terceras Partes, Seguridad Física, Seguridad de la Información, Controles sobre la operación de la tecnología, Proyectos de TI y Planes de respuesta para asegurar la continuidad ante incidentes. Respecto de los riesgos a identificar y su posterior gestión, si bien no hay una metodología única (ISO/IEC 27005, ISO/IEC 31000 y 31010), una de las más claras en su implementación y recomendable es MAGERIT, que a través de sus tres libros y sus métricas e indicadores, ofrecen una guía para una gestión prudentemente con medidas de seguridad que sustentan la confianza de los usuarios de los servicios.

A las cuatro etapas conocidas para la gestión de riesgos, recomiendo sumar una quinta asociada a la comunicación interna y externa sobre la metodología implementada, sus resultados, los mecanismos de mitigación definidos, y la asociación de la gestión de riesgos con la definición de los objetivos de control y los diferentes controles que deben ser implementados para satisfacer los requerimientos identificados a través de la evaluación de riesgos, así como la concientización sobre las amenazas de los riesgos identificados y la capacitación por área de interés (Dirección - Técnica - Gerencias - Usuarios) sobre los mecanismos de mitigación, sean estos funcionales o técnicos.

Para finalizar, y como conclusión, recordemos que ***las necesidades del negocio son cada vez más exigentes, y de igual forma las tecnologías son cada vez más complejas, por lo que brindar soluciones que aporten mayor velocidad de respuesta a la Organización tiene sus "costos" asociados... y sus riesgos.***

El Negocio necesita de la Tecnología, pero la Tecnología sin Gestión es un riesgo directo a la Operación del Negocio… y a sus Objetivos.

Fabián Descalzo

Gerente de Servicios y Soluciones en el área de Gobierno, Riesgo y Cumplimiento (GRC) en Cybsec by Deloitte S.A., con 28 años de experiencia en la implementación y cumplimiento de Leyes y Normativas Nacionales e Internacionales en compañías de primer nivel de diferentes áreas de negocio en la optimización y cumplimiento de la seguridad en sistemas de información, Gobierno de TI y Gobierno de Seguridad de la Información.

Miembro del Comité Directivo del "Cyber Security for Critical Assets LATAM Summit" para Qatalys Global sección Infraestructura Crítica (Gobiernos y empresas de América

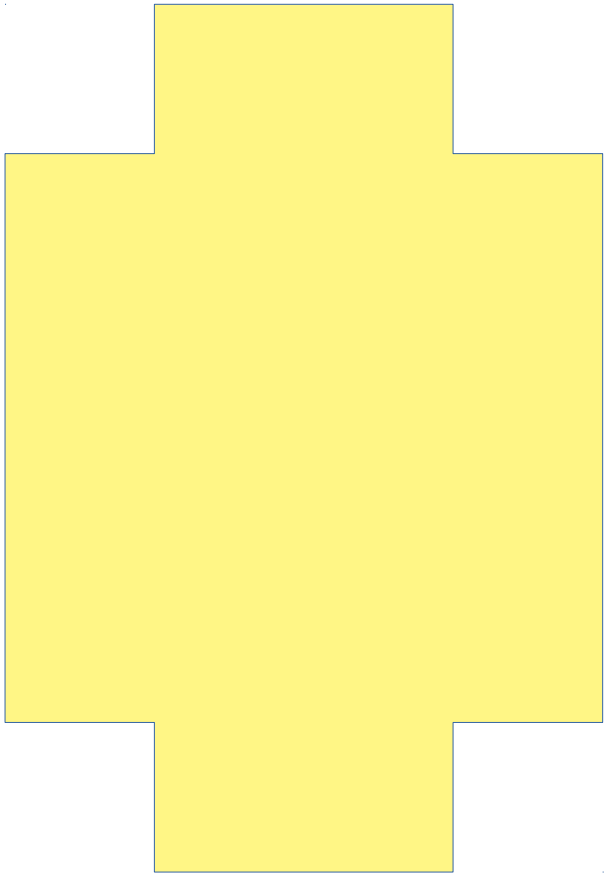
Latina en el sector de la energía, química, petróleo y gas), Miembro del Comité Científico ARGENCON del IEEE (Institute of Electrical and Electronics Engineers), Miembro del Comité Organizador CYBER 2015 de ADACSI/ISACA, certificado en Dirección de Seguridad de la Información (Universidad CAECE), instructor certificado ITIL Fundation v3-2011 (EXIN), auditor ISO 20000 (LSQA-Latu), IRCA ISMS Auditor / Lead Auditor ISO/IEC 27001 y Lead Auditor ISO/IEC 20000 TÜV Rheinland.

Columnista especializado en áreas de Gobierno, Seguridad y Auditoría, Informática en Salud y Compliance en las revistas CISALUD, PERCEPCIONES (ISACA Montevideo Chapter), El Derecho Informático, CXO-Community, EXIN Newsletter y MAGAZCITUM; y disertante para CXO-COMMUNITY, Consejo Profesional de Ciencias Informáticas, ISACA Buenos Aires Chapter, ISACA Montevideo Chapter.

Docente del módulo 27001 del curso de "IT Governance, Uso eficiente de Frameworks" y de la "Diplomatura en Gobierno y Gestión de Servicios de IT" del Instituto Tecnológico de Buenos Aires (ITBA); Docente en "Sistemas de Gestión IT" y "Seguridad de la Información" en TÜV Rheinland Argentina, Docente del módulo Auditoría y Control en Seguridad de la Información en la Universidad Nacional de Rio Negro.

CERTIFICACIONES:

- *TÜV Rheinland / Lead Auditor ISO/IEC 20000:2011 (Certificate Number 17-6510 - TÜV Rheinland Febrero 2017)*
- *IRCA ISMS Auditor / Lead Auditor ISO/IEC 27001 (Certificate Number IT2566710 - TÜV Rheinland Septiembre 2016)*
- *Dirección de seguridad de la información (Universidad CAECE Diciembre 2013)*
- *ITIL® version 3:2011, Certification for Information Management (EXIN License EXN4396338 Enero 2011)*
- *ITIL® version 3:2011, Certification for Accredited Trainer (EXIN Accreditation Enero 2012)*
- *Foundation ISO/IEC 20000-1:2011, Implementación de Sistemas de Gestión IT (LSQA - LATU Diciembre 2011)*
- *Internal Audit ISO/IEC 20000:2011, Auditor Interno en Sistemas de Gestión IT (LSQA - LATU Diciembre 2011)*



Buenas prácticas mediáticas en el universo de la pancomunicación

Por Adrián Sandler
Licenciado en Ciencias de la Comunicación (UBA).
Docente (UNPSJB e ISER Trelew).

Desde la irrupción de Internet primero, y de las redes sociales después, el periodismo cambió para siempre. El ejercicio de la profesión núcleo de los medios de comunicación se modificó, ya que las prácticas debieron adaptarse a las características del nuevo mundo comunicacional. Con una gradualidad de moderada a escasa, una multiplicidad de fuentes estuvo disponible de manera casi simultánea.

Dos consecuencias inmediatas fueron que muchos -quizás la mayoría- consideraron que ya no era imprescindible estar en el lugar de los acontecimientos. Y, de ellos, varios se aventuraron al ejercicio de informar sin apelar al chequeo, garantía del buen ejercicio periodístico.

Al interior de las redacciones, sobre todo de los medios gráficos, la aparición de Internet favoreció la comodidad, enemiga íntima de cualquier actividad. Y más de la periodística, que se hizo más sedentaria que nunca.

Las redes sociales exacerbaron, y lo sigue haciendo, las malas tentaciones. Facebook primero, Twitter después, Instagram un poco más tarde, las tres más adelante -y en la actualidad- se convirtieron, más de lo recomendable, en fuentes de información que luego no era sometida al obligado y noble ejercicio del chequeo, no ya por medio de la consulta a los protagonistas de la noticia o a los portadores del saber, sino ni siquiera a través de otras fuentes provenientes del mismo universo mediático.

El periodismo se vio y se ve contaminado por la influencia de *trolls*, *bots*, *fake news* y demás fenómenos que, con otros nombres, vinieron a exacerbar malas prácticas que siempre existieron, pero antes con otros nombres no extranjerizados: pescado podrido, mentiras, operaciones de prensa.

El escenario comunicacional es complejo en todo sentido. La multiplicidad de canales hace imposible hablar hoy de un universo clásico, compuesto por los diarios, la radio y la televisión. Desde el punto de vista académico, el panorama complica incluso a las más tradicionales y prestigiosas corrientes teóricas, que deben ser reinventadas para incorporar a esos nuevos habitantes que al parecer vinieron para quedarse, más allá de sus formas.

Ya no alcanza hoy con apelar a la expresión “estamos en un mundo hipercomunicado”, para graficar la multiplicidad de los canales y la vorágine en la que circula la información. Otro término debería ser empleado con más asiduidad, y podríamos llamarlo “pancomunicación”. Desde el punto de vista científico, no se trata de una expresión nueva, es cierto. Pero resulta necesario apelar a su etimología para graficar su alcance. El prefijo pan, en su raíz griega, tiene como significado

"todo". Y comunicar, del latín "comunis", refiere a poner "en común" ideas o pensamientos.

Hoy todo se pone en común, absolutamente todo se comunica, desde las simples acciones cotidianas de cualquier habitante del planeta, hasta los más complejos hallazgos científicos y tecnológicos.

En este contexto, el periodismo, y por consiguiente los medios de comunicación se encuentran ante desafíos permanentes.

Por eso, aunque se podría suponer que la multiplicidad de canales y el fácil acceso a las redes sociales generan que sea más sencillo hacer periodismo, la contaminación que conlleva este universo pancomunicado hace imprescindible que los comunicadores sean -seamos- cada vez más profesionales.

¿Qué significa ser más profesional? Se podría pensar que para ser un buen comunicador alcanza hoy con manejar con suficiencia las herramientas y que hasta sería recomendable convertirse en un experto en nuevas tecnologías.

Es cierto que actualmente resulta muy necesario contar con esos conocimientos, pero eso no lleva, necesariamente, a profesionalizar el periodismo.

Profesionalizar el periodismo consiste, básicamente, en rescatar ese cúmulo de prácticas, conceptos y conocimientos que están en la base del ejercicio, más allá de cualquier soporte. Y es, también, mantenerse actualizado, pero no necesariamente para conocer las últimas tecnologías y para saber manejar un dron.

Mantenerse actualizado implica saber, por ejemplo, que la primicia, producto estrella del periodismo del siglo XX, es hoy un término en desuso, no por cuestiones semánticas y por el aggiornamiento inevitable del idioma, sino porque resulta casi incomprobable decir o saber quién dio una información antes que otro. Y porque, además, en el mundo de la hipercomunicación y de la pancomunicación resulta hasta intrascendente erigirse en portador de un dato, cuando ese dato se transforma, se amplía, se deforma, se niega, se confirma -a veces todo al mismo tiempo- desde el mismo momento en que se hace visible en el universo mediático.

Profesionalizar la comunicación implica saber, entonces, que no importa quién da primero la noticia, sino quién la da mejor. Apresurarse a hacer público un dato sin el debido chequeo, sin la maduración que muchas veces necesita el

desarrollo de los acontecimientos, puede tener consecuencias no deseadas.

Y esas consecuencias no deseadas no pasan por el ya vulgar escarnio cibernético al que todos estamos expuestos, porque en la práctica profesional del periodismo no está en juego tanto el prestigio personal como la responsabilidad

social, de la que nunca un comunicador debería apartarse.
La responsabilidad social del periodismo implica contar con las competencias adecuadas para que la información dada sea la mejor posible, y en la cual los receptores -oyentes, lectores, televidentes, usuarios- puedan confiar.
Además, la responsabilidad social pondrá al periodista profesional al resguardo legal, ya que los medios de comunicación han sido siempre espacios expuestos a esas consecuencias, preanunciadas la mayoría de las veces a través de cartas documento que son el prólogo, muy a menudo, de batallas legales perdidas, por la simple razón de que, cualquiera sea el soporte, los productos de los medios siempre perduran en el tiempo y rara vez se pierden en el espacio.
La responsabilidad social que implican las buenas prácticas periodísticas pondrá, además, a resguardo a los medios de comunicación del embate de los poderes -formales o informales- a los que de manera inevitable se enfrenta, no porque uno contenga el bien y otro el mal, sino porque ambos, poderes y medios, compiten cada vez con mayor agresividad por el control de la agenda pública en la que, a su vez, ha ido creciendo la intervención de las audiencias o, simplemente, de los ciudadanos interesados en los asuntos públicos.
En definitiva, en el universo pancomunicado, los periodistas tienen enormes oportunidades: de la misma manera que tientan al mal ejercicio, presentan un escenario rico para las buenas prácticas. Ya que el periodismo se provee de fuentes, es innegable que hoy, por efecto de la tecnología, existen múltiples disponibles, al mismo tiempo. Esa sola consideración, sin mencionar otros fenómenos vinculados a la instantaneidad de comunicación que permiten los teléfonos y sus aplicaciones, puede ayudar, y mucho, a que los medios ofrezcan información variada y de mayor calidad.

Periodista de https://suractual.com.ar

LA RED EDI

INFORMACIÓN QUE SUENA BIEN

WWW.ELDERECHOINFORMATICO.COM

CIBERFORENSIC 2018

4to Simposio Nacional sobre Ciberdelitos,
Cibercrimen e Informática Forense en Guatemala
18 de Agosto del 2018. Club Centro Español, Calzada Roosevelt

CIBERFORENSIC 2018

4to SIMPOSIO NACIONAL SOBRE CIBERDELITOS. CIBERCRIMEN E INFORMATICA FORENSE EN GUATEMALA

18 de Agosto 2018. De 08am a 06pm.
Club Centro Español, Calzada Roosevelt.
General Q.500.00 en preventa hasta el 20 de Julio o al agotar cupos
Información en (502) 58666403 o capacitaciones@infogtm.com

Organizan

OGDI.ORG — Observatorio Guatemalteco de Delitos Informáticos
RVDI
INFO y más — Seguridad & Informática Forense
REDLIF — Red Latinoamericana de Informática Forense
EDI — Red Iberoamericana ElDerechoInformatico.com

Conferencia Magistral

[JAVIER LEON CABRERA]
Ecuatoriano. Ingeniero en sistemas, Abogado, CEO/Founder de REDLIF Latinoamérica.
> Peritaje forense de Smartphones
> Taller de análisis de malware

Conferencia Magistral

[JOSE R. VALLADARES]
Guatemalteco, Ingeniero. Diputado del Congreso de la Republica de Guatemala.
> Iniciativa 5254: la necesidad de una ley contra los Ciberdelitos y Cibercrimen en Guatemala

Conferencia Magistral

[GABRIEL JUÁREZ LUCAS]
Guatemalteco, Cuarto Viceministro de Tecnologías de la Información y Comunicación. Doctorado en Seguridad Estratégica, MSc. Telecomunicaciones y Redes de Computadoras.
> La estrategia nacional de seguridad cibernética para Guatemala

Conferencia Magistral

[ABNER PAREDES]
Guatemalteco, Titular de la Defensoría de la Juventud, del Procurador de los Derechos Humanos de Guatemala.
> Adolescentes, jóvenes y las redes sociales: Prevención a la vulneración de sus derechos

Conferencia Magistral

[VIVIAN RODRIGUEZ]
Guatemalteca. Coordinadora Protección Infantil en Aldeas Infantiles SOS Guatemala. Licenciatura en Psicología. Postgrado en Psicología Social y Violencia Política.
> Campaña nacional de protección infantil de aldeas infantiles SOS: Navegando seguro en el Ciberespacio

Conferencia Magistral

[ANNIELLE CABRERA]
Guatemalteca. Licenciada en Investigación Criminal y Forense, con una Maestría en Criminología y Postgrado en Victimología. Analista en el Ministerio Publico de Guatemala.
> Persecución penal y análisis criminal de abuso sexual en línea

COINSECI

VideoConferencia Magistral

[ACTIVO UNO]
Europeo. Analista de Ciberinteligencia y miembro de la comunidad de inteligencia, seguridad y Ciberdefensa.
> Ciberinteligencia en el combate de grupos Extremistas y Ciberterroristas residentes en internet

Conferencia Demostrativa

[JOSÉ R. LEO[NETT]
Venezolano. CEO/Founder Observatorio Guatemalteco de Delitos Informáticos OGDI.
>Inteligencia electrónica: CiberPandillas, Ciberterrorismo y el trafico de drogas en el ciberespacio de Guatemala

En simultaneo estaremos llevando acabo el 2do reto forense digital de Guatemala

CIBERFORENSIC 2018

4to Simposio Nacional sobre Ciberdelitos,
Cibercrimen e Informática Forense en Guatemala
18 de Agosto del 2018. Club Centro Español, Calzada Roosevelt

A propósito del fallo “Kosten” y la responsabilidad de MercadoLibre

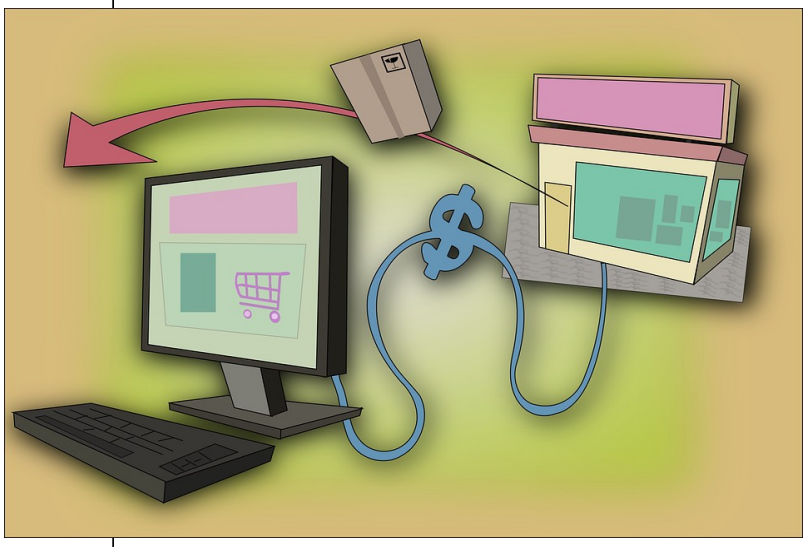
Por Christian H. Miller*

Por un lado tenemos a un hombre común que compra productos por Internet luego de varios años de mirar con cierto recelo al comercio electrónico. Y por el otro, a MercadoLibre, quien justamente ha logrado que los internautas confíen en su sitio porque, a diferencia de la competencia, modera las publicaciones, edita los comentarios y revisa los movimientos de cada uno de los usuarios.

Por un lado tenemos a un consumidor, con un conocimiento limitado a su experiencia, a la información que se le brinda y a la publicidad que lo rodea. Y por el otro, a MercadoLibre, quien con sus 15 años en línea se configura como el referente del rubro y es su posición dominante en el mercado lo que le permite ser el único sitio de “e-commerce” de nuestro país que monetiza, además de la publicidad, a través de las “mejores condiciones” de publicación y de las comisiones por ventas.

Porque para muchos usuarios, en especial para los más jóvenes, MercadoLibre se presenta como la puerta de acceso a un mercado mucho más competitivo y veloz, una oportunidad extremadamente más provechosa que el viejo sistema de revisar "local por local". De hecho, Internet en general se ha convertido en un centro de contacto para las masas, en donde se desarrollan la mayoría de los intereses individuales, como así también las operaciones comerciales y las relaciones interpersonales.

Y luego llegan a los tribunales los autos “Kosten, Esteban c. MercadoLibre SRL s. Ordinario”, donde el actor promovió demanda para lograr el resarcimiento de los daños y perjuicios que derivaron de la falta de entrega de un automotor que dijo haber adquirido a través del sitio de la demandada. Afirmó haber pagado el precio de compra mediante giros internacionales -con intervención de una empresa local- y la entrega de una suma para “gastos de entrega y documentación”, pero que pese a todo ello nunca recibió el rodado. Reclamó, en concreto, se condene a la demandada al pago de cuanto abonó por la frustrada operación, a la reparación del daño moral, y que se le aplique una multa -a su favor- en concepto de daño punitivo.



Al resolver, la Cámara Nacional de Apelaciones en lo Comercial confirmó el fallo de primera instancia y rechazó la demanda al considerar que “el actor ha sido víctima de su propia torpeza”. En la sentencia, y sin perjuicio de lo ya degradante que resulta para el Sr. Kolsen en particular -y para los consumidores en general- que se emparente a la

confianza brindada con la “propia torpeza”, se sostiene que “puede hablarse de una exención de responsabilidad del operador de un mercado electrónico de ventas o subastas on line cuando no ha desempeñado un papel activo que le permita adquirir conocimiento o control de los datos almacenados, es decir, cuando ha sido un “mero canal” limitándose a proporcionar un foro para una transacción entre un comprador y un vendedor (…) no es posible responsabilizar al operador cuando actúa efectivamente como un mero intermediario, es decir, adoptando entre los destinatarios del servicio (comprador y vendedor) una posición neutra, meramente técnica, automática y pasiva, lo que impide que tenga conocimiento y control de la información almacenada”.

Y aunque se aclara que de todas maneras “deben quedar a salvo los casos de ignorancia premeditada y de indiferencia imprudente” por parte del titular del sitio, lo que equivale a un conocimiento efectivo (conf. “Tiffany (NJ) INC. y Tiffany y Company v. EBay, Inc.”, 600 F.3d. 93, 2010), se arriba a la conclusión que “el resultado de la prueba rendida en autos demuestra, sin asomo de dudas, que la demandada Mercado Libre S.A. se comportó con relación a la oferta de venta del automotor que interesó al actor como un simple sitio web de alojamiento de datos (hosting)” y que “los recaudos que ha de adoptar el adquirente de un automotor son esencialmente dos: verificación física del vehículo y verificación de su situación jurídica… (Sin los cuales) el adquirente no podrá invocar buena fe, porque el error derivará de su propia negligencia que, naturalmente, no podrá ser alegada para justificarse”.

QUÉ ES MERCADOLIBRE

No es la primera vez que lo escuchamos, y no será la última. Consumidores estafados a través de MercadoLibre de a montones, mientras la titular de la plataforma permanece inmutable y en la búsqueda desmedida del lucro mediante el reconocimiento social que puede generar una página web justamente por presentarse como el lugar propicio para el comercio electrónico, pero también para distintas modalidades de estafa. Porque, sea cual sea el argumento que se tome, no es discutible que MercadoLibre se configura como intermediario. De hecho, la comunidad de Internet -en sitios emblemáticos como Wikipedia-, la define como tal. Es evidente que integra la cadena comercial y, en consecuencia, resulta solidariamente responsable con los otros sujetos de esa cadena tal y como lo manda la ley de Defensa del Consumidor.

Y sin embargo, en diversos procesos, tanto judiciales como administrativos, la demandada reitera argumentos defensivos tales como: “MercadoLibre no participa en la oferta de bienes, ni en la formación de los contratos que realizan sus clientes, por tanto debe ser considerado como un tercero ajeno a la compraventa”; “MercadoLibre no integra la relación de consumo”; “MercadoLibre es como el suplemento de clasificados del diario, o simplemente una biblioteca”; “De parte de MercadoLibre no hubo incumplimiento de ninguna disposición de la ley 24.240”; etc., todas premisas falsas tendientes a justificar la carencia de legitimación pasiva, una conclusión claramente errónea. Porque “lejos está de asimilarse MercadoLibre a un diario, desde ya que es una comparación absurda, pues es notorio el incumplimiento de este proveedor, a la Ley de Defensa del Consumidor, especialmente al Artículo 4º: "Informa-

ción. El proveedor está obligado a suministrar al consumidor en forma cierta, clara y detallada todo lo relacionado con las características esenciales de los bienes y servicios que provee, y las condiciones de su comercialización. La información debe ser siempre gratuita para el consumidor y proporcionada con claridad necesaria que permita su comprensión (…) de lo contrario no hubiese tenido la confianza para operar con Mercado Libre y, mucho menos no estaría siendo hoy materia de discusión" (conf. Mariángeles Schell, "Comercio electrónico vs. Responsabilidad de Mercado Libre S.A.", elDial.com - DC172A).

Resulta que MercadoLibre es responsable desde el mismo momento en que, creando una apariencia, logra atraer para sí la confianza de sus clientes. La confianza es la clave en el comercio electrónico, el mismo Lorenzetti nos dice que "desde el punto de vista del oferente, no resulta obligado por su voluntad, sino por la apariencia jurídica creada"; y "desde el punto de vista del aceptante, no interesa tanto su voluntad como la confianza que prestó para aceptar" (conf. Ricardo Lorenzetti, "Comercio Electrónico", Buenos Aires, Ed. Abeledo Perrot. Año 2001, Pág. 172), asimismo agrega un ejemplo brillante para clarificar la cuestión, "al subir a un avión no revisamos los controles del aeropuerto ni la capacidad del piloto; al contratar por Internet no hacemos una indagación sobre la solvencia del oferente o del servidor, el funcionamiento de las claves, el sistema de seguridad en las transacciones y otros aspectos. Siempre suponemos que alguien se ha ocupado de que las cosas funcionen; ese alguien no es un sujeto conocido y responsable de sus actos, como ocurre con el almacenero del barrio, se trata en cambio, de un sistema que puede aparecer ante el consumidor como una persona amable pero es sólo un empleado, de cara anónima y no responsable" (conf. Ricardo Lorenzetti, ob. cit., pág. 228/229).

Hoy por hoy, nadie desconoce la existencia de MercadoLibre, "todos sabemos que hay un mercado en Internet en el cual se pueden comprar cosas usadas o nuevas, tanto en el ámbito nacional e internacional.- Lo sabe hasta aquel que no realiza operaciones allí.- El comprador realiza el contrato virtual casi "con los ojos cerrados" creyendo y suponiendo que aquel jamás lo defraudará" (conf. Mariángeles Schell, ob. cit.). Es precisamente esa confianza la que se constituye como la fuente primaria de sus obligaciones y, como es debido, también de sus ganancias.

MercadoLibre opera en nuestro país, y, en quince años, se expandió también a Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Perú, Portugal, República Dominicana, Uruguay y Venezuela. El inversor inicial, que confió en una idea con gran potencial pero en un rubro no tradicional para la Argentina, obtuvo un enorme rédito. Hoy, MercadoLibre es la compañía de comercio electrónico más importante de América Latina. De hecho, y con motivo de celebrar el 15° aniversario de su creación, protagonizó -el pasado 14 de Octubre- el cierre de sesión del mercado Nasdaq de Wall Street, con el tradicional toque de campana. Es que MercadoLibre se negocia en el mercado tecnológico de Nueva York desde 2007 y allí compite con gigantes como Facebook, Google y Twitter. De hecho, en la actualidad, transacciona productos por un volumen mayor a los u$s5.000 millones anuales y la capitalización bursátil de la compañía es de u$s4.610 millones, equivalente al 39,4% del valor de todas las acciones de YPF sumadas, es decir que casi multiplicó por cuatro su valor de empresa en los

últimos siete años. Los economistas e inversores la catalogan como una de las empresas "más valiosas de la región". Y ese crecimiento lo logró a costa de sus usuarios y consumidores, por lo que resulta lógico que responda en relación al beneficio obtenido.

RESPONSABILIDAD DEL SITIO

En un primer momento, el tema de la responsabilidad era estudiado con normas moldeadas como expresión de la filosofía individualista, que se centraba en el elemento subjetivo de atribución (dolo o culpa), con la nueva realidad se produce la eliminación del carácter absoluto de la idea de culpa (conf. Garrido, Lidia - "Los riesgos del desarrollo en el Derecho de Daños argentino", pág. 37). "Dice Mosset Iturraspe respecto a ese ensanchamiento del que hablamos, que el Derecho Moderno que quiera progresar en la búsqueda del bien común debe luchar por la solución justa con la certeza de que detrás del daño no está el azar o la desgracia impersonal o anónima, sino el actuar de una persona o la creación de un riesgo... Además no hay que olvidar que la faz preventiva en materia de Derecho de Daños hoy se encuentra reforzada por los principios de prevención y precautorio que necesariamente confluirán frente al riesgo de desarrollo..." (conf. Garrido, Lidia, ob. cit.). Y éste es justamente el espíritu del régimen del consumidor, que centra su protección en la víctima, no en el responsable, proponiendo la prevención del daño, en contraposición al viejo régimen de responsabilidad que se sostenía sobre el culpable. Aquí MercadoLibre lleva adelante una actividad riesgosa, lucra con ella, y por ende debe responder frente a sus usuarios.

Es que las empresas actúan profesionalmente y los consumidores no son expertos, por lo que "la distancia económica y cognoscitiva que existe en el mundo real se mantiene en el mundo virtual. Podríamos afirmar que no sólo se mantiene, sino que se profundiza… Debe tenerse en cuenta también que la tecnología es cada vez más compleja en su diseño, pero se presenta de modo simplificado frente al usuario, ocultando de este modo una gran cantidad de aspectos que permanecen en la esfera de control del proveedor. Puede afirmarse que la tecnología incrementa la vulnerabilidad de los consumidores, instaurado en un trato no familiar" (conf. R. Lorenzetti, "Comercio Electrónico", Ed. Abeledo Perrot, páginas 220 y 222).

Y por otra parte, cabe agregar que es MercadoLibre quien, a través del punto 4.2 (Publicación de bienes y/o servicios) de los Términos y Condiciones, se adjudica el carácter rector al permitirle al usuario vendedor "incluir textos descriptivos, gráficos, fotografías y otros contenidos y condiciones pertinentes para la venta del bien o la promoción del servicio, siempre que no violen ninguna disposición de este acuerdo o demás políticas de MercadoLibre". De hecho, adiciona que "ninguna descripción podrá contener datos personales o

de contacto, tales como, y sin limitarse a, números telefónicos, dirección de e-mail, dirección postal, direcciones de páginas de Internet que contengan datos como los mencionados anteriormente, salvo lo estipulado específicamente para las categorías: Autos (entre otras)…" aclarando que "en caso que se infrinja cualquiera de las disposiciones (…) podrá editar el espacio, solicitar al Usuario que lo edite, o dar de baja la publicación donde se encuentre la infracción y en ningún caso se devolverán o bonificarán los cargos de publicación" dando testimonio sobre la revisión que aplica sobre las publicaciones, el contacto directo con sus usuarios, el lucro obtenido y la disposición absoluta que conserva -en su poder- sobre todo lo que se publica en el sitio.

Dicho esto, llama aún más la atención que MercadoLibre no permita a los usuarios "comunes" mostrar sus datos en las publicaciones y sí lo haga en el caso de las concesionarias, a las cuales, según el Punto 2 ("Registración"), párrafo segundo, de los mismos términos y condiciones, "podrá requerir una registración adicional (…) como requisito para que dichos Usuarios accedan a paquetes especiales de publicaciones" reservándose "el derecho de solicitar algún comprobante y/o dato adicional a efectos de corroborar los Datos Personales, así como de suspender temporal o definitivamente a aquellos Usuarios cuyos datos no hayan podido ser confirmados…".

Entonces, MercadoLibre podría haber conocido, si lo hubiera querido -en caso que no lo haya hecho-, por ejemplo si se trataba de una concesionaria "oficial", si los bienes existían, si se comercializaban realmente autos de cierta marca, etc. Sin embargo, y en busca del lucro absoluto, se permitió facilitar -si es que sólo facilitó- la estafa a tantas personas. Hoy, para el Sr. Kosten, resulta imposible reclamar a los estafadores dada la negligencia de la demandada o su desinterés por prevenir posibles daños.

Está claro aquí que la demandada abusa de su reconocimiento por parte del público en general para proliferar en un mercado mucho más oneroso que el de los "pequeños bienes". El mercado automotor implica ingresos por publicaciones, ventas y publicidad seguramente millonarios, y la demandada -en busca de ese mercado- deja a los usuarios librados a su suerte. En definitiva, MercadoLibre lucra, no solamente con el espacio que proporciona a los usuarios, sino también con las operaciones que ellos realizan allí, ESPECULA con la concreción de las transacciones, privilegia las más costosas y se beneficia con la publicidad que genera un mayor tráfico de usuarios únicos, lo que la vuelve además referente en el rubro aún para quien no conoce el sitio, por posicionarlo en los primeros puestos de los resultados de buscadores como Google o Yahoo. Obsérvese como, sin perjuicio de los anuncios propios del buscador, MercadoLibre aparece primero en los resultados de búsquedas tan simples como "comprar y vender en internet".De todas maneras y dada la complejidad de demostrar el dolo de la demandada, la responsabilidad aludida debería tener fundamento en el riesgo propio de la actividad, y el beneficio económico empresario, conforme el factor de atribución objetiva previsto por el nuevo art. 1757 del Código Civil y Comercial unificado. Dicho artículo indica que cuando el daño es producido por el vicio o riesgo del bien o servicio, se debe responder.

Inicio 10 de Julio/2018

Activismo Feminista Digital
FUNDACIÓN

Curso Virtual

LAS NUEVAS TECNOLOGÍAS Y LA VIOLENCIA DE GÉNERO ONLINE.

COMUNICAR IGUALDAD

Algunos temas: Gobernanza de Internet.
Libertad de expresión digital.
La mujer víctima de ciberdelitos.
El feminismo en Internet.

INSCRIBITE YA!!!

Costos diferenciales a grupos - Consultar

COMUNICACION
PARA LA IGUALDAD

curso virtual

LAS NUEVAS TECNOLOGÍAS Y LA VIOLENCIA DE GENERO ONLINE

DOCENTE: María Florencia Zerda y Marina Benítez Demtshchenko

INICIO / DURACIÓN: 10 de julio 2018 / 2 meses (8 semanas)

COSTO: 2200 pesos / 110 dólares

CAPACITACIONCOMIG@GMAIL.COM

Comunicalgual · Comunicación para la Igualdad · Comunicarigualdad

El criterio que debe adoptarse para atribuir la responsabilidad no debe basarse solo en la demostración de dolo o culpa sino también en el reconocimiento de la premisa que indica que el negocio que realiza MercadoLibre implica un riesgo, y que como tal debe responder por el daño causado, especialmente en casos como el que nos ocupa atento que la informática es una actividad potencialmente peligrosa, lo que implica una natural aptitud de generar daños de toda índole.

Y aquí coincidimos con el Dr. Shina en que la ley 24.240 unifica el sistema de responsabilidad, superando la división entre responsabilidad contractual y extracontractual (Fernando Shina, “El largo camino hacia la Responsabilidad Objetiva. Homenaje a Roger John Traynor, Juez - Parte 2”, publicado el 06/05/2011, elDial.com - DC15AE). La ley tiene la virtud de crear incentivos que benefician a todos. Ensanchar los límites de la Teoría de la Responsabilidad Civil tiene un inestimable efecto disuasorio de conductas nocivas, lo que se traduce en una fórmula casi matemática que indica que, a mayor responsabilidad del proveedor, menor daño para el consumidor. Los estudios sobre el análisis económico del derecho explican este fenómeno que vincula, bajo un estricto régimen de proporciones inversas, al daño con la responsabilidad civil (Shina, Fernando E., “Consumo on line. Problemática del contrato Informático”, DJ 02/02/2011, 1, con cita de Santos Pastor, en Elementos de Análisis Económico del Derecho. Ed. Rubinzal-Culzoni, año 2004, pág., 102: “El sistema de responsabilidad civil ha experimentado cambios extraordinarios en los últimos 40 años. Si su función histórica consistió fundamentalmente en proporcionar un mecanismo de compensación a favor de las víctimas y en disuadir actividades dañosas, la primera función (compensación) no parece ser hoy tan importante. Hoy la función fundamental de ésta parece ser, en la medida en que esté a su alcance, la creación de incentivos para la mejora de la seguridad y para la eliminación de los riesgos”).

En definitiva, entendemos que “el daño producido en ocasión del servicio de Internet debe ser reparado por quien lo produjo y por quien facilitó que el mismo se produzca… cuanta más tecnología se proponga utilizar para el beneficio del hombre, -sea en Internet, sea en las antenas de celulares, etc- o cuanto más peligroso sea el producto o servicio que brindamos, mayor será la necesidad de ejercer cuidado para evitar que el usuario consumidor sufra un daño. El principio precautorio representa el derecho y la obligación que poseen tanto el Estado como los particulares de adoptar medidas para evitar o disminuir un posible daño grave e irreparable provocado por una actividad o proyecto a realizar…” (Granero, Horacio - elDial.-com - DC1CE8).

O como ya ha dicho la jurisprudencia sobre MercadoLibre, "se debe entender que la demandada no está excluida de la categoría de proveedor. Por lo que está obligado frente a los actores hasta el momento mismo en que éste haga efectiva la prestación que le es debida. Ello implica que responderá en caso de que la prestación no llegue a cumplirse. Sin perjuicio de conservar para si las acciones de regreso, que estime le corresponda, contra todas las personas que participaron en el acto jurídico objeto de litis" (conf. Exp. 36440/2010, "C., E. M. y Otro c/ MercadoLibre S.A. s/ Daños y Perjuicios", CNCIV, SALA K, 05/10/2012).

*Dr. Christian H. Miller. Abogado (UCA). Socio en MCI Abogados. Asesor Jurídico de 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 tecnología. Especialista en Derecho de la Alta Tecnología (UCA)

BLOCKHAIN: TECNOLOGIA PARA REDUCIR LA BRECHA DEL FRAUDE

Capitulo 1

Autor: Dr. Emanuel Ortiz (Colombia)

Para comenzar hablando de blockchain debemos primero abordar la importancia de [1]Bitcoin la cual representa hoy por hoy la criptomoneda más popular, sin embargo para muchos se ha convertido un dolor de cabeza debido a su masiva e impactante entrada en el 2009, [2]Satoshi Nakamoto cuando diseñó la criptomoneda pudo haberla creado para reducir brechas entre el dinero físico al dinero virtualizado, sin embargo no es todavía claro este argumento; debido que bitcoin se ha utilizado de manera inadecuada para otras actividades que permiten pensar lo contrario; y en lugar de disminuir la brecha, posiblemente la han aumentado.

Bitcoin desde sus inicios estuvo al tanto de sinnúmero de relaciones entre la criptomoneda más bursátil y el método más seguro para transferir o intercambiar dinero virtual; en la actualidad Paypal o western union han logrado acaparar los métodos de pago virtual tradicionales, sin embargo, su común uso, puede llevarnos a pensar de que estas dos grandes compañías ya no tienen las mismas ventajas competitivas. En este mismo sentido la tarea de de comprar servicios en la nube, servidores en el extranjero, servicios de hacking, free selling, y porque no ir al market de darkweb y comprar software malicioso para atacar sitios web, ya no es necesario depender del tercero para realizar

---

1El bitcoin (signo: BitcoinSign.svg; abr.: BTC, XBT)3 es una criptomoneda, sistema de pago y mercancía. El término se aplica también al protocolo y a la red P2P que lo sustenta, y de forma común se denomina como una moneda digital. Concebida en 2009,7 se desconoce la identidad última de su creador o creadores, apareciendo con el seudónimo de Satoshi Nakamoto.

2**Satoshi Nakamoto** es la persona o grupo de personas que crearon el protocolo Bitcoin y su software de referencia, Bitcoin Core. En 2008, Nakamoto publicó un artículo[12] en la lista de correo de criptografía metzdowd.com[3] que describía un sistema P2P de dinero digital. En 2009, lanzó el software Bitcoin, creando la red del mismo nombre y las primeras unidades de moneda, llamadas *bitcoins*.

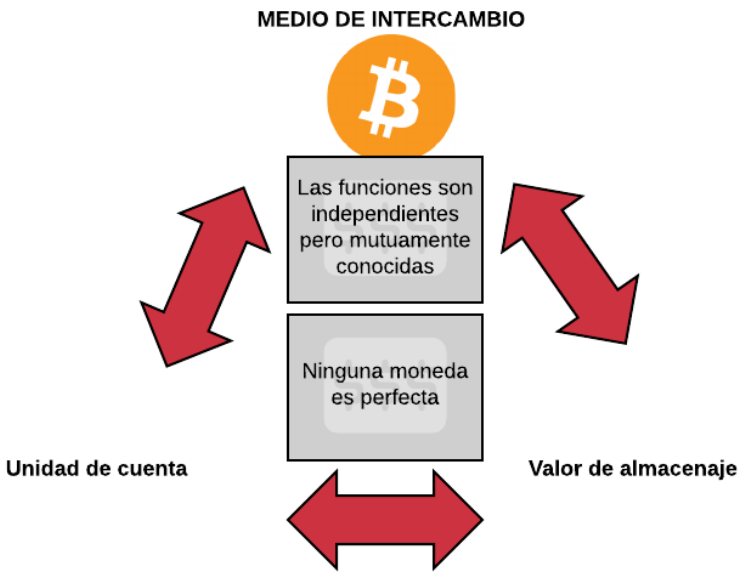
citadas transacciones , si no que dependen del buen o incorrecto uso de la criptomoneda.

Esta relación que tiene bitcoin con el uso indebido permite evaluar su pertinencia; para esto se debe examinar las ventajas que permite realizar en su etapa de intercambio y el modelo que Satoshi Nakamoto pensó para reducir tangencialmente la brecha de crear un criptosistema adecuado, seguro, confiable y que se aleje de la permeabilización del intento de fraude financiero.

Actualmente BItcoin, puede utilizar métodos de intercambio en los caules permita facilitar esta brecha transaccional; sin embargo se debe asegurar primero que todo un método de intercambio que facilite el tipo transacciones de una manera confiable desde su anonimato. Este sistema confundido por otros, puede confundirse como un método inseguro, sin embargo no pretende establecer como tercero de confianza o buena fé (una entidad financiera) si no por el contrario, permite facilitar un sistema bidireccional o directo en dos vías descrito de esta manera para brindar confianza; ofreciendo otro tipo de transacción.

Con el ciberataque al sistema financiero realizado a [3]equifax, uno de los mas grandes

ejecutado al método transaccional que tienen los emporios más importantes y destacados del sector; se sobrevaloraron las acciones sobre el Bitcoin y sobre el uso de las criptomonedas más conocidas como Bitcoin; en ese sentido los 143 millones de personas que perdieron credibilidad sobre el emporio financiero contribuyeron en buscar rutas alternativas de generar transacciones seguras a través del método de cadena de bloques “Blockchain”, por ende toda esta revuelta en materia de ciberseguridad fijó un antes y un después en el entendimiento del Bitcoin y porque no, en el uso del sistema descentralizado o distribuido financiero.



Gráfica de Intercambio:

3**Equifax Inc.** es una agencia de informes de crédito al consumidor . Equifax recopila y agrega información sobre más de 800 millones de consumidores individuales y más de 88 millones de empresas en todo el mundo. Fundada en 1899 y con sede en Atlanta , Georgia , es una de las tres agencias de crédito más grandes junto con Experian y TransUnion (conocido como los "Tres Grandes"). [4] Equifax tiene ingresos anuales de $ 3,1 mil millones y más de 9,000 empleados en 14 países. Se encuentra en la Bolsa de Nueva York como EFX.

El método de intercambio que utiliza Bitcoin posee ciertas características esenciales, una de ellas, se trata de simplificar los tipos de transacciones de volvernos tridireccionales a bidireccionales mediante la formula tradicional que existía en la antigüedad, así:

Así mismo este tipo de intercambio generó inconvenientes en la parte contable como se presentó multiples problemas en materia de contabilidad y donde apreció una de las tipologías más comunes dentro del fraude como lo fue la ***doble contabilidad.***

Método transaccional de divisas actual en el área mercantil y financiero:

Estos componentes dieron origen al Banco Italiano [4]Meidci y uno de los precursores en temas bancarios como el banco [5]ABN de Amsterdam, Holanda. En este sentido ocurrió la primera falla en el sistema bancario llamado (SPOF), en ingles Single Point of Failure, esto sucede cuando un compoennte en el sistema de hardware o software deja inoperante el sistema completo.

Este tipo de riesgos transaccionales no han sido los únicos en lo que tieen que ver con sistema financiero tradicional, en ese sentido se han presentando muchos incidentes en materia de seguridad informática y ciber ataques a infraestructuras que han provocado la facilitación del fraude en el “libro mayor”, del cual se concibe un riesgo mayor.

Si bien es cierto que se ha concebido una apreciación indebida de Bitcoin y por que no de todo el componente tecnológico que lo representa, pero esa inadecuada apreciación se ha venido culturizando en varios sectores por la comprensión inacabada de su forma de funcionar; en este sentido Blockchain puede no solamente, permitir una flexibilidad de naturaleza confiable, si no la pertinencia adecuada para la valoración de un riesgo menor.

Actualmente en el sistema financiero común conocemos los riesgos que pueden existir en cuanto a su funcionamiento, en estos se destaca, el riesgo sobre los depositarios, riesgo del emisor, riesgo de crédito, riesgo operativo, entre otros. Sin embargo Blockchain ha intentado

---

4En el sentido moderno del término, la banca tuvo sus inicios en Italia, en las ricas ciudades del norte de Italia, como Florencia, Venecia y Génova, a finales del periodo medieval y principios del Renacimiento. Las familias Bardi y Peruzzi dominaron la banca en la Florencia del siglo XIV y establecieron sucursales en muchas otras partes de Europa.[1] Quizás el banco italiano más famoso fue el Medici, fundado por Juan de Médici.

5El desarrollo de la banca se propagó del norte de Italia a toda Europa y tuvieron lugar varias innovaciones importantes en Ámsterdam durante la República de los Países Bajos en el siglo XVI, así como en Londres en el siglo XVII. Durante el siglo XX, el desarrollo en telecomunicaciones e informática llevaron a cambios fundamentales en las operaciones bancarias y permitieron que los bancos crecieran dramáticamente en tamaño y alcance geográfico. La crisis financiera de fines de los años 2000 ocasionó muchas quiebras bancarias, incluyendo a algunos de los bancos más grandes del mundo, y generó mucho debate sobre la regulación bancaria existente.

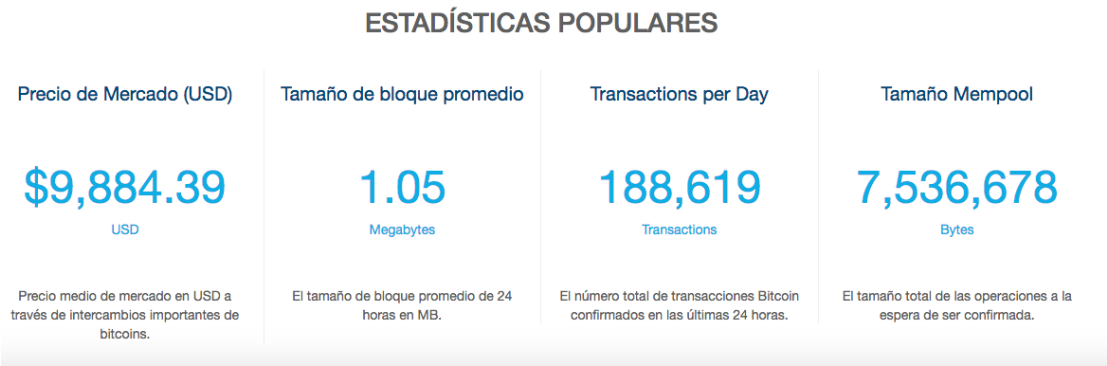
reducir la brecha sobre ese riesgo y además de eso revisar el modelo transaccional de intercambio de divisas a partir de un modelo en seguridad muchísimo más confiable, No repudiable, sin intermediario y con el ahorro de los costos en materia de impuestos.

Verificación y autenticación de una transacción en Blockchain:

Desde la caída y estampida interbancaria lehman brothers en el 2008 la situación no ha sido la misma en materia financiera, quizás las apariencias en seguridad tecnológica no han superado los niveles de veracidad aplicados actualmente al sistema financiero centralizado; sin embargo Blockchain ofrece nuevas expectativas en este tema por medio del intercambio seguro de divisas, y a partir de este, un modelo de transparencia y confiabilidad financiera.

El aspecto reductor no se convierte en una necesidad por parte de las entidades financieras, sin embargo tampoco puede ayudar a confiabilizar las transacciones por medio del uso punto a punto de la transacción sin utilizar una “centralización” de un libro mayor, sin embargo no es muy bien acogido en el sector porque elimina el intermediario que concibe la autorización del movimiento financiero.

La verificación de la confiabilidad de la transacción se puede hacer de muchas maneras, sin embargo las más utilizada es utilizando un código pseudoaleatroio y seguro para generar autenticidad para iniciar una transacción; este se trata de un hash (Un calculo algorítmico) para identificar el origen de la transacción, una vez se autentica este sistema (*ver video: https://www.youtube.com/watch?v=kh43-cC42-o&feature=youtu.be*) mediante una plataforma blockchain se diligencia los datos y cantidad a transaccionar y se ejecuta la transacción. Una vez realiza esto el medio origen tiene una confirmación temporal de la transacción en BTC y en el transcurso de varios segundos se confirma la transacción con los mismos medios de autenticación y no repudio por medio del criptosistema.

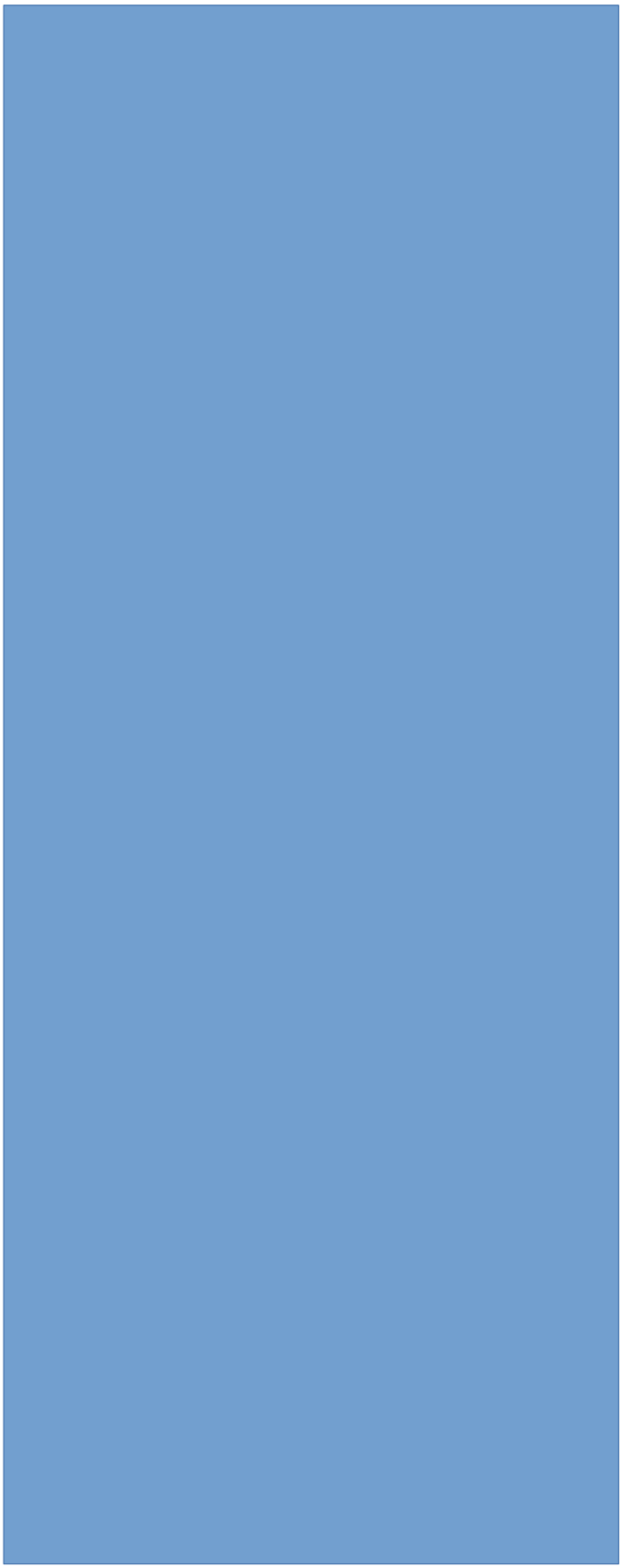


Actualmente la valorización del Bitcoin ha estado varias veces en el tope de inversión; por ende Blockchain hoy se puntualiza en el sentido más popular como medio de pago actualmente:

Figura 3: Tomada como captura de pantalla https://blockchain.info/es/charts

La anterior figura muestra la popularidad que el precio del mercado asciende a 9,884.39 dolares y su tamaño de bloque promedio puede alcanzar el 1.05 de longitud en megabytes; esto indica que a pesar de la complejidad de su sistema interno de uso y su masiva propagación en la red, propende por ser uno de los más usados para la generación y criptomonedas. Como lo señala la gráfica las transacciones en blockchain deben ser confirmadas por medio de la autenticación “Hash” que le permite al usuario financiero la verificación de que su BTC ya esté en billetera virtual.

Por lo anterior y muchas cosas, actualmente es usado Blockchain, y a pesar de su modo de interacción con el mundo virtual, hoy por hoy suele ser uno de los conceptos más cercanos a la reducción del fraude o el uso de tipologías de criminalidad financiera. Por tanto esperemos que su método siga fortaleciéndose para llevar acabo fortalecimiento en transacciones actuales y permita al usuario de la banca facilitar y asegurar cada vez más sus datos y su dinero.



El valor de la pericia informática en el ámbito judicial

En el último tiempo mucho hemos escuchado sobre la "pericia informática" y el valor que tiene en el proceso judicial. Cámaras, teléfonos celulares, computadoras, entre otros dispositivos, se han vuelto fundamentales para echar luz sobre un hecho o acto delictivo. ¿Cómo hacen esto los peritos informáticos?

La revolución tecnológica ha llegado, y desde hace ya un tiempo venimos siendo testigos de un importante proceso de penetración de la informática, la tecnología y los datos digitales en la vida cotidiana de las personas. Es una realidad que ya nadie cuestiona el hecho de que gran parte de nuestras actividades queden registradas en algún medio tecnológico: computadoras, cámaras digitales, dispositivos móviles y celulares, entre otros.

Pero, **¿cómo llega esto a volverse concluyente para la resolución de un delito? ¿Cómo se convierte en una prueba digital?** Aquí, la labor del perito informático forense cumple un rol crucial.

Una prueba digital se puede definir como todo dato no tangible resguardado en algún tipo de dispositivo de almacenamiento magnético o digital. En el último tiempo, ésta ha sido de sumo valor en la resolución de múltiples causas, permitiendo liberar de culpa y cargo a personas totalmente inocentes, o bien descubriendo la implicación de otras.

La evidencia digital se puede considerar como un tipo de prueba donde los datos pueden ser recolectados, almacenados y analizados con herramientas de informática forense y técnicas especiales. Si la prueba ha sido presentada correctamente y su cadena de custodia no ha sido alterada, puede resultar fundamental para resolver un litigio o delito.

Entonces, nos preguntamos en estos casos **¿cuál es el valor de la pericia informática en un proceso judicial?** Y nuevamente afirmamos que en muchas ocasiones puede ser concluyente para la resolución de cualquier tipo de delito o litigio. Por eso, se vuelve fundamental conocer la cantidad de dispositivos tecnológicos que se encuentran vinculados al hecho o acto delictivo.

Si el hecho en cuestión se trata de un delito informático, a través de la pericia informática puede llegar a encontrarse toda la evidencia. Ahora bien, si estamos ante un delito en donde la tecnología se utilizó como "medio para" entonces la resolución del mismo dependerá de la utilización que se haya hecho de ella.

En ambos casos, el tiempo transcurrido entre el hecho y la intervención de un perito informático forense que lleve adelante el análisis de los dispositivos es fundamental para obtener y resguardar la pericia informática, así como el método utilizado, evitando que se llene de nulidad la prueba o evidencia digital.

Por eso, una vez más es importante conocer cómo se realizan las pericias informáticas. En primer lugar, es útil saber que se ejecutan preservando todo el material informático: computadoras, teléfonos celulares, cámaras, filmadoras, GPS, y todo elemento que pueda ser de valor para la causa.

Una vez preservado esto, se extrae la información con herramientas de informática forense y técnicas especiales. Para la búsqueda de resultados, se realiza un análisis de la información obtenida según las pautas solicitadas por las partes (juez, fiscales, querellantes, etc.). Los resultados pueden arrojar elementos claves del delito o litigio que permitan resolver la causa, o bien puede no encontrarse nada y aún así la pericia sirvió justamente para demostrar esto.

También, otros elementos probatorios son los chats, redes sociales, correos electrónicos, entre otros. Aquí también actúa **el perito informático forense** para **buscar el intercambio que se**

haya mantenido por cualquiera de estos medios.

Dependerá del expertise de quien se encuentre a cargo de los dispositivos o medios digitales, el dejar huellas o no sobre el hecho cometido. En muchos casos, se utilizan encriptaciones o borrados que hacen muy difícil la tarea de encontrar “huellas”; pero, en otros, el recupero de la información y la actividad del dispositivo puede ayudar a los investigadores a armar una línea de tiempo con los hechos sucedidos.

Nunca debemos olvidar que todas las acciones que realizamos dejan una “huella” en algún medio digital.

Por el Ing. Pablo Rodríguez Romeo (MP 49452 - MN 5117) – Perito Informático Forense, especialista en Seguridad - Socio del Estudio CySI de Informática Forense – www.cysi.com.ar

Acerca de CySI

CySI es un Estudio de Informática Forense especializado en el Peritaje Judicial, integrado Peritos Informáticos Forenses con más de 15 años de experiencia en el ámbito legal argentino. Su misión es colaborar con abogados, jueces y organizaciones para recuperar y preservar datos electrónicos de importante validez para posibles procesos judiciales, capacitándolos en las cuestiones técnicas que implican.

Más información: www.cysi.com.ar

El derecho preventivo es el deber ser jurídico. EL AUTOR

EL DERECHO PREVENTIVO PARA LA VALIDEZ DE LA PUBLICIDAD DIGITAL Y LA EFICACIA DEL DERECHO DEL CONSUMO

Por: Camilo Alfonso ESCOBAR MORA[6]

En este artículo se consagran los fundamentos principales de mi doctrina de derecho preventivo para el aseguramiento de la eficacia, formal y material, de las normas del régimen publicitario (general) de las relaciones de consumo que se presentan en medios digitales. Las relaciones de consumo son las que tienen en un extremo a una empresa y en el otro uno o varios consumidores. Esto delimita el campo de aplicación del derecho del consumo. Solo procede en dichas relaciones.

La publicidad es cualquier clase de actuación humana que promueva el consumo de los productos de una empresa. Lo importante es que esa persuasión sea válida, jurídicamente. Se puede hacer cualquier clase de publicidad siempre que se protejan los derechos del consumidor a la información, a la calidad de los productos, al tratamiento adecuado de sus datos personales, a la presentación de mensajes que no lesionen sus prerrogativas jurídicas (ni las de ningún otro grupo de interés involucrado) y al cumplimiento del vínculo contractual que pueda derivarse de una publicidad.

La publicidad presentada en medios digitales goza de pleno reconocimiento y sometimiento jurídico. Su fondo sigue siendo

---

6Profesor, Conferencista y Doctrinante de Derecho Preventivo para la Eficacia Jurídica del Derecho a Recibir Información que tiene el Consumidor frente a la Publicidad Digital ©. Fundador de JURÍDIA®, Centro de Investigación de Derecho Preventivo del Consumo en la Publicidad Digital www.juridia.co. Contacto gerencia@juridia.co.

publicidad (y las formalidades que le apliquen dependerán de cada caso, según el mensaje o mensajes involucrados), simplemente que el medio se cataloga (de conformidad con esta norma) como un mensaje de datos. Lo relevante es que su contenido sea válido en los términos propuestos en este texto.

La empresa debe asegurar que éstos derechos sean eficaces. No es acertado restringir la actividad publicitaria mediante un control público de legalidad ex-ante que tenga una dimensión arbitraria. No aplica un principio de precaución en este objeto. Por el contrario, se permite y promueve al ser un medio de información en el mercado. Lo determinante es que la empresa sea diligente en la elaboración y presentación del mensaje. En definitiva, que asegure que su publicidad es válida. La validez significa que sea conforme con las normas que apliquen de acuerdo a la clase de mensaje y de producto (bien o servicio) que estén presentes. En cuanto al mensaje, se hace referencia a que cumpla los deberes de información que apliquen según el sector y modalidad publicitaria empleada. En relación al producto se deben ofrecer productos cuya comercialización esté permitida (y que solo se promocionen ante los consumidores que tengan capacidad legal para adquirirlos), que sean de calidad y que se entreguen de acuerdo a lo indicado en la publicidad. Si esa validez se logra la consecuencia es la eficacia del régimen (el goce material de los derechos del consumidor).

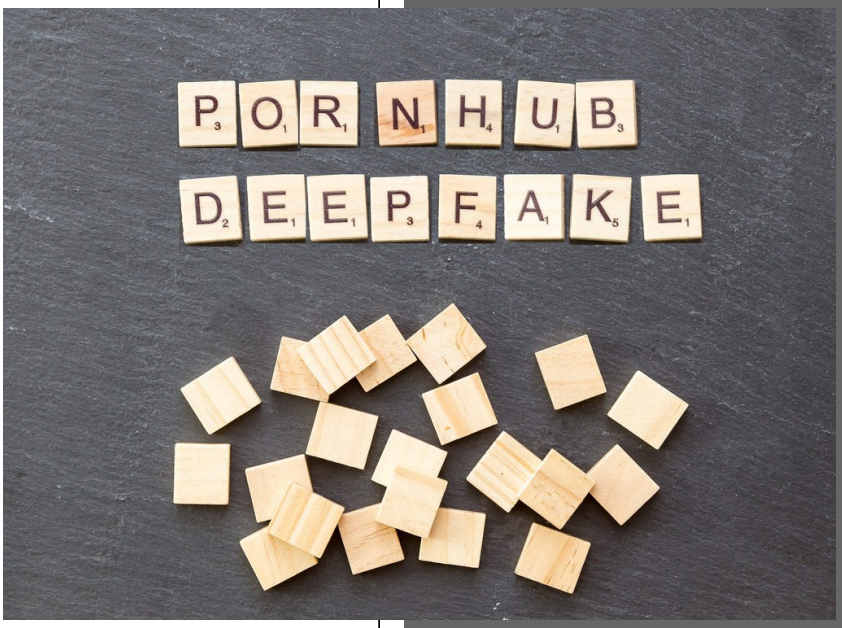
En la práctica, la validez se puede afectar por una visión del derecho meramente formal. Nada se gana con documentos estáticos. Lo importante es que se gocen los derechos y cumplan los deberes, por parte de cada sujeto u organización involucrada en el caso (que tanto la empresa como sus grupos de interés gocen sus derechos y cumplan sus deberes). En ese orden, la validez depende de la instrumentalización material de las normas, a la medida de las variables que estén presentes. La autorregulación es la respuesta. Lo que sucede es que ciertas connotaciones de la autorregulación pueden conllevar a remedios más graves que las enfermedades. No es un neoliberalismo ni una anarquía. Es construir embudos, donde las normas generales y especiales se aterricen y cumplan, según cada situación. Se trata de una autorregulación válida, conforme con el Estado de derecho que sea vigente. La denotación jurídica de la autorregulación es que se diseñen soluciones para cumplir las normas que imperen (bien sea por mandato de normas abstractas o por actos dispositivos válidos de las partes) en un asunto específico. Ese es el axioma para producir teoremas (de autorregulación) idóneos.

En eso consiste el derecho preventivo que se sugiere. Es un medio (ser) que contiene y hace efectivo (es decir: eficiente y eficaz) a las normas que sean procedentes (deber ser) en el caso. En relación con la publicidad, se trata de crear piezas que permitan que el consumidor (receptor) goce de su derecho a una información lícita, suficiente, veraz y oportuna frente al mensaje o mensajes que transmita la obra publicitaria.

La diligencia (mercantil) para la atención de este deber depende del estado del arte que se encuentre vigente. La empresa responde por lo previsible, y la única forma de excluir su responsabilidad es lo que le resulte irresistible. Como la diligencia a cargo de la empresa es especial, al ser de naturaleza mercantil, la regla general es que debe actuar con profesionalismo y ello implica que lo irresistible debe ser algo que en el estado del arte de su mercado o campo de acción interno no sea previsible o controlable. En el campo de la publicidad, el estado del arte permite que se usen los medios digitales de una manera personalizada para el consumidor, según su perfil y demás variables que permitan la precisión del mensaje para el receptor. La inteligencia artificial hace que los sistemas de información digitales reconozcan datos (personales, organizacionales o del ambiente implicado) y presenten soluciones de acuerdo a dichos insumos. La empresa que incrementa los riesgos o amenazas por omisión del uso del estado del arte es negligente. En la publicidad dichos riesgos son el aumento de las posibilidades de incumplimiento normativo, que le pueden generar al consumidor incomprensión, incumplimiento o engaño, bien sea por vicios de vaguedad o de ambigüedad en el mensaje. Lo diligente es hacer una publicidad que use las bondades del estado del arte para que las normas que apliquen sean eficaces en la práctica. La innovación no es un valor agregado, es el ejercicio del deber de diligencia.

Como la realización de una publicidad válida implica diversos espacios de interacción con el consumidor, la empresa debe diseñar soluciones de derecho preventivo para cada variable, según las circunstancias de cada caso. Por ejemplo: hardwares de calidad, softwares idóneos, redes seguras, contenidos digitales comprensibles y eficaces para el consumidor, formatos de autorización para la recolección y uso de los datos personales del consumidor,

sistemas que aseguren pruebas pertinentes y conducentes sobre las autorizaciones otorgadas por el consumidor y los actos de diligencia realizados por la empresa, políticas de tratamiento de los datos personales, protocolos jurídicos de seguridad de la información, documentos de fundamentación jurídica para la clasificación y uso de la información corporativa, personal y del sector público, contratos con los trabajadores, proveedores y aliados que aseguren el cumplimiento de las publicidades que tengan la forma de oferta y sean aceptadas por el consumidor, sistemas de buenas prácticas de protección al consumidor en medios analógicos y digitales, y modelos organizacionales de capacitación permanente sobre derecho preventivo a todo el grupo de trabajo interno y externo (pues ambos pueden interactuar con el consumidor).



La empresa es un medio de desarrollo si su estructura es válida y logra, comercializa y promueve un producto que respete (formal y materialmente) los derechos del consumidor y de los demás grupos de interés involucrados en el caso. La publicidad es el reflejo de la diligencia (mercantil), tanto en las relaciones jurídicas previas en materia de obtención y distribución del producto como en las posteriores en cuanto al consumo del producto. El derecho preventivo es un generador de calidad de vida.

Escuela de privacidad

Visitenos: Cra. 7B Bis No. 126 – 36 Bogotá
Llamenos: (57- 1)489 86 87 – 318 407 66 55
Escribanos: contacto@escueladeprivacidad.com

¿Estamos preparados para la deepfake?

Autor: Sebastián Gamen

El fenómeno de la deepfake aparece a finales del año 2017 cuando un usuario anónimo apodado justamente como "deepfake" publicó varios videos pornográficos en Reedit. En uno de ellos se veía a la actriz Gal Gadot con su hermano manteniendo relaciones, cuando en realidad eran dos actores y el rostro de la mujer había sido reemplazado por el de la actriz. Las imágenes llamaron la atención por la perfección y su realismo. Otras personalidades perjudicadas fueron Emma Watson, Katy Perry, Taylor Swift, Scarlett Johansson y hasta la mismísima Michelle Obama. A partir de allí se llama deepfake a la inteligencia artificial que permite cambiar un rostro por otro, o incluso permite recrear discursos utilizando la voz de la persona y adulterando los movimientos de labios para un realismo total.

Esta tecnología llama la atención en dos aspectos preocupantes. El primero, es la perfección del resultado final. La segunda, es que esta tecnología está disponible al público y su acceso es relativamente fácil. La conjunción de esto es realmente grave, no solamente por la posibilidad de cambiar discursos, o generar noticias falsas sino porque leyes nuevas ya tienen olor a viejo.

Hace pocos días se divulgó con bombos y platillos la ley que condena la tenencia de pornografía infantil y me pregunto cómo afecta esta tecnología a ese delito.

Antes de responder, quiero hacer un breve resumen de lo ocurrido en EEUU. La sección 2256 del Título 18 del Código de los Estados Unidos define pornografía infantil como cualquier representación visual de una conducta sexual explícita que involucre a un menor, categorizando a éste como a una persona con menos de 18 años de edad. Cuando se hablaba de representación visual se incluía a fotografías, videos, y también a las imágenes generadas en forma digital o por computadoras indistinguibles de un menor real, como así también a las imágenes creadas, adaptadas o modificadas que parezcan representar a un menor identificable, como lo establecía la Child Pornography Prevention Act de 1996. Se puede observar que una ley de hace 22 años ya contemplaba la posibilidades tecnológicas pero, la Suprema Corte de Justicia de los Estados Unidos, en la sentencia Ashcroft v. Free Speech Coalition dijo que esa definición de representación era muy amplia invalidándola, como así también dijo que no era constitucional la inclusión de imágenes

generadas por computadoras dentro del concepto de pornografía infantil.

Por nuestra parte, el artículo 128 del Código Penal de la Nación Argentina dice que "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores".

En la interpretación de este artículo hay dos posturas. Por un lado quienes interpretan el término "representación" de acuerdo al artículo 2 inciso c) del "Protocolo facultativo sobre la venta de niños, la prostitución infantil y la utilización de niños en la pornografía" que exige que la representaciones de un niño dedicado a actividades sexuales explícitas o sus partes genitales sean reales. Por el otro lado, ubicamos a quienes tienen una interpretación amplia de la palabra incluyendo imágenes virtuales de menores de edad, hasta incluso animes o mangas pornográficos. Esta interpretación tan amplia parecería chocar de frente con la novísima incorporación al código penal que condena la simple tenencia de pornografía infantil. Es decir, una persona que tenga guardados en su computadora dibujos animados de pornografía infantil podría ser condenado. Ello, aún cuando no haya menores reales involucrados y cuando no hay estudios contundentes que demuestren que el consumidor de pornografía infantil virtual quiera luego consumir real, o que sienta una propensión por abusar o cometer abusos sexuales en menores reales. Es decir, se lo condenaría por un peligro abstracto.

Está vigente la discusión sobre la porno venganza (disiento en la denominación) y existe consenso en castigarla penalmente. La porno venganza o *revenge porn* es la distribución no consentida de imágenes pornográficas o de desnudez de otra persona.
Sin embargo, al momento de buscar soluciones a este problema las voces que se escuchan más alto pecan de ingenuidad o de ignorancia.
Cualquiera de los dos supuestos son muy peligrosos y pueden engendrar una ley que no sirva para mucho, desampare y desanime a las víctimas de estos delitos.
El proyecto de ley que más avanzó en el Congreso es el que trascribo a continuación, obteniendo media sanción en el Senado de la

Nación. Este proyecto incorpora el artículo 131 bis al Código Penal el que dirá que “Será reprimido con la pena de prisión de seis (6) meses a cuatro (4) años, el que hallándose en posesión de imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas, las hiciere pública o difundiere por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos, sin el expreso consentimiento de la o de las mismas para tal fin, aun habiendo existido acuerdo entre las partes involucradas para la obtención o suministro de esas imágenes o video. La persona condenada será obligada a arbitrar los mecanismos necesarios para retirar de circulación, bloquear, eliminar o suprimir, el material de que se tratare, a su costa y en un plazo a determinar por el juez”.

Lo primero que debemos tener en cuenta al legislar este tipo de conductas es que el daño ocasionado a la víctima es grande y muy serio, basta recordar el caso de la italiana Tiziana Cantone que decidió quitarse la vida. Por ello, se deben exigir penas graves que realmente disuadan este tipo de conductas. Ello aun cuando se deban respetar los principios y garantías del derecho penal. Penas menores o multas como proponen algunos de los proyectos difícilmente solucionen este problema.

La segunda cuestión que se debe considerar es qué bien jurídico se pretende proteger. Hay proyectos enfocados a la protección de la imagen, otros la intimidad y muchos otros hacen una ensalada con ambos. El proyecto que se analiza aquí se ubica en el Capítulo del Código Penal correspondiente a la protección de la integridad sexual de las personas.

Lo que se menciona tiene una significado importante si se recuerdan algunos antecedentes y si se considera todo el potencial de las tecnologías. En mi opinión el bien jurídico que se debe proteger por sobre cualquier otro es el honor de las víctimas, mayoritariamente mujeres. Basta recordar el video de Wanda Nara, donde nunca se supo exactamente si era ella pero que los rumores sobre su autoría fueron suficientes para causarle un daño enorme. Lo mismo podría suceder si publico una foto de cualquier persona y se la adjudicó a otra mujer. Esto es lo que le aconteció a Jimena Sanchez presentadora de FoxSport. Es decir, para generar un daño no necesariamente tengo que usar la imagen de la víctima. Sobre este último supuesto se podrían dar dos situaciones, una es que no se vea el rostro de la víctima pero se la identifique con su nombre real; la segunda posibilidad es que aun cuando la imagen sea de otra persona la identifico con nombre falso del modo que la

víctima queda representada por ese cuerpo o imagen ajena frente a terceros. En ninguno de los dos casos se usó la imagen de la víctima solo su nombre pero, ¿acaso no se afecta gravemente su honor?

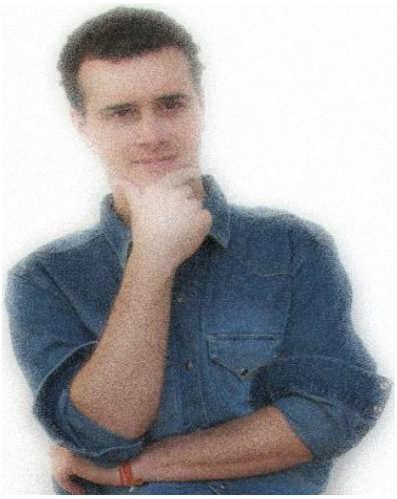
Cuando digo que se afecta el honor de la persona no sería por el contenido de la publicación en sí mismo, porque ya entrados en años en el siglo 21 sabemos que la mujer tiene los mismos derechos que el hombre en vivir libremente su sexualidad, sino por la clara falta de consentimiento en la divulgación de un retrato o video que nació para vivir en la intimidad o por los comentarios injuriantes que las víctimas terminan recibiendo. Hecha esta aclaración queda claro que el sexting no debe penarse y es inocente de todo cargo.

Volviendo a la deepfake, la ley que pretende condenar la porno venganza va a nacer vieja, obsoleta e inservible para proteger la imagen y el honor de la víctima. El proyecto con media sanción en argentina pretende modificar el Código Penal, incorporando penas de 6 meses a 4 años de prisión a quien, hallándose en posesión de imágenes de desnudez total o parcial, o videos de contenido sexual o erótico de una o más personas, las hiciere públicas o difundiere por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otro medio o tecnología de transmisión de datos. Con la deepfake ya no preciso estar en posesión de ningún video íntimo, solo preciso cualquier foto de la víctima para usar su rostro como quiera y hacerle cualquier daño. Bienvenidos nuevamente al mundo de los delitos impunes.

En conclusión, la deepfake nos recoloca en una zona gris legal, nos desacomoda y nos obliga a repensar el derecho para no darle la oportunidad a los delincuentes de seguir haciendo de las suyas.

Introducción al Big Data. Una mirada analítica de lo que hay detrás

Autor: Isidro Morganti Hernández[7]



La problemática que voy a exponer tiene, al igual que la mayoría de los temas que comprende el Derecho Informático, un padecimiento en su origen: la falta de exploración, el desinterés y, tal vez, el miedo a investigar y preguntar sobre lo que se desconoce. No obstante, gracias a profesionales especializados en la Informática y en esta tan especial rama del Derecho, aquellos que somos inquietos podemos compartir en espacios como este, la poca, suficiente o mucha información digerida que tenemos y, desde ya, aprovechar la ocasión para dar nuestra humilde opinión.

Habiendo mencionado, en otra oportunidad[8], los típicos casos que acontecen con cierta asiduidad desde hace años, ahora corresponde abordar un tema que nos invade a todos y a cada uno de los usuarios de bienes y servicios multimedia en este siglo.

La temática a la que me refiero es el Big Data. Sin definirlo, en una primera aproximación rudimentaria puedo afirmar que es como el oxígeno que está en el aire: está, pensamos y sabemos que existe (aunque tal vez no todos le den ese nombre), pero nos cuesta verlo, descubrirlo. Me sentí motivado a escribir sobre este asunto luego de leer una impecable publicación de Juan Cruz González Allorca y Esteban Ruiz Martínez titulada “Big Data: riesgos y desafíos en el tratamiento masivo de datos personales”[9]. Tal como allí mencionan dichos autores, “la actividad informativa actual

---

7 Abogado egresado de la Facultad de Derecho de la Universidad Nacional de Rosario. Diplomado en Derechos Económicos Sociales y Culturales por la Universidad de la Patagonia San Juan Bosco. Ex integrante de la Cátedra de Derecho Político de la UNR. Cualquier consulta o inquietud se me puede contactar en LinkedIn

8 MORGANTI HERNANDEZ, Isidro. *“Responsabilidades civiles y penales en la web: tres fallos relativamente recientes que prometen instalarse”*, Revista Digital El Derecho Informático, Ed. Nº 27. Septiembre, 2017. https://issuu.com/elderechoinformatico.com/docs/revista_27/23

9 GONZÁLEZ ALLONCA, Juan Cruz y RUIZ MARTÍNEZ, Esteban. *“Big Data: riesgos y desafíos en el tratamiento masivo de datos personales”*, *Nota a fallo* publicada en diario La Ley. Buenos Aires, 24/6/2016. Cita online: AR/DOC/373/2016.

desarrollada a través de informática aplicada a dispositivos e Internet, está convirtiendo la realidad concreta en virtual, reflejando a las personas como un conjunto complejo de datos conformando un 'yo virtual' de gran trascendencia a los fines relacionales, en particular para la actividad económica del individuo". Esto es así, me atrevo a decir, desde la llegada del nuevo milenio, solo que en la última década los avances sorprenden a paso cada vez más agigantado. La afirmación de los autores se erige como una verdadera radiografía de la realidad. En efecto, si buscamos trabajo tenemos disponibles plataformas como *LinkedIn* donde podemos – además de postularnos con nuestro CV como sucede en *Computrabajo*, *Bumeran*, *Zona Jobs*, *Jobomas*, *Trabajando* –, desarrollar nuestro perfil profesional de manera online, agregar contactos, hacer publicaciones, etc. Pero si lo que estamos buscando es compartir efímeramente contenidos con otras personas tenemos *Snapchat*, si solo queremos subir fotos, *Instagram* lidera hoy el mercado, si nos interesa describir brevemente acontecimientos, a nuestro alcance está *Twitter* y si hacemos todo lo anterior o un poco de cada cosa todavía nos queda *Facebook*. Considero que la posibilidad de crear un único "yo virtual" se extinguió desde el momento en que se crearon y tuvieron buena llegada en la sociedad todas estas redes que se autocatalogan para determinados usos, lo que ha dado lugar a una multiplicidad de 'yoes virtuales'. Hace poco llevé a cabo una encuesta de manera absolutamente informal – espero que el lector aprecie mi sinceridad –, tomando como público a todas las personas de mi entorno (familiares, amigos y conocidos allegados) para saber qué redes sociales usan más en orden a determinar, posteriormente, qué cantidad y calidad de datos personales vuelcan en la nube. Obtuve el siguiente resultado:

-Todos los encuestados utilizan con cotidianeidad al menos tres redes sociales, una de las cuales es Facebook;

-Las dos redes restantes se debaten entre usuarios que las usan en parejas siendo las más destacadas las duplas de *Twitter* e *Instagram*, *Twitter* y *LinkedIn*, *Snapchat* e *Instagram*;

-Cabe destacar que la franja etaria de 20 a 30 años tiene perfiles creados en portales de trabajo como *Computrabajo*, *Bumeran* y *Zonajobs*.

Con esta encuesta comprobé mi hipótesis acerca de que tenemos un sinnúmero de "yoes virtuales". Vivimos conectados, y ello no escapa a la actividad económica, sino que todo lo contrario. Aun cuando solo tuviéramos una cuenta en una sola red, tendríamos un "yo virtual" que construiríamos día a día, minuto a minuto. Cada "yo virtual" creado significa un flujo constante de datos, información directa que proporcionamos voluntariamente o respetando los asteriscos colocados en los campos "obligatorios" de los formularios de registro, así como también cada cosa que publicamos…Además de eso, se crea un flujo de datos entre el dispositivo que usamos para acceder a tal o cual red y la red misma y su base de datos.

El artículo doctrinario que estoy comentando apunta al análisis concienzudo que debe hacerse del tratamiento deficitario de nuestros datos personales. Datos personales vienen a ser, como expuse en el párrafo anterior, no simplemente los que se requieren al momento de crear un perfil en cualquiera de estas redes sino también toda la información que nosotros mismos y nuestros dispositivos vuelcan en la web. Y en este punto está la puja: "Los medios informativos pretenden saber lo más posible sobre las personas, mientras que el titular del dato pretende ejercer libremente y sin interferencias todas sus libertades" [10]. Aquí se ve el choque constante que hay entre ambos polos. Resulta que, para estos medios la persona es un objeto de conocimiento, lo cual no puede ni debe ser sino únicamente cuando se trate de derechos que ya sea el Estado u otros particulares tengan a saber de ella. Como bien manda el principio constitucional de exterioridad establecido en el art.19 de nuestra Carta Magna "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero están solo reservadas a Dios y exentas de la autoridad de los magistrados"[11].

Hoy día hay una clara y notable injerencia en los derechos de las personas a preservar su intimidad, a mantener su esfera privada inviolable, a estar solas, a no ser seguidas ni perseguidas, a su libre autodeterminación y a la postre, a su libre albedrío…Los autores de la publicación que comento afirman que hoy "más que nunca debe reconocerse el derecho de las personas a no ser detectadas y/o seguidas, y/o controladas en sus consumos y demás actos salvo que presten su consentimiento con carácter

10Ibídem.
11Art. 19 de la Constitución de la Nación Argentina.

previo"[12]. Hay una palabra que leyendo con moderada fluidez podría pasar desapercibida para el lector en su significancia: *salvo*. Es justo después del *salvo* que se abre el portón y se deja entrar todo lo que, valga la redundancia, en algún punto se pretendía dejar fuera. De tal manera le propongo al lector un breve ejercicio mental: ¿ Suele brindar su consentimiento cada vez que carga una foto, escribe un post, comenta una publicación o emprende cualquier acción en una plataforma 3.0? Una respuesta rápida se escuchará al sonido grave del "no". La verdad es que, aun pensándolo un rato todos diremos que no. Esto es así porque si tuviéramos que brindar nuestro consentimiento una y otra vez en cada oportunidad que efectuamos alguna acción en una plataforma de este tipo probablemente no tendrían ni tanta fama ni tantos usuarios de sus servicios. Otra pregunta: ¿Recuerda el día que creó su cuenta de correo electrónico? ¿Y cuando creó su perfil en Facebook? ¿Y cuando hizo lo mismo en LinkedIn? "Sí, lo recuerdo perfectamente. Era un día soleado cuando decidí quedarme en casa y crearme un usuario en Facebook. El de LinkedIn fue un invierno que quise probar cosas nuevas. El correo electrónico fue por el año 2003, en casa de mi tío. Recuerdo que también imprimí todas las bases y condiciones de uso y las guardo en el primer cajón de mi escritorio, siempre a salvo para mi consulta ante eventuales dudas e interrogantes."[13] La respuesta que más se aproxima a la realidad es que muy probablemente no recordemos el día, podríamos llegar a saberlo si hay datos de registro que sean asequibles en nuestra cuenta como sucede con Facebook, por ejemplo. En cada una de esas oportunidades todos hemos aceptado, tildado casi por costumbre la casilla blanca que espera nuestro "OK" para poder "continuar". Por medio de esa aceptación tan fugaz como es un clic, dimos nuestro consentimiento para todo lo que haríamos con posterioridad a ese instante. Arribamos a este punto porque nos estábamos refiriendo a la injerencia, al control de nuestros consumos y datos, y al peligro de que se hurguetee en nuestra privacidad. El lector no se sorprenderá ya que seguramente lo ha vivenciado al leer que, cuando se ingresa a una de las famosas redes desde un dispositivo que contiene un chip telefónico luego se asocia ese número a la cuenta y se le pregunta al usuario si quiere vincular la cuenta con dicho número: lo cierto es que, el dispositivo, la cuenta y el número ya fueron vinculados, solo que se le pregunta al usuario si quiere hacerlo público. Allí hay una

12GONZÁLEZ ALLONCA, Juan Cruz y RUIZ MARTÍNEZ, Esteban. *"Big Data: riesgos y desafíos en el tratamiento masivo de datos personales"*, *Nota a fallo* publicada en diario La Ley. Buenos Aires, 24/6/2016. Cita online: AR/DOC/373/2016.

13Respuesta de…ninguna persona que conozca o imagine.

Activismo Feminista Digital

FUNDACIÓN

/femhackARG/

/FemHackARG

/femhackarg

https://activismofeministadigital.org/

grave intromisión. De todos modos, la función resulta útil para saber cuando alguien no ıtorizado por nosotros ingresó a nues ıenta desde su celular.

Ya vimos entonces lo que implica el *consentimiento previo* señalado por los autores que, me atrevo a afirmar, fue otorgado hace tanto tiempo que poco recordamos de ese efímero pero trascendental *clic*. Es cierto que las políticas aceptadas hace diez años atrás mutan año a año y, de vez en cuando, se nos notifica a través de una leyenda que casi siempre se manifiesta en una presentación poco atractiva, aburrida, tediosa, que en definitiva no invita a seguir leyendo. Esa lectura que decidimos precipitadamente posponer, o que jamás realizaremos, no es otra cosa que una modificación unilateral – claramente – del gran paquete de políticas de privacidad y tratamiento de la información. Y aquí está la clave: el *tratamiento* de la información. Precisamente, el iceberg al que me estoy dedicando a escribir se vincula a la protección de nuestros derechos en la red y se llama Big Data. Su propio nombre deja entrever que consiste en mucha información; más que información, datos precisos sobre nosotros, los usuarios online.

Los autores cuyo artículo acerca del Big Data estoy comentando lo describen como una tecnología capaz de tratar datos con complejos algoritmos que permiten adquirir nueva ación sobre los individuos. También, ·an que consistiría en un anticipo ndental y clave de lo que se viene en ma de desarrollo de los países, sustentando nuevas olas de crecimiento en la productividad, innovación y excelencia. Luego de esta noticia, no resulta llamativo que año a año queden miles de vacantes para ocupar puestos de programadores en Argentina.En este breve comentario no hago más que girar en torno al epicentro de proteger nuestra identidad e intimidad, de cuidar de nuestra privacidad y de decidir y ser realmente conscientes de qué contenidos compartimos o volcamos en la web, así como de cómo y cuándo lo hacemos. La tecnología del *Big Data* viene a “tratar” nuestra información pero no solo la nuestra sino la de todo el mundo. Escribí tratar entre comillas porque creo que hay un verbo, un tanto más tendencioso pero más preciso: “manipular”. Así como en la gastronomía se manipulan alimentos y existen normas de seguridad e higiene a respetar, el Big Data, cual mayor cadena de restaurantes del mundo, manipula grandes toneladas de información en un proceso donde nada se descarta, que requiere un software y hardware que permitan cumplir este ciclo a la más alta velocidad posible. De ahí que se diga que el Big Data es el rey de las tres V: volumen,

variedad y velocidad de la información. La manipulación de todos estos datos personales de millones y millones de personas es incalculable pero nos permite llegar a comprender, muy a grandes rasgos, que al igual que sucede con las cookies el historial de visitas web, las sugerencias de búsqueda, todo depende de nuestras conductas como usuarios. De tal forma se crean estadísticas, preferencias, se determina la proclividad de cada usuario según su idioma, ubicación geográfica, tipos de contenido que vuelca y comparte en la web; se elaboran índices de probabilidad y luego con esos datos se condiciona al usuario a través de los famosos contenidos sugeridos o publicidades bien direccionadas, pero el control va mucho, mucho más allá...

Los medios periodísticos estadounidenses recientemente han festejado los avances de la tecnología cuando un altavoz inteligente conectado al sistema Google Home interpretó una pregunta subida de tono de parte del agresor a su víctima como una orden: la frase que desató la polémica fue algo así como *"did you CALL THE POLICE??"*. El resultado siguiente significó que el sistema inteligente lo tomara como un mandato y entonces llamó a la policía. Si bien a todos nos alegra que haya habido un final feliz en esa historia, resulta un tanto preocupante la inexistencia de privacidad e intimidad de las personas. A la vez, podría haberse tratado de un chiste y la policía habría movilizado sus recursos y agentes en vano. La noticia se viralizó rápidamente por todo el mundo con todo tipo de redacciones, entre las menos felices "Google se dio cuenta que había una mujer, en peligro, llamó a la policía y dejó el micrófono abierto"… La realidad es que frases semejantes[14] invitan a leer la noticia, comentarla y compartirla con allegados; sin embargo, la realidad es que el sistema tecnológico inteligente de Google Home simplemente lo que hizo fue reconocer mediante la técnica de reconocimiento por voz, la voz de uno de los configurados como dueño de la casa. En ningún momento el software del "departamento inteligente" comprendió ni comprobó que había una situación de peligro para personas dentro de la casa y decidió autónomamente llamar a la policía y "dejar el micrófono abierto". La verdad es que el sistema pre configurado para recibir órdenes de quienes fueron establecidos desde un principio como dueños, reconoce las voces de los mismos y, ante la desafortunada frase de uno de ellos (el victimario) preguntándole a su pareja, la víctima, si había llamado a la policía, el software de última

14 http://www.montevideo.com.uy/contenido/EEUU-Google-Home-detiene-incidente-de-violencia-domestica-al-llamar-automaticamente-al-911-348417

generación lo interpretó como un mandato, una orden a cumplir, e inmediatamente realizó la llamada “solicitada”. Lo mismo sucede, no solo con Google Home, sino también con cualquier teléfono de gama media-alta con sistema operativo android de los que andan circulando hoy en día: si se tiene configurado el dispositivo con el reconocimiento por voz que ofrece la interfaz operativa de Google, se puede llamar a cualquier contacto o entidad que el teléfono tenga agendado o no, buscándolo en ese caso vía web. Al respecto, solo puedo decir que en lo personal esta configuración me resulta de gran utilidad pero por ahora, solo funciona en idioma inglés, dado lo cual quien no hable dicho idioma no podrá sacar provecho de la función hasta que incorporen otros idiomas. Aun así, llegado el caso de una emergencia o situación de peligro, sería muy raro estar discutiendo con alguien y de pronto cambiar de idioma y decir la expresión “call the pólice” en medio de una discusión. Incluso, si manejamos el idioma inglés, hay que tener presente que el dispositivo puede no reconocer nuestra voz producto de la euforia del momento, lo cual sucederá aun cuando hablemos nuestro idioma nativo.

La noticia que traje a colación se vincula estrechamente con el Big Data, al consistir en lo que se ha denominado Internet of Things (Internet de las cosas). Este nuevo concepto representa una tecnología capaz de “dotar a los dispositivos de la capacidad de observar, identificar y entender el mundo real sin la participación (ni la limitación) de una persona (…). Se trata en definitiva, de protocolos, sistemas y dispositivos interconectados con la capacidad de observar el mundo, generar información y de “interactuar” entre sí sin la intervención de una persona. Conforman una red con la capacidad de tomar información del ambiente y generar decisiones basadas en ese análisis”. Conforme esta definición y los titulares de los periódicos acerca del hecho acaecido que comenté más arriba, habría sido una decisión del propio sistema de software de la casa llamar a la policía, pero no fue así en ese caso, ya que Google Home no detectó en ningún momento una situación de peligro sino que se limitó a cumplir la orden de realizar una llamada.

La capacidad de generar decisiones basadas en análisis, es la verdadera concreción práctica de las intromisiones e injerencias en la privacidad de los usuarios de esta tecnología: llegamos a tal avance tecnológico, que la misma novedad tecnológica atenta por la definición del servicio o función que presta contra nuestra intimidad y privacidad. Pero no hace falta vivir en una casa o departamento inteligente para que suceda lo anterior: los últimos televisores lanzados al mercado, los microondas, equipos de

música, heladeras, lavarropas, son todos "inteligentes". Esto es lo que se conoce como la automatización de las cosas o domótica, e implica que todos los electrodomésticos están conectados a Internet, funcionan en base a un software. Prender la luz sin botones, apagar las cámaras sin interruptores abrir puertas sin llaves ni tarjetas, que la heladera detecte el stock de alimentos y pida al supermercado los faltantes suena a ciencia ficción pero es el mundo que ya existe y que, solo por subdesarrollismo, demora un poco más en llegar a Argentina.

El reconocimiento por voz pasa a ser el eje del funcionamiento de todos los equipos y dispositivos que nos rodean en el hogar; nuestros hábitos cobran significado y relevancia cuando son traducidos para cada aparato doméstico como patrones de conducta a tal escala como puede pensarse en los siguientes ejemplos:

*consumir todos los días café de la cafetera inteligente genera más temprano que tarde que ella misma se auto programe para tener listo el café a tal hora.

*ver cierto reality, telenovela, canal de películas o series, lleva a nuestro televisor a poner en pantalla dicho canal cuando es el horario correspondiente y el aparato está apagado o mostrando otro canal.

Detrás de todos estos avances en materia telecomunicacional están las grandes empresas, y detrás de ellas, personas.

Pero la tecnología, no solo nos invade in-house. Existe también la denominada wearable computing, que no es otra cosa, como la expresión lo indica, que la aplicación de la tecnología a lo que nos ponemos y usamos sobre nosotros mismos: viene a ser la integración entre los dispositivos y la vestimenta y los accesorios para medir signos vitales. Si queremos sorprendernos en serio, podemos debatir sobre las smart cities, ciudades automatizadas por medio de sensores que controlan, monitorean y regulan desde el tránsito hasta los servicios públicos domiciliarios.

Cuando se inventó el correo electrónico, cuando nació Google Mail, ¿hubiéramos imaginado que dicha cuenta era necesaria para utilizar un teléfono? Más aun, ¿hubiéramos pensado que podíamos enlazar nuestro teléfono con gps a la cuenta y permitir un seguimiento de nuestros contactos en vivo y en directo de nuestra ubicación y que otros compartan su ubicación con nosotros? Creo que no. Al margen de todos estos avances, no hay nada más invasivo que la información de geolocalización personalizada. La recolección de los datos personales, de los lugares que visitamos, la transferencia de esos datos con terceros "para mejorar el servicio" son a las claras injerencias en

nuestra intimidad en nuestros datos, gustos, consumos, lugares que visitamos con frecuencia (lo que me recuerda a la clásica pregunta cuando salgo de un lugar "¿quieres dar tu opinión y calificar?"). Pero eso, no es automático dirán, todos los prestadores de estos servicios. Claramente es cierto y tienen la razón: hemos dado, antes de comenzar a utilizar todos estos servicios y productos, nuestro consentimiento. Con ese tilde – obligatorio para poder iniciarse en la utilización de cualquier servicio – que colocamos al aceptar las bases y condiciones de uso y las políticas de privacidad dimos nuestro consentimiento revocable solo desinstalando la aplicación y dejando de usar el servicio en cuestión. Incluso los smartphones forman parte de estas prácticas cuando uno los enciende y lo primero que muestra la pantalla después de los logos es una advertencia de uso que exige aceptar una extensa política de uso (que no hace más que dejar en claro que cedemos casi todos nuestros derechos, permitimos prácticamente el acceso remoto a nuestro equipo, que se elaboren estadísticas y un sinnúmero de etc) para proseguir con el encendido del equipo. Paradojalmente, este proceder es acorde y legal conforme la legislación vigente, en especial, la reiterada ley en materia de Derecho Informático: la ley 25.326 de Protección de Datos Personales. Dicha ley consagra dos requisitos legales de todo tratamiento de datos personales:

1_Requerir el consentimiento previo del titular del dato (art. 5°), requisito que se cumple a la hora de exigirnos tildar la frase que dice que aceptamos y leímos las bases y condiciones.

2_Brindar información sobre el tratamiento previsto al titular del dato (art.6º). Este segundo requisito se cumple también, en el momento en que aceptamos marcando con un tilde y debajo o próximo a ese clic se pueden consultar los términos y condiciones que estamos aceptando.

Como conclusión, considero que toda la información que volcamos a la red es almacenada y utilizada para producir ganancias, para adecuar los productos, servicios y sus publicidades a los destinatarios de tales bienes. Como dice el dicho popular, *quien tiene la información tiene el poder*, a lo cual agrego que el poder en torno a la información se presenta como un gran rédito financiero. Como medida de precaución, sugiero tomar conciencia de la magnitud de datos personales nuestros que circulan en la web a modo de primer paso. En una segunda etapa, el quid de la cuestión radicará en reflexionar y decidir con fundamento si queremos seguir dejando esa información online y qué tipo datos *regalaremos* a partir de ahora.

Bibliografía

ALLENDE LARRETA, Agustín. “La protección de datos personales y el riesgo de la ciberseguridad en los procesos de auditoría previa (duediligence) en las adquisiciones y fusiones de empresas (M&A)”, editorial El Derecho. Buenos Aires, lunes 29 de mayo de 2017.

GONZÁLEZ ALLONCA, Juan Cruz y RUIZ MARTÍNEZ, Esteban. “Cloud Computing: la regulación de la transferencia internacional de datos personales y la prestación de servicios por parte de terceros”, Infojus. 1 de Octubre de 2015

GONZÁLEZ ALLONCA, Juan Cruz y RUIZ MARTÍNEZ, Esteban. *“Big Data: riesgos y desafíos en el tratamiento masivo de datos personales”*, *Nota a fallo* publicada en diario La Ley. Buenos Aires, 24/6/2016. Cita online: AR/DOC/373/2016.

PALAZZI*, “Pablo A. Transferencia internacional de datos personales”* publicada en diario La Ley. Buenos Aires 15/2/1017. AR/DOC/3904/2016

http://www.redipd.es/actividades/Seminario_2015_Montevideo/common/Ponencias/Panel_1/6._Ana_Brian.pdf

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

LAS 5 RAZONES PARA TENER UN BLOG PROFESIONAL

Para hacer marca en internet tenemos que diferenciarnos, no se trata de ser mejor que nuestra competencia, sino diferente. Todas las marcas buscan posicionarse en la mente de los consumidores/usuarios ¿cómo podemos diferenciarnos del resto si hacemos lo mismo?
Y si hay algo que nos ayuda a nuestro branding es generar contenido propio, para ello no hay mejor herramienta que un blog profesional o corporativo ¿todavía no tienen uno? hoy voy a contarte las 5 razones para tener un blog profesional.

COMPARTIR CONTENIDO AJENO TE SACA CLIENTES (?)

Compartir contenido de colegas o sitios relacionados a nuestra temática no está mal, no es que no se pueda hacer, el problema radica cuando lo único que hacemos es compartir artículos de “otros”.
Si vamos a usar las redes sociales para hacer marca, y esto significa que no vamos a molestar a nuestra audiencia con mensajes de autopromoción todo el tiempo, entonces tenemos que trabajar con contenido propio enfocado en estrategias claras que obtengan objetivos claros.
¿Cómo podemos hacer marca en redes si lo único que compartimos es contenido de otros? en realidad, estamos llevando tráfico a otros sitios ¿es como que vayan a tu estudio y en vez de abrirle la puerta le pongas un cartel “para consultoría jurídica puede dirigirte al estudio de mi competencia” ¿no es lo que buscas o si?

TRÁFICO A TU WEB Y REDES SOCIALES

SOMOS EDI LA RED

EL CENTRO DE INFORMACIÓN

y contenidos
más grande iberoamerica

TWITTER: ELDERECHOINF

Tener un blog profesional no solo te posiciona como especialista en un tema jurídico, sino que también ayuda (y mucho) a llevar tráfico a tu sitio web ¿qué significa esto?
A Google le encanta el contenido fresco, mientras más actualices tu blog (notas periódicas, semanales o mensuales) más posibilidades de posicionarte tendrás. Un sitio con blog es un sitio dinámico con muchas palabras claves que ayudarán a posicionar tu web (y tus servicios) en la búsqueda. Vamos con un ejemplo:

Si escribes un artículo titulado " Lo que tienes que saber antes de adoptar", puede que alguién que esté buscando información sobre "adoptar" encuentre tu artículo en Google, lo lea y entonces empiece a seguirte en redes, o de pronto lea más artículos, o de pronto mirá tus "servicios" en la web. Eso es "tráfico a tu web y redes" ¿no es genial?

Tener un blog sirve para darle dinamismo a tu web, eso le encanta a Google

HACIENDO MARCA EN MEDIOS OFFLINE

Voy a contarte mi propia experiencia: mi marca es un antes y después de mi blog, y si bien no me conoce el mundo entero, de hecho falta mucho para que eso suceda, me he posicionado en mi ciudad gracias a él.
Nunca pensé que la gente iba a leerme tanto, no solo que me leyó, sino que allí, en ese momento, empezaron los mensajes privados por redes; algunos para felicitarme otros para consultarme y otros para debatir. Eso me dio más energía para seguir escribiendo. Y a los dos meses, me llamó el primero medio, luego otro y así empecé a salir en radios, luego diarios, luego escribí artículos para medios de la zona,salí en programas de TV de otras provincias, y de a poco la cosa creció; llegué a Buenos Aires, llegué a Latinoamérica y acá me ves, con más energías que nunca. ¿te gustaría que te pase lo mismo? haz un blog

CONVERTIR LECTORES EN CLIENTES

Supongo que no solo quieres posicionarte como abogado, sino que también quieres vender, o mejor dicho, conseguir nuevos clientes. Bien, resulta que cuando le demuestras al mundo todo lo que sabes y encima lo haces para ayudar a otros (tu target) a resolver sus problemas, tus lectores, esos que ayudaste durante semanas, meses y años, pensarán en ti cuando requieran de un abogado o cuando algunos de sus conocidos lo requiera. La ecuación es simple:

librería | hammurabi

Talcahuano 440 - C1013AAI
CABA - Argentina
Tel.: (54-11) 4371-8179
info@libreriahammurabi.com.ar

en preparación

Colección «elderechoinformático.com»

11 volúmenes

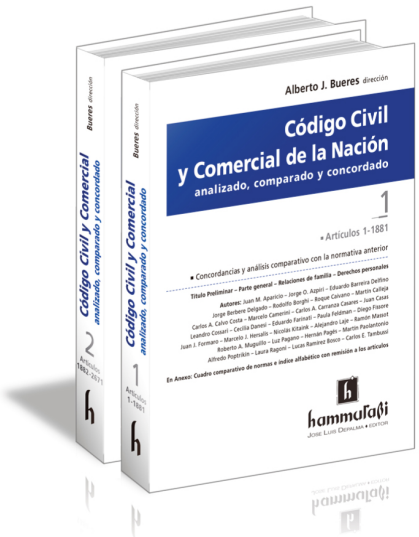
Guillermo M. Zamora dirección

1 — La prueba informática
2 — Negocios jurídicos en tiempos de Internet
3 — Delitos informáticos
4 — Propiedad intelectual en la era de la información
5 — Gobierno digital y gobierno abierto
6 — Datos personales, su protección
7 — ODR, Resolución de Disputas Online
8 — Firma digital
9 — Régimen jurídico de nombres de dominio
10 — Teletrabajo
11 — Aspectos jurídicos del *cloud computing*

Novedad

Código Civil y Comercial de la Nación

analizado, comparado y concordado



Alberto J. Bueres dirección

2 tomos | Artículos 1 - 2671

Análisis complementario de las principales normas que inciden en el «Derecho del trabajo» al cuidado de Juan J. Formaro

Contiene: Cuadro comparativo de normas. Indice alfabético de voces

• Tomo 1. Arts. 1 a 1429. Autores: Juan M. Aparicio – Jorge O. Azpiri – Eduardo Barreira Delfino – Jorge Berbere Delgado – Rodolfo Borghi – Martín Calleja – Marcelo Camerini – Carlos A. Carranza Casares – Rubén Compagnucci de Caso – Leandro Cossari – Cecilia Danesi – Paula Feldman – Diego Fissore – Juan J. Formaro – Marcelo J. Hersalis – Germán Hiralde Vega – Nicolás Kitainik – Alejandro Laje – Sabrina Luini – Ramón Massot – Luz Pagano – Hernán Pagés – Alfredo Popritkin – Laura Ragoni – Lucas Ramírez Bosco – Carlos E. Tambussi.

• Tomo 2. Arts. 1430 a 2671. Autores: Liliana Abreut de Begher – Beatriz Areán – Jorge O. Azpiri – Eduardo Barreira Delfino María I. Benavente – Gabriela Boquin – Roque Caivano – Carlos Calvo Costa – Marcelo Camerini – Juan Casas – Federico Causse Rubén Compagnucci de Caso – Leandro Cossari – Nelson Cossari – José Fajre – Eduardo N. Farinati – Juan J. Formaro – Andrés Fraga – Alberto Gabás Lidia Garrido Cordobera – Marcelo J. Hersalis – Gabriela Iturbide – Jorge Juliá – Alejandro Laje – Ricardo Nissen – Martín Paolantonio Christian R. Pettis – Lucas Ramírez Bosco – Javier Rosembrock Lambois – Luciana Scotti – Gabriel Ventura – Luis M. Vives.

Escribo artículos para ayudar a resolver problemas(jurídicos) a mi target, me posiciono en la temática y categoría (eje: Abogado, Derecho de Flia), consigo lectores, con el tiempo se acercan e interactúan con mi marca, cuando necesiten servicios jurídicos me contratan.

Con un blog llegas a tu público, se convierten en lectores y finalmente puedes convertirlos en clientes.

IDENTIFICAR TEMAS DE INTERÉS Y NUEVOS SERVICIOS

Mi blog tiene un poco más de dos años, mucho de política digital, después empecé a pulir la notas y me fui más para lo técnico. Haber conocido la comunidad de El Derecho Informático y todos los grandes profesionales que la componen, ha despertado mi interés por temas de seguridad y demás. Me di cuenta que mi profesión podía ayudar no solo a mejorar aspectos de marca sino también, a colaborar para generar más conciencia en internet. los últimos años me dedique a estudiar, investigar y aprender sobre estas cuestiones, y cómo no podía ser de otra manera, tuve que escribir sobre ello ¿el resultado? mi público se amplió, di charlas sobre “comportamiento responsable en internet” y colaboré con abogados

Lo mismo me pasó en otras áreas, descubrí qué es lo que realmente necesita mi audiencia, lo que les aqueja, lo que buscan. A raíz de esto armé capacitaciones nuevas, todo esto lo aprendí escribiendo en un blog y escuchando a mis lectores.

Sí, tener un blog es la mejor estrategia para hacer marca personal, pero no olvides que también debes difundir tus notas, y que la redacción web tienen sus características diferenciales, pero eso creo que es tema para un próximo artículo ¿no?


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

ELDERECHOINFORMATICO.COM

ESPERAMOS HAYAN DISFRUTADO

Revista Digital EDI -estamos comunicados