EDI

REVISTA DIGITAL
DISTRIBUCIÓN GRATUITA
ABRIL 2017

EDICIÓN N° 26

Colaboran:

Fabián Descalzo
Ismael Lofeudo
Sebastián Gamen
Info-Lab

José Maria Cifuentes
Bárbara Peñaloza
Pedro Macias
Nahuel Alvarez Toledo

Selene Pereza Rosas
Carolina Marín
Erick López
Natalia Toranzo

ROSARIO 9 Y 10 DE JUNIO

I CONGRESO DE CIBERCRIMEN E INVESTIGACIÓN DIGITAL

9 Y 10 DE JUNIO 2017

AUDITORIO FACULTAD DE INGENIERÍA - ROSARIO

PARA MÁS DETALLES INGRESAR EN ELDERECHOINFORMATICO.COM

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

CONTENIDOS

TERCER ENCUENTRO ELDERECHOINFORMATICO.COM URUGUAY

Sociedad Red y derechos humanos

Jueves 15 de junio de 2017 ▪ 9:00 hs.

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






PANELES

Las nuevas tecnologías y el empoderamiento de la mujer
Los datos personales y la Sociedad Red
¿Los avances del gobierno digital otorgan más participación al ciudadano, mejor servicio y más democracia?
Ciberdelitos, ciberseguridad: ¿el derecho tiene respuestas a los problemas planteados en la Sociedad Red?

CONFERENCIAS

Informática forense y manejo de la evidencia digital
Dimensión tecnológica de la protección de los más vulnerables

CHARLAS

Medios de pago electrónicos en Uruguay: ¿inclusión financiera para quién?
Teletrabajo en el desafío socio-laboral de la inclusión

Inscripciones: Red Pagos, cuenta 61919, a nombre de «Tercer Encuentro Uruguay»
Informes: uruguay@elderechoinformatico.com

AUSPICIA: Ethical Hacking Consultores

ORGANIZA: La Red (EDI) ElDerechoInformatico.com — El Centro de Información más grande de Iberoamérica

APOYA: Asociación de Escribanos del Uruguay

EDITORIAL

/ ELDERECHOINFORMATICO

QUERIDOS AMIGOS

Estamos lanzando con esta edición la primera del año 2017, son 13 artículos donde hay de todo, como siempre, me enorgullezco de la calidad del producto, podría ser mejor?? Obvio, siempre se puede mejorar, pero eso no quita que el esfuerzo, las ganas, el tiempo que le dedican los colaboradores a mandar sus textos es invaluable y con ello solo refuerce mi orgullo.-

Ha sido un comienzo tardío, estamos casi en mayo, pero bueno, las otras actividades de la Red que estamos lanzando ameritaban esta demora. En Marzo lanzamos el Diplomado con nuevas materias y la Certificación de la Universidad Nacional de Rio Negro de la República Argentina, estamos abocados a la organización de los Congresos en Rosario/ Santa Fe (Argentina) - Montevideo (Uruguay) Medellín (Colombia) aparte haremos presencia en el organizado desde APANDETEC en Panamá, al del Ilustre Colegio de Abogados de Lima (Perú), participamos en Buenos Aires organizado por Mente Jurídica Digital, estamos siempre atentos a las charlas organizadas desde Guatemala por Seguridad INFO y MAS, en fin, procurar ser útiles es la idea.-

EDIPODCAST, EDINoticias, y todo aquello que nos haga sentir que podemos aportar nuestro granito de arena. Estamos donde nos gusta estar, cerca de la mayor cantidad de lugares posibles, donde podamos, donde nos dejen, donde sea que nos haga sentir cerca.-

FORUM NACIONAL SOBRE NUEVAS TECNOLOGIAS y

CIENCIAS EN LA INVESTIGACION CRIMINAL.

12 de mayo 2017, Hotel Savoy av. callao 181
Salón Olimpo - Horario de 9 a 17 hs
https://juridica-digital.com.ar

“UNA VISIÓN PROPEDEÚTICA DEL DELITO DE SEXTING EN EL CÓDIGO PENAL ESPAÑOL”

Autor: Pedro Jesús Macías Torres

El desarrollo tecnológico ha conllevado y sigue así haciéndolo cambios de comportamiento en adultos, también jóvenes (y menores de edad). Este trabajo explica someramente la práctica de lo que de manera coloquial se denomina “Sexting”, es decir, el envío de imágenes y fotos en postura sexual o provocativa dirigida a un tercero, por medio de la webcam o del teléfono móvil en sí. Este vocablo es la fusión de “sex” (sexo) y “texting” (texto) y su principal repercusión es el mayor grado de afectación hacia un colectivo como el de los menores de edad, que por su todavía escaso desarrollo de la personalidad no son capaces de calibrar todos y cada uno de los perjuicios que esta práctica lleva implícita. Muchas veces se hace para impresionar a alguien al que se conoce desde hace tiempo, a una expareja o compañeros de instituto o de trabajo.

En los supuestos de chicos cuyas edades oscilan entre los 12 y los 16 años, la gravedad es aún mayor, dado que no conocen la relevancia de su privacidad. Una relación entre el que genera estas imágenes y el que la recibe queda reducida exclusivamente a un ámbito de dos personas: el emisor y el receptor. Hasta aquí no cabe ningún tipo de problema; la persona que ha realizado dichas fotos o el video (o conjuntos de ellos) tiene la única intención de compartir esas imágenes con el que la recibe; por tanto se presume que no ha otorgado un consentimiento efectivo para la cesión o reenvío de las imágenes recibidas a terceras personas, salvo excepciones que siempre puede haberlas.

Tal vez por razones de descaro, de ser una persona despechada, por ira, venganza o por impresionar a los demás, se suelen reenviar las imágenes a otro tipo de personas generando un daño irreparable hacia el protagonista de los videos. Decimos que es irreparable porque todos aquellos que en mayor o menor medida han tenido cierto contacto, bien con las redes sociales, bien a través de telefonía móvil y créannos, son ya muchos los que están conectados a estos vehículos transmisores de información instantánea, conocen que todo dato que pase a una colectividad virtual en ésta se queda. Existen opciones varias que explicaremos posteriormente. Tan sólo pretendemos dejar claro que un receptor de un video o foto (sext) de alguien de su entorno en una pose crítica para muchos, puede hacerse viral, es decir, conocido por muchos o siendo más bien justos: conocido por todos, salvo que quieran algunos desvincularse de estas nuevas tendencias sociales, algo que se antoja como prácticamente imposible viniendo de las nuevas generaciones que poseen un conocimiento mayor si cabe que sus padres.

El problema que se suscita en primer grado, no está tan engarzado con el Derecho, sino más bien con cuestiones de índole psíquica. No sería la primer ni única vez que protagonistas jóvenes de estos *sexts* (en la mayoría de las ocasiones mujeres), han optado por el suicidio, debido a la no superación de reacciones provocadas a un nivel social por sus actos cometidos: depresión, ansiedad, fobias, estigmatización, pérdida definitiva de reputación según determinados ámbitos y que trasladan al protagonista emisor el blanco de todo tipo de críticas. Es más que recomendable que no sólo nos decantemos por una vía represora y/o sancionadora; cometido del Derecho Penal, también ha de hacerse hincapié como la prevención para eludir en última instancia la intervención jurídica y que en el caso de nuestro Derecho español tipifica estas conductas hasta con penas de prisión.

De manera diáfana lo expone el artículo 197.7 del Código Penal al afirmar: *"Será castigado con pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aún sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa"*.

Pero el problema del Sexting no finaliza aquí; debemos entender la estrecha relación que existe entre esta nueva figura delictiva y los derechos recogidos en el artículo 18.1 de la Constitución española; a saber: honor, intimidad personal y familiar y propia imagen. Los textos en los que debemos basarnos son la Carta Magna como acabamos de mencionar y la no tan reciente Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, la Intimidad y la Propia Imagen.

Por todos es conocido que la intimidad es el ámbito más reservado de una persona. La sexualidad forma parte de ésta, aunque no deben descartarse otros escenarios como puede ser el consumo habitual de drogas o el alcoholismo; facetas que también influyen en el área al que nadie tiene derecho a saber, como a su vez perteneciente al honor de la persona, si lo consideramos como la reputación, fama o estimación.

La legislación penal actual ha colocado el tipo en el artículo 197.7 CP, pero anteriormente en fase de tramitación parlamentaria, par de la doctrina mostraba cierto desencanto con una protección jurídico penal por esta clase de actos. No podemos poner en duda el daño que reviste para la víctima la difusión masiva de sus imágenes o videos en redes sociales, sin olvidar la inconsciencia que muchos

jóvenes poseen con la producción de estos videos (siempre de carácter casero y de rápida elaboración), de ahí que la tarea de asunción de responsabilidades por parte de los menores de edad es algo esencial, para que en lo sucesivo abandonen de manera definitiva estas actitudes. Tan nociva es desde un punto de vista la conducta de la que puede ser la víctima como de la persona que recibe los *sexts* y lejos de los que conforma la prudencia, no solo no borra los datos, sino que a la vez los reenvía a terceros ocasionando un daño mayor. Obviamente no es lo mismo un reenvío a dos amigos reduciéndolo a un círculo más bien cerrado que el envío a una red social en la que participan millones de personas, por eso los jóvenes en un supuesto de este tipo deben valorar y mucho el perjuicio generado a la víctima en aquello foros donde pueden consultarse múltiples videos similares con un punto en común: el despertar un deseo sexual en aquel que se convierte en mero espectador.

Es aconsejable en el Sexting que la persona que ha recibido esos videos los anule lo más rápido posible o incluso que pueda ponerse en contacto con el centro escolar en caso que la víctima sea aun adolescente; eso sí, siempre con la ayuda de un adulto cuyo acompañamiento es más llevadero, presuponiéndose por su edad un mejor conocimiento de los riesgos que existen a la hora de difundir una información de carácter privada. En mi opinión, creo que la persona recibidora de esos videos solo podría responder personalmente si el acceso a esas imágenes fuera no consentido. En esta realidad no ha sido así, puesto que la víctima parte de una cuasi seguridad que demuestra ante los demás; los ha enviado sin mediar coacción o error alguno. Si la persona que recibe el Sexting, que adopta una postura pasiva, decide borrar esos datos, el problema finaliza en ese mismo momento, pero la casuística demuestra una realidad totalmente opuesta cuando atendiendo a los foros de imágenes o a los círculos de pornografía, es más que probable que puedan aparecer imágenes de personas a las que conocemos de un entorno más bien cercano.

Se ha hecho un gran favor a la sociedad esta regulación *ex novo* de este tipo de conductas, era más que conveniente, lo que no sabemos todavía es el desenlace que puede tener para muchas de estas víctimas de cara a los responsables de las webs que incorporan las fotos "colgadas" por terceros y no precisamente por el protagonista de las mismas. La persona autora de los *sexts* no va a ser ingenua como para colgar unas fotos a sabiendas de un perjuicio que puede llegarle a ella. Por estadística, podremos encontrar en la vida un grupo de jóvenes que poco teman a la opinión ajena y como nada tienen que perder adoptan en su caso conductas muy arriesgadas; ya lo es, de hecho enviárselo a personas de su entorno con el peligro de una acción malintencionada, como para situarse en un ciberescaparate y por tiempo indefinido.

La Ley Orgánica de Protección de Datos del año 1.999, (LOPD), asegura que la imagen de una persona física es un dato personal y por tanto para iniciar un tratamiento de éstos es relevante haber recabado el previo consentimiento de los interesados. Suponiendo que el adolescente que ejerce la práctica

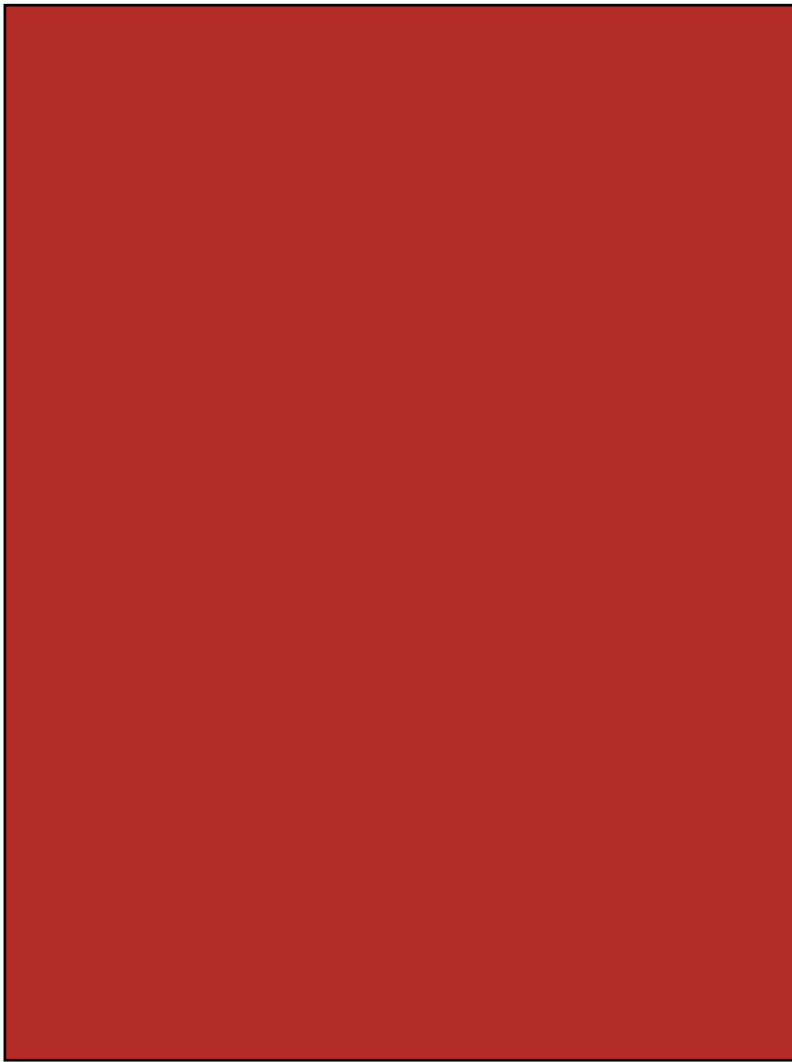
del Sexting encuentra sus videos almacenados en una red social, tiene a su favor varias opciones de defensa, por un lado presentar una denuncia ante el Grupo de Delitos Telemáticos de la Guardia Civil (o la Brigada de Investigación Tecnológica de la Policía Nacional) o contar con ciertas antelación con una resolución administrativa o judicial favorable a sus intereses para ejercer ese derecho de cancelación que toda persona merece. Según la LOPD el consentimiento ha de ser: libre, inequívoco, específico e informado.

En la mayoría de las ocasiones, tal beneplácito es inexistente, por lo que su tutela jurídica le posibilita para ponerse en contacto con los administradores de la web para que eliminen esos contenidos totalmente ilícitos.

La ley de Servicios de la Sociedad de la Información y del Comercio Electrónico de España (LSSICE) en lo concerniente a los Prestadores de Servicios regula una responsabilidad y una excepción a ésta. Para el tema que aquí exponemos del Sexting nos interesa fundamentalmente en qué supuestos los Prestadores se ajustan a una responsabilidad, bien civil, penal o administrativa. Esos dos requisitos o supuestos como decimos son los siguientes: por un lado el denominado "conocimiento efectivo"; tal vez el más importante de ambos. Ese conocimiento efectivo se llega a él desde el instante en que la víctima presenta alguna de las dos resoluciones antes aludidas. Los responsables del canal o de la red social examinarían estas resoluciones y en virtud de la ley y a tenor del artículo 16.1 de la LSSICE eliminarían los contenidos del Sexting hechos tiempo atrás o bien tendrían que evitar el acceso de los internautas a estas imágenes o fotos.

El segundo de los requisitos viene dado por lo que se llama el carácter manifiestamente ilegal de lo que es susceptible de ser visualizado. No es complicado a mi modo de ver realizar un rápido análisis para deducir la legalidad o ilegalidad de las fotos. En este segundo requisito, si las imágenes fueran de una claridad meridiana la presentación de una resolución de la Agencia Española de Protección de Datos (AEPD). Como los foros son distintos los unos de los otros y para evitar sorpresas de última hora conducentes a un nerviosismo sobre la mayor viabilidad de mantener esas fotos expuestas, es por lo que se aconseja (aun mostrando una ilicitud totalmente visible a todas), presentar una sentencia que reforzarse en cierto modo la petición emanada de la víctima.

Sevilla – Marzo 2017



Usuarios de acceso restringido

Por Nahuel Álvarez Toledo[1]

Los tiempos han cambiado, las realidades han cambiado, los vínculos cambiaron y por sobre todo las relaciones personales cambiaron. El nuevo siglo nos encontró en un mundo hiperconectado, hoy en día en cuestión de segundos podemos usar un buscador y obtener información de todo tipo y de todos los lugares del mundo que queramos; el problema de los tiempos modernos no está dado por la complicación en la falta de acceso, sino más bien por la famosa "brecha digital".

Qué es la brecha digital: La brecha digital se define como la separación que existe entre las personas (comunidades, estados, países…) que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben cómo utilizarlas. [2]

Debemos saber que existen dos grupos de personas que son abarcadas por el concepto de brecha digital, diferenciadas por un criterio de tipo volitivo, si quisiéramos darle un concepto. Es decir, tenemos aquel grupo de personas que no pueden acceder al "*sistema*" por desinformación o imposibilidades estructurales y/o económicas; y aquellas que simplemente **desean** mantenerse al margen de la globalización.

El mundo tal como lo conocíamos está cambiando, qué quiero decir con esto, la gente "común" está tomando participación en las resoluciones sobre temas globales, el ejemplo más concreto de esto lo encontramos en la Gobernanza de Internet, donde confluyen los diferentes sectores representantes de los gobiernos, la comunidad técnica, la sociedad civil y el sector privado, para la toma de decisiones sobre la sociedad de la información y el mundo de lo intangible.

Ahora, si la sociedad se encuentra jugando un rol central en la toma de decisiones, ¿cómo es posible que sigamos hablando de brecha digital?.

Según un informe del Banco Mundial sobre "Dividendos Digitales", casi el 60% de la población mundial aún no tiene conexión a internet y no puede

[1] Abogado egresado de la Universidad Nacional de Córdoba.

[2] Arturo Serrano, Evelio Martinez; "La Brecha Digital: Mitos y Realidades", México, 2003, Editorial UABC, 175 páginas, ISBN 970-9051-89-X www.labrechadigital.org

participar de la economía digital. También persisten las brechas digitales geográficas, de género, de edad y de ingresos dentro de cada país (…) Argentina estuvo a la vanguardia en la adopción de tecnologías por encima de la media regional, pero no ocurre lo mismo con los componentes analógicos que incluyen desde cuestiones culturales hasta la bancarización de la economía y la regulación de las telecomunicaciones.[1]

Un informe del INDEC[2] del año dos mil quince[3] demuestra que nuestro país tiene una brecha digital muy acentuada en las provincias del norte, ya que las mismas cuentan con un lamentable atraso que las condena a una conexión precaria y aristocrática. Los grandes núcleos de conexión se centran en las principales provincias argentinas, ya que su flujo económico y poblacional es de constante movimiento, y el movimiento trae cambios y renovaciones.

El informe del mismo organismo del año dos mil dieciséis[4] denota un crecimiento porcentual de un dígito. Crecimiento dado por la conectividad de diferentes aparatos a redes, pero no acompañada de crecimiento en infraestructura y conectividad con las provincias que aún siguen siendo pequeños feudos ajenos a la globalización e interconexión.

Lamentablemente, los gobiernos aún no comprenden (asumiendo que esa sea la idea en realidad) la importancia de garantizar la infraestructura para una conectividad con los ciudadanos, no solamente por la necesidad de integrar al vecino al mundo globalizado, sino más bien por los beneficios que ello conlleva, beneficios como por ejemplo permitir una mejor transparencia en las gestiones gubernamentales, beneficios económicos relacionados con la reducción del consumo de papel es en la emisión de tributos, gozando de los beneficios que trae el uso de internet para las instituciones educativas, los turneros digitales que descomprimen la presencia física en diferentes organismos públicos o privados, etc.

Igualmente, además de la infraestructura, otro de los problemas que trae aparejado el mundo virtual, es la incorporación generacional a la red. No hablo de los niños ya que el viejo adagio ha cambiado, los niños ya no vienen con un pan bajo el brazo, sino más bien, con un usuario y contraseña. El gran problema, si se quiere darle una connotación dramática, está centrado en los adultos mayores, si, nuestros abuelos están siendo absorbidos por la red y no saben ni siquiera de qué se trata.

Como sabemos, internet es un contenedor de información, el problema es que se debe generar educación en su uso para su aprovechamiento, eso es

---

[1] BRECHA DIGITAL: LA MAYOR PARTE DE LA POBLACIÓN MUNDIAL AÚN NO POSEE INTERNET. 16 de Marzo de 2016. www.periodismo.com. Véase: http://www.periodismo.com/2016/03/16/brecha-digital-la-mayor-parte-de-la-poblacion-mundial-aun-no-posee-internet/

[2] El Instituto Nacional de Estadística y Censos (INDEC) es un organismo público, de carácter técnico, que unifica la orientación y ejerce la dirección superior de todas las actividades estadísticas oficiales que se realizan en el territorio de la República Argentina.

[3] Guillermo Tomoyose. UN MAPA INTERACTIVO MUESTRA EL NIVEL DE ACCESO A INTERNET EN LA ARGENTINA. LA NACION LUNES 09 DE FEBRERO DE 2015. Véase: http://www.lanacion.com.ar/1766327-un-mapa-interactivo-muestra-el-nivel-de-acceso-a-internet-en-la-argentina

[4] CRECIÓ UN 9,5% EL ACCESO A INTERNET RESIDENCIAL EN LA ARGENTINA. 16 de Junio 2016. www.infotechnology.com. Véase:http://www.infotechnology.com/online/Crecio-un-95-el-acceso-a-internet-residencial-en-la-Argentina-20160615-0007.html

lo que genera que nuestros abuelos estén apartados de la sociedad 2.0.

La generación de los adultos mayores se encuentra signada por una división interna, es decir, tenemos abuelos que no quieren *ingresar* a la sociedad de la información por comodidad- recelo- enojo- etc.; y los abuelos que quieren ingresar, o fueron ingresados de manera arbitraria por ejemplo por el uso de la red para los trámites gubernamentales, pero no saben cómo manejarse en la web.

Tomando como ejemplo datos de países vecinos, según la Séptima Encuesta Nacional de Acceso y Uso de Internet en Chile 2016, realizada por la Subsecretaría de Telecomunicaciones (Subtel), el 60% de quienes tienen entre 61 y 75 años declara no haber usado nunca un computador.[1] Es decir, los abuelos de todo el mundo están siendo sujetos *desconectados* de la red.

El problema está en cómo generar en los adultos la empatía para con la red, estudios demuestran que la

manera más simple de comenzar es demostrándole los usos más básicos de la web, ejemplo leer el diario, ver algún programa, leer un libro, etc. Con el tiempo se pueden ir ampliando horizontes de uso, pero siempre se requiere el acompañamiento de familiares que guíen en el uso y en el descubrimiento de beneficios sobre el uso de internet.

En Argentina nos encontramos atravesando una digitalización de diversas entidades administrativas que ofrecen una serie de servicios por sus respectivas páginas web. Por ejemplo el ANSES[2], un organismo

[1] LOS ABUELOS DIGITALES (O CÓMO INTRODUCIR A LOS ADULTOS MAYORES EN INTERNET). 06/10/2016.www.casablancahoy.cl. Véase: http://www.casablancahoy.cl/2016/10/06/los-abuelos-digitales-o-como-introducir-a-los-adultos-mayores-en-internet/

[2] La Administración Nacional de la Seguridad Social (ANSES) es un Organismo descentralizado que desarrolla sus funciones en el ámbito del Ministerio de Trabajo, Empleo y

que pone a beneficio de los abuelos en sus casas una serie de prestaciones que le permiten ahorrarse el viaje hacia la dependencia y garantizar una agilidad en las mismas. O, a nivel provincial, en Córdoba el gobierno realizó una digitalización de tributos, los cuales si se quieren de manera física se debe solicitar. Es decir, se impuso a nuestros adultos mayores una <digitalización forzosa>.

El tema central para el uso correcto y aprovechamiento de los beneficios de Internet está dado por la necesidad de educar en su uso, y para su uso, para así garantizar una explotación y aprovechamiento del cúmulo infinito de información. La educación en internet y con internet debe ser uno de los ejes centrales de las políticas gubernamentales en pos del futuro (un futuro que llegó ayer en el mundo, pero que aún se encuentra en suspenso para muchos países por decisión o por imposibilidad), un pueblo que tiene acceso a la información es un pueblo informado y culto. Además un gobierno que cuente con una plataforma virtual donde se garantice un gobierno abierto, es un gobierno que (en principio) goza de una mayor transparencia en sus funciones.

Es importante pugnar por un internet libre, un mundo con mayor privacidad para el usuario particular y mayor publicidad para los gobiernos, de esa manera se genera y garantiza la participación en las sociedades democráticas.

La brecha digital es una realidad, pero es solucionable con políticas públicas de calidad e inserción, estamos atravesando un segundo milenio, no podemos permitirnos que haya problemas de "desconexión" en nuestro mundo. El derecho a la información es uno de los derechos que más vulneraciones sufre cotidianamente y los estados, junto con la sociedad civil, deben pelear para garantizar el ejercicio activo del mismo.

Mientras siga habiendo brecha digital (reitero que hablo de aquella brecha dada por quienes no pueden acceder a la sociedad de la información por desconocimiento o falta de infraestructura) todos somos cómplices de la vulneraciones y vejaciones de los derechos de nuestros vecinos. En una época de hiperconectividad, la solidaridad debería ser el valor reinante, por lo cual todos los ciudadanos deberían pelear para lograr una red de lazos que garanticen que todos formemos parte de un mundo que busca conectar para solucionar problemas, dar información, garantizar transparencias, permitir participación, etc.

"Para muchas personas, la actual expansión del acceso a las tecnologías digitales amplía las opciones disponibles y facilita diversas actividades. A través de la inclusión, la eficiencia y la innovación, el acceso a estas tecnologías brinda oportunidades que antes estaban fuera del alcance de los pobres y de los sectores desfavorecidos."[1]

[1] Banco Mundial (2016), Informe sobre el desarrollo mundial 2016: Dividendos digitales, cuadernillo del "Panorama general", Banco Mundial, Washington DC. Licencia: Creative Commons de Reconocimiento CC BY 3.0 IGO

UNIVERSIDAD AUTÓNOMA®
LATINOAMERICANA - UNAULA
SNIES 1814

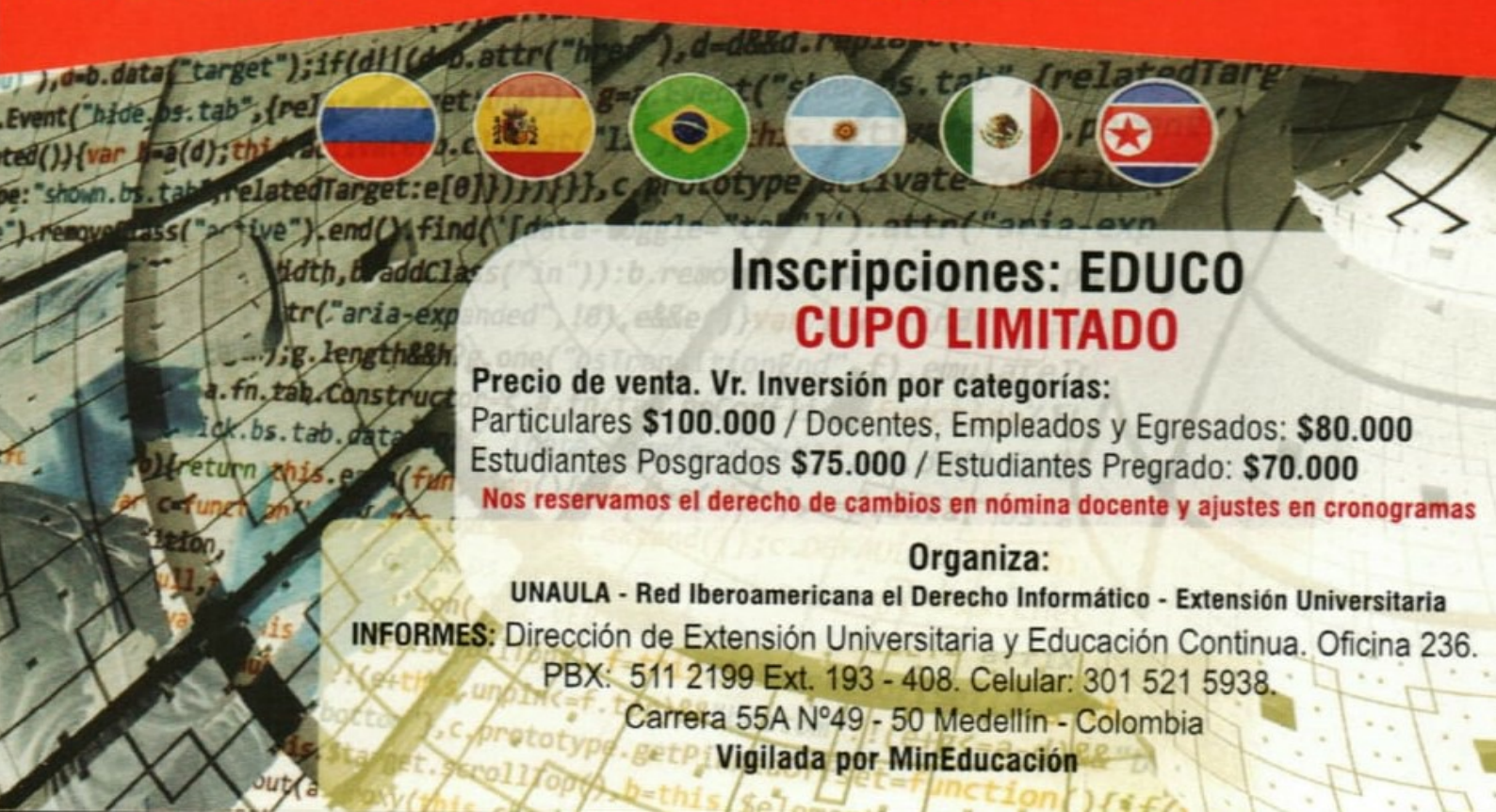
IV Curso Internacional DI + TI

Ciberseguridad y Ciberdefensa

Dirigido a: Empresarios, Investigadores, Abogados, Funcionarios Judiciales, Ingenieros Informáticos, Ingenieros de Sistemas, Estudiantes de Ingenieras de Sistemas e Informática, Investigación Judicial y entes del Estado.

26 al 28 de Julio

Lugar: Auditorio Rafael Uribe Uribe
Fecha: 26 y 27 de julio de 7:30 a.m. a 6:00 p.m.
28 de julio de 7:30 a.m. a 12:00 m
Incluye certificado



Inscripciones: EDUCO
CUPO LIMITADO

Precio de venta. Vr. Inversión por categorías:
Particulares **$100.000** / Docentes, Empleados y Egresados: **$80.000**
Estudiantes Posgrados **$75.000** / Estudiantes Pregrado: **$70.000**
Nos reservamos el derecho de cambios en nómina docente y ajustes en cronogramas

Organiza:
UNAULA - Red Iberoamericana el Derecho Informático - Extensión Universitaria

INFORMES: Dirección de Extensión Universitaria y Educación Continua. Oficina 236.
PBX: 511 2199 Ext. 193 - 408. Celular: 301 521 5938.
Carrera 55A N°49 - 50 Medellín - Colombia
Vigilada por MinEducación

DIPLOMATURA

POSGRADO EN DERECHO INFORMÁTICO
ORGANIZA: ELDERECHOINFORMATICO.COM

1. Delitos Informáticos
2. Informática Forense
3. Aspectos Legales Datos Personales
4. Gobierno Digital
5. Aspectos Legales Cloud Computing
6. Régimen Jurídico Nombres de dominio
7. Aspectos legales del e-commerce
8. Teletrabajo
9. Propiedad Intelectual
10. Certificaciones Digitales

CERTIFICA UNIVERSIDAD NACIONAL
DE RIO NEGRO/ARGENTINA

ESTAMOS EDIficando

RESPONSABLE
SEBASTIÁN
GAMEN

Mujeres y tecnologías. Puntos a favor y en contra.

Ab. Sebastián A. Gamen

El 95% de las conductas agresivas como acoso, lenguaje insultante e imágenes denigrantes online se dirigen hacia las mujeres y proceden de sus parejas o ex parejas, según la ONU[1]. Sin dudas, un dato abrumador que justifica las marchas y reclamos de las mujeres contra la violencia de género en todo el mundo.

En este artículo deseamos hacer un análisis, con las limitaciones de la extensión, de cómo las tecnologías actúan a favor y en contra.

Comenzando con las contras, no podemos pasar por alto que las tecnologías facilitan algunas conductas violentas contra la mujer. Sabemos que las tecnologías, en muchos casos, atentan contra la privacidad y los datos personales, y veremos que justamente los violentos hacen lo mismo aprovechándose de las facilidades que los celulares proveen.

Enumerando algunos ataques que sufren las mujeres podemos mencionar el control de sus mensajes o conversaciones. El monitoreo de mensajes, mails o redes sociales es una conducta violenta. Una conducta que denota claramente una patología del agresor y que puede derivar hasta en el asesinato de su pareja[2].

Otros tipos de ataques tiene que ver con el chantaje. Una vez que los hombres consiguen videos o fotos íntimas es muy común que las mujeres se vean involucradas en relaciones asfixiantes[3]. El chantaje se usa para conseguir más videos o fotos hasta para conseguir relaciones sexuales no consentidas.

Sin dudas los sistemas de geoposicionamiento son una herramienta peligrosísima en manos de hombres violentos[4]. En su máxima expresión las mujeres saudíes son vigiladas constantemente por sus "guardianes". Sin llegar a ese extremo, tu pareja podría saber exactamente tus recorridos y lugares donde estuviste, como los horarios. Si quieres ver más info entrá a https://maps.google.com/locationhistory/b/0/ y verás

[1] Naciones Unidas. daccessods.un.org/TMP/7121883.html

[2] http://www.elsalvador.com/articulo/sucesos/hombre-mata-pareja-por-encontrarle-mensajes-celular-133704, recuperado el 21-03-17.

[3] http://www.t13.cl/noticia/tendencias/las-mujeres-son-extorsionadas-y-humilladas-publicacion-sus-fotos-intimas-internet, recuperado el 21-03-17.

[4] http://www.infobae.com/2012/11/21/1061901-mujeres-saudies-rastreadas-electronicamente/, recuperado el 17-03-17.

con extrema precisión todos los lugares donde estuviste, día x día.

Si hablamos de acoso sexual las conductas llevadas a cabo son varias y usan las tecnologías en diferentes niveles.

Parece que recibir llamadas de otros hombres, conocidos y desconocidos, para realizarles propuestas sexuales es algo común. Por ejemplo en Pakistan (2009) el 94% de las mujeres dijo haber recibido alguna llamada o mensaje para acosarla sexualmente[1].

En el mismo sentido, en India la mitad de las denuncias de mujeres por ciberdelitos tiene que ver con el uso del rostro de la mujer para insertarlo en fotos pornográficas, hasta incluso se llegó a incluir el teléfono de la mujer con su identidad robada.

Es común que por venganza se publiquen anuncios falsos de citas o búsquedas de parejas. Por esos hechos una mujer fue violada y el hombre dijo al ser detenido que estaba obedeciendo a los deseos de la mujer, según habían chateado antes. El robo de identidad en esos casos es peligrosísimo, y lamentablemente en pocas ocasiones encuentra su castigo legal.

Otro problema que facilita internet es la captación de mujeres para la trata. Los delincuentes consiguen captar y encontrarse con las víctimas, anunciando falsas agencias de modelos o agencias matrimoniales.

Mencionados algunos de los problemas que la tecnología facilita en contra de la mujer. Pero podemos hablar de la otra cara, ¿de qué modo las tecnologías ayudan?

El primer uso que las tecnologías facilitaron es el de la comunicación. La comunicación claramente ayuda a viralizar y fortalecer campañas, crear nuevas redes, prevenir y prestar apoyo a las víctimas.

Existen varias aplicaciones para realizar denuncias, rescatando la española de la Secretaría de Estado de

[1] https://www.amnesty.org/es/latest/campaigns/2016/01/online-harassment-in-pakistan-and-how-women-are-fighting-back/, recuperado el 17-03-17.

Seguridad, llamada AlertCops. Esa aplicación, de descarga gratuita, permite generar alertas seleccionando el icono de acuerdo a la agresión sufrida. El hecho que sea con íconos facilita las denuncias para aquellas personas con dificultades auditivas.

La aplicación más innovadora de la cual tuve noticia es iEAA (Evidentiary Abuse Affidavit), desarrollada por la abogada estadounidense especialista en violencia de género Susan Murphy Milano[1]. Con esta aplicación la víctima puede sacar fotos, grabar videos o conversaciones las cuales quedan almacenadas en la nube. En casos de extrema necesidad, muerte o desaparición de la mujer, se puede pedir una copia de la cuenta obteniendo los investigadores una prueba fundamental para resolver el caso.

Creemos que las tecnologías vienen a mejorar la situación de las mujeres. Por un lado, mostrando una realidad violenta que antes no se conocía. Vemos como hoy en día mujeres de países árabes o de África pueden mostrar al mundo su realidad, para así movilizar protestas o concientizar sobre sus derechos.

Del mismo modo, vemos que existe una comunión de las mujeres del todo el mundo en contra de la violencia de género y ello se ve fortalecido por la comunicación online.

Claro que la violencia contra la mujer que se da en internet es alarmante. Es indignante que se use la tecnología para usos violentos. Pero, en contraposición es gratificante ver como mujeres de todos los rincones del planeta pueden gritar fuerte, y hacerse oír gracias a las tecnologías.

[1] http://www.documenttheabuse.com

Gobierno Abierto – Y el Open data day 2017

El pasado 4 de marzo se celebró el "Día de los datos abiertos", un evento a nivel global que busca impulsar políticas de aperturas de datos en los Estados.

Crónica: Dr Ismael Lofeudo

Pero... ¿Que son los datos abiertos y por que ahora hablamos de ellos?.

Los datos abiertos forman parte del llamado Gobierno Abierto (del inglés Open Government, pero que sería correcto traducir como "Estado Abierto").

La iniciativa de Estado Abierto fue promovida desde Estados Unidos, por la Administración del ex presidente Obama. La misma busca hacer a los gobiernos más eficientes incentivando a los gobiernos a ir más allá en materia de transparencia, rendición de cuentas y participación ciudadana.

Las iniciativas son promovidas a través de la Alianza para el Gobierno Abierto, lanzada formalmente el 20 de septiembre de 2011 cuando los 8 gobiernos fundadores (Brasil, Indonesia, México, Noruega, las Filipinas, Sudáfrica el Reino Unido y los Estados Unidos) suscribieron la Declaración de Gobierno Abierto y anunciaron sus planes de acción nacionales. Luego fueron incorporándose alrededor de 60 países (hoy son 66), la mayoría en los primeros 3 años, adhiriéndose cada vez menos estados por año.

Es dable destacar que es una iniciativa multiactoral, que busca incorporar diversos actores de la sociedad civil, universidades, Ong´s, empresas y gobiernos. Sin embargo, quedan fuera otro tipo de asociaciones, como las gremiales, que no son considerados dentro del esquema planteado.

Los compromisos de la OGP (Open Government Partnership, por sus siglas en inglés) se centran en 3 ejes fundamentales: Rendición de Cuentas o Transparencia, Colaboración y Participación Ciudadana.

La Jornada del pasado 4 de marzo buscó difundir y fomentar la implementación de políticas de apertura de datos públicos mejorando la rendición de cuentas, transparencia, y participación ciudadana, así como la reutilización de los mismo.

Cabe aclarar que no todo dato publicado entra dentro de la categoría de "dato abierto", y aquí tenemos que distinguir categorías y establecer criterios:

Son considerados datos abiertos, todos aquellos datos que son accesibles y reutilizables, sin exigencia de permisos específicos, y se encuentran respetando estándares. Es decir, que deberían ser tablas sin formato, que puedan ser leídas por cualquier sistema, sin adoptar tecnologías propietarias. Además, la descarga y el acceso no debe estar vedado por captcha, o contraseñas, sino que deben poder ser relevados o recopilados por sistemas sin encontrar obstáculos que requieran de la intervención humana, o algún tipo de conversión. E incluso, pueden ser datos enriquecidos con vínculos a otros datos.

No podemos dejar de referirnos al sistema de 5 estrellas utilizado para hablar de datos abiertos. Fué Tim Berners-Lee, el inventor de la Web e iniciador de los Datos Enlazados (Linked Data), quién lo sugirió, y es el siguiente:

* : En este nivel, los datos están publicados en la web, como sea. Es decir, en cualquier formato (por ejemplo en un PDF no modificable)

**: El segundo nivel es para aquellos datos publicados, pero en tablas que permitan la sistematización. (ej: Excel en vez de una imagen de una tabla escaneada)2

***: El tercer nivel queda reservado para aquellos datos publicados en tablas en formatos no propietarios. (ej: CSV en vez de Excel)

**** Un cuarto nivel agrega URI´s para denotar cosas en los datos.

***** El máximo nivel enlaza los datos a otros datos y enriquece el contexto.

Cada nivel de datos abiertos permite ventajas sobre el anterior, tendiendo a una mayor utilización y reutilización de los mismos. Es una temática interesante que espero podamos tratar en otro artículo.

Volviendo al evento, el "Open Data Day" es una iniciativa lanzada en 2010 por la fundación Open Knowledge. Consiste en un conjunto de actividades por todo el mundo para la promoción de una cultura de datos científicos, meteorológicos, culturales, financieros, ambientales, estadísticos y de transporte entre otros.

La Fundación Conocimiento Abierto estuvo a cargo del evento en Argentina, y realizó un excelente trabajo con la organización en el Centro de Convenciones de Vicente López. Acompañaron los sponsor como "Here", y el Municipio de Vicente López, que facilitaron el lugar mas que confortable, en donde pudimos disfrutar de las charlas y de un

almuerzo al aire libre en un día que tuvo su pequeña llovizna, pero que no entorpeció las actividades.

El evento contó con varios paneles que trataron temas como "¿Es posible un Estado abierto?", con la participación de Agustin Frizzera, Mariano Heller y la Diputada Nacional Karina Banfi.

Un segundo panel que trató la temática de "Los datos para el fortalecimiento ciudadano", con participación de Romina Colman, Andrés Vázquez, Agustina De Luca, Valentín Muro y Paula Moreno Frers.

Y un tercer panel sobre "Datos abiertos en municipios", con la participación de Ana Lis Rodríguez, Mariano Mosquera, Cecilia Lucca, Bruno Cataldi y Marcelo Cossar.

Luego de las charlas, y con el estómago lleno, se abrieron las mesas de diálogo con referentes de las diversas temáticas, entre las que se encontraban: Gobiernos y apertura de datos, ¿Cuáles son los datos relevantes para los ciudadanos?, Desarrollo de Software libre para potenciar la transparencia activa, Los Objetivos para el Desarrollo Sostenible (ODS) y datos abiertos, Como los datos pueden ayudar a la equidad e igualdad de género, Cómo generar valor socio económico con datos públicos, El impacto de los datos abiertos: ¿Cómo medir resultados?, Desafíos para la apertura de Datos Abiertos en los Municipios, Periodismo de datos y Justicia Abierta. Todas mesas sumamente interesantes, con varios integrantes, y con conclusiones plasmadas en afiches y luego expuestas en una corta presentación.

Feliz día de los datos abiertos 2017!

Fotos: gentileza de Fundación Conocimiento Abierto.

CIBERSEGURIDAD Y SOCIEDAD DIGITAL

Desafíos Sociales Empresariales y Gubernamentales

Talleres Prácticos de 4 Hrs.

Cómo combatir el Cibercrimen sin morir en el intento
Viernes 19 de 08:30 - 12:30 (25 Plazas)

Manejo de Evidencia Digital en Procesos Judiciales
Viernes 19 de 13:00 - 17:00 (25 Plazas)

18 y 19 de Mayo 2017

Hotel El Panamá
Convention Center & Casino

CUPOS LIMITADOS

Conferencias: Jueves 18, Hrs. 08:00 - 17:00

- Miguel Sumer Elias
  El Cibercrimen solo pasa en las noticias
- Guillermo Zamora
  El desafío en el uso responsable de las Tecnologías
- José Vega
  Infracción de Marcas en Internet ¿Oportunidad para el Cibercrimen?
- Augusto Ho
  Análisis de la Ciberseguridad en América Latina
- Alvaro Andrade
  Tu Seguridad a través de los ojos de un Hacker

Inversión:

Entrada a Conferencias: B./ 50

Conferencia + Taller: B./ 150

Ambos Talleres: B./ 200

Reservas e Inscripciones

(+507) 3873850 (+507) 69836454 info@ehcgroup.io

Ethical Hacking Consultores · APANDETEC Derecho y Nuevas Tecnologías · fiadi · La Red ElDerechoInformatico.com · Hullmarn & Co.- Abogados

CHILD GROOMING. ALCANCES DE UNA NUEVA REALIDAD DELICTUAL (*)

Autor: José María Cifuentes Villanueva.

I.- La exposición de los niños y niñas en la red. II.- Child Grooming. III.- Fases del hostigamiento. IV.- Recomendaciones

I.- LA EXPOSICIÓN DE LOS NIÑOS Y NIÑAS EN LA RED

El avance de las redes sociales en la vida diaria ha significado una verdadera revolución que no sólo nos obliga a estar más actualizados en lo que respecta a las nuevas tecnologías de la información y la comunicación, sino que a su vez requiere extremar los recaudos cuando los usuarios finales de la tecnología son los más chicos.

El acceso a internet y la publicación de nuestras vidas en la red ha provocado un fenomenal cambio social en el que la personalidad se ve expuesta como nunca antes. La transmisión masiva de fotos y videos, así como la asistencia a determinados eventos, las preferencias de lectura o de series en streaming, por dar solo unos ejemplos, son símbolos de una nueva era.

El tema se pone más serio cuando vemos que la Argentina se encuentra entre los primeros veinte países en el ranking de acceso a internet, según un informe de The Economist publicado recientemente. Este estudio analizó la calidad y amplitud de la infraestructura nacional, el costo de acceso, la existencia y alcance del contenido del idioma local y la capacidad de acceso incluyendo habilidades, aceptación cultural y políticas de apoyo; todo sobre una base de setenta y cinco países.

Ahora bien, la consultora Markwald, La Madrid y Asociados publicó un estudio denominado Kidditos que fue realizado con 502 niños y niñas de nuestro país de entre 4 y 5 años de edad. Los resultados son llamativos. El 100% de los menores entrevistados tienen al menos un celular en su casa. El 74% posee computadora y el 55% tiene acceso diario a internet (dato que coincide con las estadísticas de The Economist). El 54% sabe utilizar tabletas y el 64% computadoras. A la hora de utilizar el celular, el 56% lo hace para jugar con aplicaciones y el 10% para ver videos. Piensen un segundo los riesgos que corren los niños en este momento.

Los Echo Boomers, también conocidos como Generación Y o Millenials, ya no recuerdan cómo era el mundo antes que existiera internet. Y mejor aún, los nacidos en la era de la World Wide Web (www) no conciben el mundo sin la red.

Todo este panorama nos lleva a una conclusión: nativos e inmigrantes digitales debemos conocer las potencialidades que ofrece internet para resguardar la integridad de nuestros hijos y aprovechar al máximo las herramientas que esta nueva era nos brinda.

En este sentido, el Congreso Nacional sancionó el 13 de noviembre de 2013 la Ley N° 26.904 (B.O. 11/12/2013) conocida como “Ley de Grooming” que incorpora el art. 131 al Código Penal Argentino.

Dicho texto establece que "*Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma". Su sanción fue motivo de diversos debates en el Congreso Nacional, cuyo análisis será motivo de nuestro próximo trabajo.*

II.- CHILD GROOMING

El vocablo Grooming deriva del inglés *groom*, y alude al acicalado social que realizan los animales gregarios al limpiarse entre ellos, desparasitarse o cuidar del cuerpo y la apariencia de los semejantes.

El término Child Grooming o Internet Grooming, comenzó a utilizarse para significar al proceso gradual de acciones que lleva a cabo un mayor de edad para ganarse la confianza de un niño o niña creando una conexión emocional a través de diversas tecnologías de comunicación con el fin de disminuir las inhibiciones del niño y cometer un delito contra la integridad sexual.

Hoy en día el Child Grooming es la herramienta más usada por los pedófilos en las redes sociales y este es el peligro que se torna complicado al contrastar las estadísticas de acceso de menores de edad a la red en nuestro país.

Lo dicho no implica que tengamos que prohibir que los niños utilicen la tecnología, todo lo contrario, debemos permitirles su utilización estando siempre atentos y enseñándoles los beneficios y los riesgos a los que se verán expuestos.

III.- FASES DEL HOSTIGAMIENTO

Cuando un ciberhostigador contacta a un niño o niña menor de edad a través de internet, intenta llevar a cabo las siguientes acciones: obtener imágenes íntimas de índole sexual del menor, enviarle imágenes de similar tenor y establecer diálogos de confianza con contenido sexual.

Estas acciones tienen como finalidad disminuir las inhibiciones del menor fingiendo empatía y cariño, obteniendo así el marco propicio para lograr algún tipo de satisfacción sexual indirecta (sin encontrarse físicamente) o directa (propiciando un encuentro en algún lugar).

Todas las acciones llevadas a cabo por el ciberhostigador tienen directa relación con los delitos contra la integridad sexual como los abusos sexuales, la corrupción de menores, la pederastia, la pornografía infantil en internet y la prostitución infantil. Si bien cada caso es único, por lo general se pueden distinguir tres fases de Child Grooming: 1. El

primer contacto del groomer tiene como finalidad hacerse de la confianza del menor simulando una amistad; 2. Ese amigo virtual comienza a obtener mayores detalles de la vida del niño y por lo tanto va formando un vínculo emocional mucho más afianzado que en los primeros diálogos. Por lo general en esta etapa comienza el intercambio de fotos o videollamadas con algún término sexual esporádico y 3. El contenido sexual se transforma en el centro de la relación digital y comienza la transmisión de imágenes y/o videos de contenido sexual explícito.

Si la confianza con el niño se mantiene, esta relación puede prolongarse en el tiempo sin que nadie lo perciba. De allí lo peligroso de permitir que los menores tengan libre disponibilidad de computadoras, tabletas o celulares sin supervisión.

Ahora bien, cuando esa confianza se rompe, aparece la extorsión. El groomer exige al menor que continúe transmitiéndole fotos o videollamadas con contenido sexual explícito y, si el niño se niega, lo amenaza con todo tipo de argumentos: desde la publicación de videos y fotos personales a todos sus contactos y familiares hasta la muerte de sus padres. Es aquí donde más cuidado debemos tener.

Ello se debe a que las víctimas reaccionan de manera muy disímil dependiendo su edad y personalidad. Si el niño o niña no se animan a contar lo que les sucede por vergüenza o miedo, se cierran sobre ellos mismos y no les resulta para nada fácil superar la situación. Muchas veces es preciso que profesionales de la salud los asistan para ayudarles a salir del trance vivido. Aún en los casos en que las víctimas han dialogado esta situación con alguna persona de confianza les cuesta tiempo sobreponerse.

III.- RECOMENDACIONES

El sitio Internet Grooming (www.internet-grooming.net), enumera ocho consejos útiles para evitar el grooming, los que pasamos a detallar:

1.- Ubicación de la computadora

Colocar la computadora en un lugar de paso de la casa o en un espacio común y de uso frecuente (por ejemplo el salón), desde donde poder observar el uso que hacen los niños y niñas de él. Evitar instalarla en el cuarto de los niños y niñas.

Debemos tener en cuenta que, hoy en día, los dispositivos más utilizados para conectarse a internet son los celulares, lo que dificulta este tipo de protección. Por tanto, conviene que cuando se conecten a Internet, lo hagan en un espacio común.

2.- Cuidado con el malware

Seguir los consejos de seguridad generales para mantener los dispositivos libres de virus y otro malware que podría revelar nuestras claves a los groomers. Instalar un buen antivirus y un buen cortafuegos y mantenerlos actualizados con la mayor frecuencia posible. Advertir a los niños de que nunca deben descargar archivos procedentes de personas que no conozcan bien.

3.- Webcam

Evitar la instalación de cámaras web (webcams) o restringir su uso mediante algún programa o mediante claves o controles parentales que algunos modelos ya incorporan. Si además la computadora está en un lugar no privado, aumentaremos la seguridad en los casos en que les permitamos usar la cámara.

4.- Educación, educación y más educación

La base de toda medida de protección de los menores

en la Red es la educación, no el disponer de unas u otras tecnologías, que siempre pueden fallar. Por tanto, debemos explicarles a nuestros hijos e hijas cuáles son los peligros de la Red y las medidas de protección básicas para evitar cada uno de ellos: en este caso, por ejemplo, no revelar nunca sus datos personales ni sus claves a conocidos de Internet.
Los adultos también debemos aprender a manejar las nuevas tecnologías para saber qué hacen los niños y niñas cuando están conectados y cuáles son los riesgos que deben afrontar.

5.- La importancia del nombre

Es más seguro, en general, y muy usual desde los inicios de Internet, utilizar un sobrenombre (nickname) en vez de los nombres y apellidos propios. Explique a sus hijos que deben evitar usar en Internet sobrenombres (nicks) que revelen su sexo o su edad. Deles ejemplos de nombres neutros que les puedan gustar.

6.- Conocer a sus amigos

Es importante que conozcamos quiénes son sus contactos en la Red, por tanto revisar con ellos su agenda de contactos en el chat, en la mensajería instantánea, en las redes sociales nos permitirá estar al día de sus intervenciones digitales.

7.- Proteger los datos

Explicar a los niños que no deben rellenar formularios en los que den datos personales suyos, de amigos o conocidos o de su familia. Siempre deberían contar con su presencia para completar este tipo de cosas y pedirles aprobación antes de apretar la tecla “enter”.

8.- La hora de ir a la cama

Es conveniente evitar que chateen a partir de cierta hora, como las 10 de la noche. Es conveniente ponerles una norma al respecto y vigilar que la cumplan.

En resumen, debemos permitir que los niños y niñas puedan utilizar las nuevas tecnologías, acompañándolos en el proceso de conocimiento de todo su potencial y comprendiendo la relevancia de proteger su vida íntima a fin de no caer en manos de ciberdelicuentes que permanecen a la espera de una víctima desprevenida.

(*): Autor: José María Cifuentes Villanueva. Abogado; egresado de la Pontificia Universidad Católica Argentina (2009); Secretario de Fiscalía General del Departamento Judicial Pergamino (Ministerio Público Fiscal de la Provincia de Buenos Aires – República Argentina), Docente por concurso de la Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA) de la cátedra Derecho Público.

librería | hammurabi

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

en preparación

Colección «elderechoinformático.com»

11 volúmenes

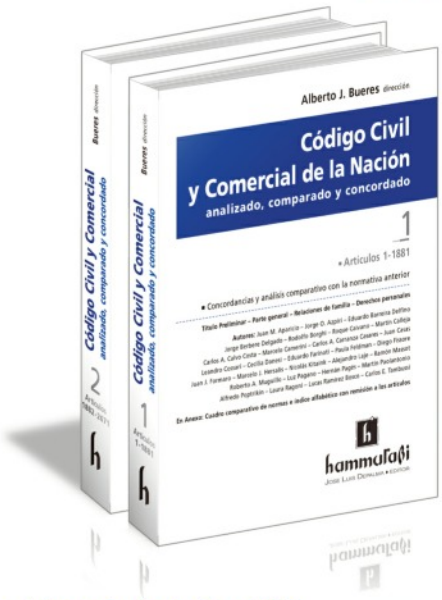
Guillermo M. Zamora dirección

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.

2017
La Red EDI

En crecimiento constante

EDI - La RedIBEROAMERICA

Facebook.com/elderechoinformatico | www.elderechoinformatico.com
Twitter: elderechoinf

La difícil tarea de ser Cyberpapàs

Autora: Natalia Toranzo

Cuando era una niña las recomendaciones de mis padres era que no hablara con extraños, que no aceptara nada de extraños, que no hablara cuando los mayores lo hacían, que jugara siempre a la vista de ellos, que no llevara amig"o"s a mi casa cuando ellos no estaban –mi inocencia no me permitía darme cuenta porquè no podía-.

Iba creciendo y esas recomendaciones las tenía grabadas a fuego en mi consciente, subconsciente, inconsciente y todas las formas de "sciente" posibles y en una especie de película fui viviendo situaciones en las que aquellas palabras me ayudaron a resguardarme y resguardar a otros también.

Al llegar a mi adultez uno se desenvuelve con total naturalidad en el mundo y las relaciones interpersonales se vuelven normales hasta que a uno le llega, me llegó, el momento de ser mama (feliz por cierto) de un bello nene que hoy tiene 3 años y vuelven a resurgir las palabras de mis padres en cuanto a los cuidados que debemos tener. Hoy es doble trabajo inculcarle a nuestros hijos: que no hable con extraños y que no chatee con extraños, que no acepte nada de extraños y que no acepte invitaciones en redes sociales de extraños, que juegue a la vista de los adultos y que tenga total transparencia de lo que hace en internet, que no lleve amig@s a mi casa cuando nosotros no estemos y que no chatee con niñ@s que no conoce porque pueden no ser niñ@s en realidad. Sin contar que uno debe inculcarles que no se les pega a sus amigos, que deben compartir, que deben… y deben… pero a la vez están mirando videos en Youtube (kids) y en la televisión en donde van asimilando hay malos y buenos, que hay personas que pegan y se la devuelven, que hay personas que lastiman a otras. Como lo que me paso hace unos días y que es lo que me llevo a escribir estas líneas: yo cocinando y mi hijo jugando en el patio con su pistola de agua, de pronto escucho que se abre la puerta y entran mis 3 perros aterrorizados intentando escapar y mi hijo atrás disparándoles agua y riéndose cual villano como en los videos que ve en Youtube (que por cierto le sale igual la risa para mi asombro y desesperación en parte). Por supuesto que le dije que eso está mal, que los perros se asustan, que eso no les gusta y el me aseguraba "Si le busta mama". No hablemos que es fanático del Hombre Araña y que intenta subirse por las paredes.

Entonces mi cabeza empezó a recorrer miles de imágenes y textos que gracias a mi profesión de informática y conocimientos de delitos informáticos he ido adoptando estos últimos años y pienso, pobre mi hijo que nació en esta era digital y pobres

nosotros que DEBEMOS estar a la altura de las circunstancias, por lo tanto doble trabajo como padres.

En este preciso momento es cuando pienso que debemos convertirnos en Cyberpapas. Si bien todas las amenazas en el mundo real ya los adultos las conocemos, considero que sea la tarea o trabajo que cada padre tenga es imperativo conocer las amenazas a que nuestros hijos están expuestos en Internet. Para ello por un lado debemos conocer que existen leyes que sancionan hechos ofensivos cometidos a través de la red y por otro lado, como adultos, ser sumamente conscientes y cuidadosos en cómo nos comportamos en internet asumiendo que los riesgos existen y pueden ser mortales para nuestros hijos.

Un error muy común, a veces grave, que lo veo a diario es que la mayoría no configura su cuenta de Facebook, por ejemplo, con perfil privado. Una mama o papa que publica fotos con su hij@ de 8 años en las vacaciones jugando en el agua, otra en su primer día de escuela luego una foto en la plaza con la leyenda “en su plaza preferida” y etiquetándol@. Listo! para un pedófilo es información muy valiosa, sabe cuál es su perfil de Facebook, sabe a qué escuela va y sabe a qué plaza va siempre. Este Pedófilo puede hacerse pasar por un niño de 8 años, agregarlo como amigo, hacerse el amigo y luego pedirle fotos en malla o bombacha, luego las amenazas para que no diga a sus padres lo que está viviendo. -Para tanto va a ser? – Si para tanto! Esto pasa! Y cada vez más. Esto es un Delito, está penado por la ley, y se llama **Grooming** un acto con fines exclusivamente sexuales.

En noviembre de 2013 la Cámara de Senadores aprobó la Ley 26.904, Ley de Grooming, en donde dispone “Artículo 131: Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.”

El acoso en general, hoy denominado **Bulling**, es el acoso físico y/o psicológico al que someten, de forma continuada, una persona o grupo a otra. Este acoso también se da en la escuela entre niños o adolescentes.

Con el uso de los teléfonos celulares que tienen cámara de fotos o las notebook o tablets conectadas a internet las 24 horas del día este acoso se desprende el **Cyberbulling** que es el acoso realizado por medios tecnológicos o digitales, de los cuales algunas características son:

•La mayoría de los acosadores intentan dañar la reputación de la víctima manipulando a gente contra él.

•Publicar información falsa sobre las víctimas en sitios web.

•Monitorizar las actividades de la víctima en internet.

•Los ciberacosadores pueden espiar a los amigos de la víctima, su familia y compañeros de trabajo para obtener información personal.

•Envíar de forma periódica correos difamatorios al entorno de la víctima para manipularlos.

En este sentido existe "Desamparo legal de estas formas de acoso, ya que aunque cierren un sitio web con contenido sobre la víctima, puede abrirse otra inmediatamente.

El Ciberacoso, al tratarse de una forma de acoso indirecto y no presencial, el agresor no tiene contacto con la víctima, no ve su cara, sus ojos, su dolor, su pena, con lo cual difícilmente podrá llegar a sentir empatía o despertar su compasión por el otro. El ciberacosador obtiene satisfacción en la elaboración del acto violento y de imaginar el daño ocasionado en el otro, ya que no puede vivirlo en su lugar." (extracto obtenido de https://es.wikipedia.org/wiki/Ciberacoso).

Ahora veamos, una chica o un chico se saca una foto con su teléfono, tablet, notebook con poca ropa o sin ropa en alguna postura con tono sensual/sexual. Hasta acá todo bien porque esa foto queda para el/ella y no está cometiendo ningún delito. Ahora decide enviársela a otra persona con total consentimiento y tampoco es delito. Hoy esta actividad se la denomina **Sexting**. Seguimos, esta persona la publica en redes sociales, se la envía a otras personas sin el consentimiento de quien se sacó la foto y esa foto comienza a circular por internet, puede llegar a manos de pedófilos si quien se sacó la foto es menor y puede suceder que quien posea la foto logre contactarlo y comenzar las amenazas para que envíe mas fotos, por ejemplo. Esto también está penado por la ley.

Pedofilia, Pornografía infantil, son términos relacionados a la excitación o placer sexual relacionados a actividades sexuales con niños menores de 14 años. En este sentido está penado por la Ley 26388 tanto la divulgación, comercialización, distribución como la tenencia de imágenes con detonación sexual de menores de 18 años.

Los niños y adolescentes necesitan tener la contención emocional de sus padres o quienes estén a cargo de ellos. Deben encontrar en nosotros la confianza de poder decirnos si están siendo amenazados, si alguien que no conocen les pide fotos desnudos, si alguien que no conocen los invita a tomar un helado o los invita a algún lugar "cómodo", si algún compañerito o amigo les dice cosas que los hace sentir tristes o incomodos. Por este motivo es necesario que como adultos le demos la importancia que esta problemática merece, no minimizar los riesgos, interiorizarse de las redes sociales que existen, en cuales se mueven nuestros hijos y estar atentos a los cambios de actitud que puedan tener. Saber con quienes se relacionan, resguardar su identidad tanto en nuestros perfiles en las redes sociales como en sus propios perfiles si es que ya tienen acceso a las redes, no publicar imágenes con perfil público, no enviar imágenes a personas que no conozcan, no etiquetar a nuestros hijos en ninguna foto y estas son algunas recomendaciones que puedo ofrecer para concientizar y estar atentos.

Natalia S. Toranzo
-Licenciada en Informática, Perito Informático, Docente, en constante especialización en delitos y derecho informático.

Ethical Hacking Consultores

Nuestros Servicios

- Security Penetration Testing
- Auditoria y Certificación de ATM's
- Informática Forense
- Auditorias Especializadas
- Asesoramiento en Derecho Informático
- Inteligencia Informática
- Entrenamiento en Seguridad
- Soluciones Big Data

Nuestros Productos

pentest365

- Pentesting Persistente desde la Nube
- Identificación automatizada de Tecnologías, Vulnerabilidades y Exploits
- Monitoreo de Seguridad 24x7x365
- Alertas en tiempo real
- Escaneo de puertos Programable
- Dashboard Perzonalizable
- Reportes con cumplimiento PCI v3

K&S

- Reducción del fraude en ATMs
- Monitoreo y Seguridad en tiempo real
- Servicios y Salud del ATM 24x7
- Alertas en tiempo real ante incidentes
- Agilidad en la investigación Forense
- Reportes con cumplimiento PCI v3
- Dashboard 100% personalizable
- Protección Multivendor

TMFdesk

- Call Center por Redes Sociales
- Sistema distribuido de mensajes
- Administración de multiples Redes Sociales al mismo tiempo
- Administración de histórico de Chats
- Estadisticas de atención por Agente
- Respuestas Automáticas y Enlatadas
- Reportes automáticos.

FIRMADOR

- Firma Electrónica
- Correo Electrónico Certificado
- Firma de Documentos Online
- Testigo Digital Online
- Sello HTTP Seguro
- Factura Electrónica
- Firma de Transacciones

Visitanos: www.ehcgroup.io Contactanos: (+507) 3873850 | info@ehcgroup.io

EXTERNALIDADES AMBIENTALES DE LA INDUSTRIA TECNOLÓGICA:

Residuos de aparatos eléctricos y electrónicos

BÁRBARA VIRGINIA PEÑALOZA

Son innegables los beneficios y ventajas que la tecnología ha aportado a la humanidad. La sociedad de la información en la que estamos insertos ya no tiene fronteras ni límites geográficos, la inmediatez en las comunicaciones, el acceso ilimitado a la información, el confort que los aparatos electrónicos nos aportan en lo cotidiano hacen que la tecnología ocupe un papel fundamental en la vida de cada individuo y en el desarrollo de las empresas, la ciencia y los Estados.

Tales beneficios, sumados a las conductas de consumo que ya se han arraigado en nuestra sociedad, motivan a cada individuo, a las empresas y al mismo Estado a adquirir aparatos eléctricos y electrónicos, y al consiguiente desecho de los mismos en un corto período de tiempo, ya sea porque la industria tecnológica desarrolla nuevos aparatos que cubren más necesidades que los anteriores, porque dichos aparatos tienen una vida útil preestablecida por el productor, o porque es muy costosa o imposible su reparación. Esto es lo que se conoce como “obsolescencia programada”

El aumento de este tipo de residuos se traduce en la socialización de una de las externalidades negativas de esta industria: la contaminación ambiental y el daño a la salud de las personas, provocados por una gestión inadecuada de los aparatos eléctricos y electrónicos al llegar al final de su vida útil.

Ahora bien, ante este panorama, debemos preguntarnos ¿quién debe responder por cada uno de los aparatos eléctricos o electrónicos al llegar al final de su vida? ¿Quién debe soportar el costo ambiental que provoca la inadecuada gestión de este tipo de residuos que se acumulan vertiginosamente? entre quienes debe repartirse el costo ambiental de este tipo de residuos.

Externalidades ambientales

Según Gregory Mankiw, una externalidad surge cuando una persona se dedica a una actividad que influye en el bienestar de un tercero al que no se le paga ni se le compensa por dicho efecto. Si el impacto sobre el tercero es negativo, se conoce como externalidad negativa. Si le beneficia, se llama externalidad positiva. En presencia de externalidades, el interés de la sociedad en el resultado del mercado va más allá del bienestar de los compradores y

vendedores que participan en el mercado para incluir el bienestar de terceros que resultan indirectamente afectados. 1

En el caso de la industria tecnológica, se pueden diferenciar externalidades positivas y negativas. Respecto a las primeras no es necesario indagar demasiado, es que los beneficios que trae aparejados el avance tecnológico son indiscutibles.

Respecto a las externalidades negativas de esta industria, son la contaminación ambiental y el daño a la salud de las personas, provocados por una inadecuada gestión de los residuos eléctricos y electrónicos las más preocupantes y las que requieren de un pronto abordaje jurídico y económico.

Algunas cifras

Según el último Monitoreo Global de e-waste[2] efectuado por la Universidad de Naciones Unidas en 2014, se estima que la cantidad total de basura electrónica generada a nivel mundial en 2014 fue de 41.8 millones de toneladas métricas (Mt). Se pronostica que para 2018 dicha cantidad aumentará a 50 Mt. Esta basura electrónica está compuesta por 1.0 Mt de lámparas, 6.3 Mt de pantallas, 3.0 Mt de pequeños equipos de la tecnología de la información (como teléfonos móviles, calculadoras de bolsillo, ordenadores personales, impresoras, etc.), 12.8 Mt de pequeños equipos (como aspiradoras, microondas, tostadoras, máquinas de afeitar eléctricas, cámaras de vídeo, etc.), 11.8 Mt de equipos grandes (como lavadoras, secadoras, lavaplatos, estufas eléctricas, paneles fotovoltaicos, etc.) y 7.0 Mt de refrigeración

[1] MANKIW, N. Gregory, Microeconomía, Versión adaptada para América Latina, 6ta edición (Cengage Learning 2014). Capítulo 10 “Externalidades” pág 196

[2] C.P. BALDÉ. - F. WANG- R. KUEHR -J. HUISMAN, The global e-waste monitor – 2014, Quantities , Flows and resources, United Nations University, IAS – SCYCLE, Bonn, Germany (2015), pág. 8 y 64.

y equipos congelantes (equipos de temperaturas de cambio).

Según el mismo informe, en Argentina en 2014 se generaron 292 kilotones (KT) de basura electrónica y se calcula que cada habitante genera un promedio de 7 Kg de residuos de este tipo al año.

Residuos electrónicos y la necesidad de una regulación especial

Lo que distingue a los RAEE del resto de los residuos y hace necesaria una gestión diferenciada de los mismos, principalmente son sus componentes, pues estos son de diversa naturaleza, y algunos de ellos son considerados "potencialmente peligrosos", por lo que una vez desechados inadecuadamente se transforman en residuos peligrosos[1].

Los residuos electrónicos contienen, entre otros contaminantes, metales pesados como cadmio, plomo y níquel, además de mercurio y plásticos bromados. Durante su vida útil, estos componentes son inofensivos, ya que están contenidos en placas, circuitos, conectores o cables, pero al ser desechados, si toman contacto con el agua o la materia orgánica, reaccionan liberando tóxicos al suelo y a las fuentes de aguas subterráneas. Debido a su carácter no biodegradable, estos desechos atentan contra el ambiente y la salud de los seres vivos.

A su vez, los aparatos eléctricos y electrónicos también contienen elementos valiosos en su interior, tales como oro, plata, estaño, cobre, metales ferrosos (hierro), metales no ferrosos (aluminio), entre otros, lo que lleva a recolectores informales que forman parte del circuito de la basura a desmantelar los aparatos caídos en desuso, sin ningún tipo de protección sanitaria, en el afán de extraer dichos materiales y comercializarlos, desechando el resto del residuo inadecuadamente, lo que permite que los componentes peligrosos entren en contacto con el aire, el agua y el suelo, desatando su poder contaminador.

En la actualidad, tanto a nivel nacional como provincial, el manejo de la basura electrónica es inadecuado, pues no existe regulación de ningún tipo que establezca un mínimo de presupuestos o de buenas prácticas en materia de gestión de residuos de aparatos eléctricos y electrónicos, lo que se traduce, por un lado, en un riesgo para la salud de las personas y para el medioambiente y, por otro lado, en la pérdida en rellenos sanitarios o basurales de residuos sólidos de aquellos componentes valiosos que pueden ser recuperados adecuadamente para su reutilización o reciclaje, lo que brindaría oportunidades de trabajo y de integración a los recolectores informales o pequeños emprendedores que pueden intervenir en las etapas de recolección, tratamiento y disposición final de los mismos, actividad que actualmente se denomina "minería urbana" o "minería inversa".

Por otra parte, algunos de los aparatos eléctricos y/o electrónicos tienen un alto potencial de reutilización, como es el caso de los computadores, lo que puede tener impactos socioeconómicos relevantes al contribuir –en países en vías de desarrollo– a la superación de la brecha digital y de conocimiento a través del acceso, uso y aprovechamiento de las tecnologías de la información y de las comunicaciones.

Concluyendo

El aumento de residuos eléctricos y electrónicos y su manejo informal es un problema que ha llegado para quedarse y es lo que ha motivado

[1] Anexo I de la Ley Nacional Nº 24.051 con características de peligrosidad del Anexo II de la misma norma

al autor a redactar estas líneas, a los fines de contribuir en la toma de conciencia de la magnitud de esta problemática y de la importancia de tomar medidas preventivas para evitar desastres ambientales mayores en el futuro.

Partimos preguntándonos quién debe afrontar el costo ambiental que provoca la inadecuada gestión de este tipo de residuos. Luego de analizar la problemática de los RAEE como externalidad negativa de la industria tecnológica podemos concluir que es indispensable un cambio de paradigma, el cual implica un compromiso social, empresarial y estatal, que se traduce en la participación activa y proactiva de los diferentes actores, entre quienes debe repartirse el costo ambiental de este tipo de residuos, con el fin de prevenir daños a la salud de las personas y al ambiente.

Por un lado, se requiere de un marco legal que regule el tratamiento de estos residuos, en el que se prevean mecanismos de control y se fijen sanciones para el incumplimiento. Deben prohibirse prácticas abusivas, tales como la alteración de los aparatos eléctricos con el fin de acortar su vida útil, así como también debe exigirse un diseño ambientalmente amigable y que permita la desmantelación y reciclaje de los aparatos cuando lleguen al final de su vida útil.

Por su parte, los fabricantes, productores y empresas comercializadoras de aparatos eléctricos y electrónicos, , deben cumplir con requisitos mínimos de calidad y durabilidad de sus productos, utilizando materiales amigables con el medioambiente. También deben asegurar al consumidor un servicio postventa de reparación a costos razonables en comparación con los valores del producto nuevo; la comercialización de piezas de repuesto y garantías extendidas de los productos.

Finalmente los consumidores deben redefinir su rol y tomar conciencia del impacto ambiental que un consumo desmedido e innecesario provoca. Es importante que los consumidores adopten un rol activo contra prácticas poco éticas como la obsolescencia programada, así como también que opten al momento de adquirir bienes por aquellos que son más amigables con el medioambiente. También es necesario que el consumidor se responsabilice de la manera en que desecha sus productos cuando estos caen en desuso.

La tensión que ejercen sobre el medioambiente los actuales niveles y pautas de consumo, traducida en el deterioro de los recursos renovables, el daño provocado por la contaminación y el problema de la eliminación de los desechos, afecta a los seres humanos desigualmente, en materia de salud, medios de vida y seguridad, de allí la importancia que el paradigma de consumo sustentable tiene.

Asimismo, el desarrollo sustentable como principio rector en la configuración de las políticas públicas, en la producción y también en el consumo y la consagración constitucional del derecho a vivir en un ambiente sano, hacen que la gestión ambientalmente adecuada de los residuos se haya convertido en una cuestión de derecho y un deber del Estado.

Más que un blog.
Toda la actualidad jurídica.

información jurídica ágil, eficiente y relevante

aldiaargentina.microjuris.com

Llámenos (5411) 5031-9300

microjuris.com
inteligencia jurídica

ILUSTRE COLEGIO DE ABOGADOS DE LIMA

DIRECCIÓN DE COMISIONES Y CONSULTAS
Comisión Ejecutiva de Derecho Informático, Tecnologías de la Información y las Telecomunicaciones.

"Primer Taller de Derecho Informático y Tecnologías de la Información - TIC"

DÍAS:

Jueves 4 y viernes 5 de mayo de 2017

09:00 a 17:00 hrs.

LUGAR:

SALA JOSÉ GALVEZ EGÚSQUIZA
Colegio de Abogados de Lima
Av. Santa Cruz 255 Miraflores

VACANTES LIMITADAS

CERTIFICACIÓN PREVIA INSCRIPCIÓN

CODIGO DE PAGO
TA083
S/.30.00
ASISTENCIA CONFIRMADA

INFORMES: DIRECCIÓN DE COMISIONES Y CONSULTAS:
Telf.: 7106657 / 7106616
Email: comisionesyconsultas2016@gmail.com

TEMAS:

- Derecho Informático
- Informática Jurídica
- Gobierno Electrónico
- Firma Digital
- Telecomunicaciones y TIC
- Las Microformas Digitales - Requisitos y Finalidad
- Contratos por Internet y Economía Colaborativa
- Internet y Redes Sociales - Privacidad y Buen Uso

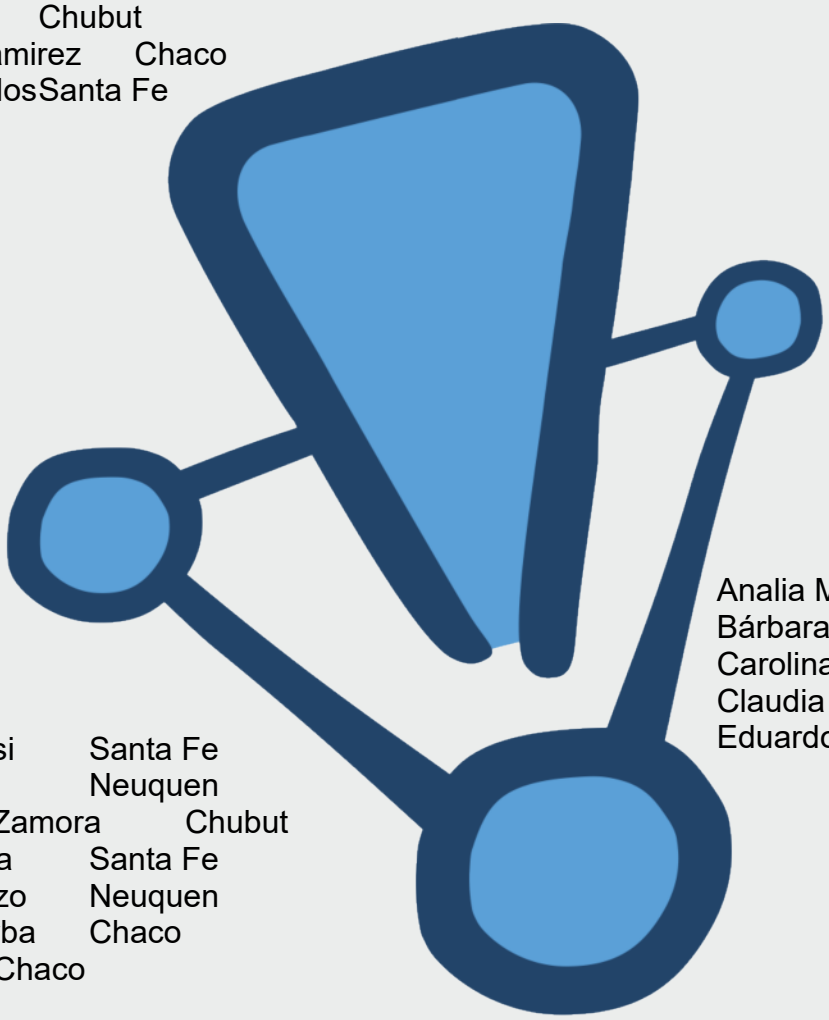
EDDA KAREN CÉSPEDES BABILÓN
Presidenta Comisión Ejecutiva de Derecho Informático, Tecnologías de la Información y Telecomunicaciones - TIC
Ilustre Colegio de Abogados de Lima

PEDRO M. ANGULO ARANA
Decano

WILLIAM CONTRERAS CHAVEZ
Director de Comisiones y Consultas

https://docs.google.com/forms/d/e/1FAIpQLSfLD3hdlSBcVfAkP3K-elEhfBdP1aqdexzkDz9tdxXF9EAF9w/viewform?c=0&w=1

Cecilia Cristina Lara Sgo del Estero
Valeria Cecilia Acosta Sgo del Estero
Juan Martín García Santa Fe
Lucia Masciotra Chubut
Carlos Alberto Ramirez Chaco
Rubén Darío Ávalos Santa Fe



Analia Martinez Santa Fe
Bárbara Virginia Peñaloza Mendoza
Carolina Marín Chubut
Claudia Williams Chubut
Eduardo Escobar Chaco

Facundo Rossi Santa Fe
Gladys Mella Neuquen
Guillermo M. Zamora Chubut
Juan Quaranta Santa Fe
Natalia Toranzo Neuquen
Vanina Kandyba Chaco
Lorena Sian Chaco

CER

En el mes abril de 2017, nació CONCIENCIA EN RED (CER). Una ONG creada por un grupo de personas conectadas con las Tecnologías de la Información y la Comunicación (TIC's) que entendieron que en estos tiempos que corren podrá haber buenos y malos, pero más existen buenas y malas formas de usar la tecnología.

CER, busca crear conciencia sobre el uso responsable de Internet y las Redes Sociales.

CONCIENCIA EN RED piensa en un mundo con gente tecnológicamente activa, no buscamos generar miedo a las TIC's, sino que educamos para el respeto a ellas y es ese el mensaje que queremos hacer llegar a niñ@s y adolescentes, a empresas, y a todo integrante de nuestra sociedad que de una forma u otra impacte con su accionar en la vida de otro, buscando como fin último una comunidad tecnológicamente conciente.

"CER y Hacer", este es nuestro lema, por eso acompañamos a todo aquel que desempeñe cualquier rol en la Red Internet, lo que por cierto día a día nos desafía a un continuo aprendizaje.

Nosotros charlamos y debatimos con todos los miembros de la sociedad sobre su vida online y offline. Como medio de llegar a la comunidad, implementamos charlas en instituciones públicas y privadas. Pretendemos estar presentes para brindar contención emocional y asesoría legal GRATUITA a víctimas de grooming, ciberbullying, extorsión, violencia y acoso virtual.

CONCIENCIA EN RED está conformada como una ONG bajo el formato de contrato asociativo conforme el capítulo 16° del Código Civil y Comercial de la Nación promulgado en el año 2015.-

Su conformación es federal, con un Coordinad@r y Secretarí@ Nacional, anualmente renovables y nodos provinciales organizados de manera similar.

Esta estructura busca descentralizar de la manera más extensa posible el trabajo y las actividades a desarrollar así cada nodo puede abordar de forma puntual la problemática local.-

CONCIENCIA EN RED se presenta a ustedes con miembros de Mendoza, Santa Fe, Chaco, Santiago del Estero, Neuquén, Chubut y Misiones dejando abierta la puerta para todas aquellas nuevas conciencias que quieran sumarse a esta Red.

Comunicado de prensa.-


AL
UNIVERSIDAD
AUTÓNOMA
LATINOAMERICANA
UNAULA

Información de microondas para personas sin tiempo

Selene Peraza Rosas[1]

(México)

En 1946, el estadounidense Percy LeBaron Spencer[2]**, inventó el horno de microondas. Un chocolate que traía en su bolsillo fue el primer alimento afectado accidentalmente por un tubo con el que trabajaba. Después de darse cuenta que las ondas del tubo habían derretido su chocolate, puso semillas de maíz e hizo palomitas. Luego puso un huevo de gallina y este se coció. Un año después, salieron a la venta las primeras versiones del *microwave oven*. En 1975, sus ventas rebasaron a las de las estufas de gas, gran parte de los hogares de los Estados Unidos y Japón cocinaban ya con microondas. Y así surgió uno de los inventos más populares del mundo, que le facilita la vida a millones de personas que no tienen tiempo para preparar manualmente lo que se comen; (para los privilegiados) calmar el hambre hoy toma tan sólo unos segundos.**

Esto mismo ocurre con la información en Internet. Al igual que con el horno de microondas, podemos consumir lo que tengamos a la mano, sin cuestionarnos sobre su origen, "ingredientes" y procesamiento, mucho menos sobre las posibles consecuencias que nos acarrea su consumo. Ejemplificar esta analogía simplona sería infinito.

Las noticias

En los primeros días de este mes de marzo, circulaba en Internet un video donde un profesor mexicano explicaba a sus alumnos de preparatoria cómo trataba a su mujer cuando ésta no cumplía con sus deseos, relatando un grave ambiente de violencia y misoginia. Este hecho causó alarma en el país y más allá; en menos de 24 horas el video había alcanzado más de ochenta mil visitas en YouTube, al punto tal que se lanzó una campaña a través de Change.org, donde se solicitaban firmas para presionar a las autoridades para que tomaran cartas en el asunto "Es necesario que la Universidad de Guadalajara investigue el tema y emita las sanciones correspondientes, pues normalizar la violencia como lo hace este docente, es la forma de perpetuarla. ¿Cómo avanzar a la igualdad si en las aulas tenemos docentes reproduciendo estos mensajes misóginos?" decía el comunicado. Luego de eso, la Universidad de Guadalajara emitió un comunicado donde señalaba que sometería al docente a un proceso administrativo y que lo citaría ante la Comisión de Responsabilidades y Sanciones, y a los demás procedimientos correspondientes. Así mismo, la institución puso de manifiesto la sorpresa de su Rector General, aludiendo que las lamentables

[1] Consutora independiente. Maestra en Derecho con orientación en Derecho Penal y Sistema Acusatorio por la Universidad Autónoma de Nuevo León – UANL, México. Becaria de la South School on Internet Governance –SSIG 2017, Río de Janeiro, Brasil.

[2] FAMOUS INVENTORS. Publicado en: http://www.famousinventors.org/percy-spencer

expresiones "No corresponden al lenguaje de un académico".[1]

Lo cierto es que nadie se tomó el tiempo de indagar quién era ese profesor, ni las circunstancias de ese video; no lo hizo Change.org, no lo hizo la Universidad antes de emitir su comunicado, no lo hizo la prensa, ni mucho menos lo hicieron los cibernautas ardidos. La realidad es que se trata de un video incompleto, en el que, previo a los minutos que se *viralizaron*, el famoso #LordPrepa10, como lo llamaron, hablaba de las circunstancias de maltrato que viven muchas mujeres, intentando hacer reflexionar a sus alumnos sobre la importancia del respeto hacia la mujer, por lo que esos famosos minutos no constituían más que una ejemplificación de un caso de maltrato.

Y así podemos encontrar muchos ejemplos de noticias que son compartidas con la ligereza que nos caracteriza hoy en día, muchas de ellas con inocencia, otras con plena maldad, lo cierto es que, todo lo que consumimos, es un reflejo de lo que somos. El caso del profesor de la Universidad de Guadalajara fue aclarado, pero, ¿cuántos no lo son?

Por mencionar sólo un dato, BuzzFeed News realizó una investigación en 2016, en la que se pudieron detectar por lo menos 750 noticias falsas que circulaban por Internet sólo ese año[2], noticias que, sin mayores razonamientos fueron leídas y compartidas por miles de usuarios alrededor del mundo, manifestando tristeza, alegría o indignación, según sus contenidos. Y es que, por más falsos que para muchos parezcan los enlaces, incluso sin necesidad de abrirlos, lo cierto es que la mayoría de las personas no se percatan de ello. *"Navegan por la red de forma natural para mantenerse informados. Ni conocen ni les importan demasiado las trampas"*[3] señala Trend Micro, al hablar sobre toda una ingeniería social con la que trabajan quienes quieren engañar a la gente, tema que merece toda una reflexión aparte.

[1] EXCELSIOR. Publicado el 05 de marzo de 2017, en: http://www.excelsior.com.mx/nacional/2017/03/08/1150815

[2] BUZZFEED NEWS. "Nos EUA, noticias falsas ultrapassam jornalismo em engajamento no Facebook". Publicado el 17 de noviembre de 2016, en: https://www.buzzfeed.com/craigsilverman/noticias-falsas-facebook?utm_term=.eb51YeLYJ#.agPpAvbAJ

[3] TREND MICRO. *Guía electrónica para la vida digital de TrendLabs*. "5 motivos por los que las trampas de la ingeniería social funcionan". Publicado en: http://www.trendmicro.es/media/br/5-reasons-why-social-engineering-tricks-work-es.pdf

El entretenimiento

En 2003, el niño Ryan Patrick Halligan de apenas 13 años se quitó la vida. Sus compañeros de clases se burlaban de él por creer que era homosexual, y decidieron divertirse haciéndole una broma que no pudo soportar. Una niña comenzó a comunicarse con él por Internet y fingió que le gustaba. Cuando por fin Patrick decidió dar el paso en el mundo real, ella lo humilló rechazándolo delante de todos sus compañeros y publicando los mensajes que él le había enviado. "*Una cosa es sufrir bullying y ser humillado delante de unos pocos chicos […] Pero tiene que ser una experiencia totalmente distinta a la de una generación anterior, cuando este dolor y esta humillación son ahora contemplados por una audiencia muchísimo mayor de adolescentes online. Creo que mi hijo habría sobrevivido a estos incidentes de no haber tenido lugar en Internet" dijo su padre.*[1]

Pero este caso es sólo la punta del iceberg, si nos ponemos a pensar que todos los días pasamos "de mano en mano" videos, fotografías, chistes y memes (los reyes de las redes sociales) donde nos burlamos de personas obesas, con discapacidades, maltratadas, o en desgracia, normalizando esta conducta, sin pensar que en medio de nuestra diversión puede haber un ser humano que como Patrick no soporte aquello que con tanta ligereza compartimos.

La nota roja

¿Cuántos de nosotros hemos recibido, por lo hemos una vez, mensajes de alertas sobre presuntos delincuentes? ¿Cuántos nos hemos encontrado con imágenes de hombres golpeadores, mujeres ladronas o pederastas expuestos valientemente por las víctimas o sus conocidos, en las redes sociales? Nuestra necesidad de informar, ser informados y sobre todo, de protegernos, se expone ante los cientos, miles y millones de veces que las personas comparten esa información, muchas veces infundada, "por si las dudas". Incluso muchas instituciones encargadas de la procuración de justicia lo hacen: *"Capturan a asqueroso violador"*[2] se lee en las páginas de la prensa, que publica datos obtenidos de las fiscalías, exponiendo foto, nombre y hasta domicilio de los acusados, en apenas sus primeras horas de detención.

En abril de 2015, Andrea Femía, una mamá argentina de 39 años, recibió por WhatsApp un mensaje que alertaba sobre la presencia de un presunto violador que se ubicaba frente a la escuela donde estudiaba su hijo, por lo que, con la intención de hacer lo correcto, compartió el mensaje a otras mamás, acompañándolo de una fotografía. Días después, la señora fue citada a un Juzgado para que respondiera sobre los daños causados al hombre de la fotografía compartida. Se trababa de Orlando Heredia[3], un albañil en retiro, de 45 años, quien fue alertado por sus hijos que le pedían una explicación, al enterarse que su reputación circulaba por Facebook. Aquella vez, el señor se encontraba frente al Colegio Santa Rosa de Lima, esperando a su hermano, cuando le tomaron la fotografía publicada por esa mujer que nunca había visto en su vida y que tendría que pagar por los daños causados, según

[1] "Ryan's History". Publicado en 2010, en: http://www.ryanpatrickhalligan.org/

[2] DIARIO CRÍTICA. Publicado el 26 de febrero de 2015, en: http://diario-critica.mx/nota.php?id=39299

[3] DIARIO PRIMERA LÍNEA. Publicado el 28 de abril de 2015, en: http://www.diarioprimeralinea.com.ar/nacionales/2015/4/28/acuso-falsamente-secuestrador-albanil-facebook-podria-presa-13383.html

determinaran las leyes, pero ¿cuánto cuesta verdaderamente el daño social? ¿se repara?

Nuevamente, este se trata de un caso que logró aclararse pero, ¿cuántos no lo son?

Derecho e Internet

Uno de los retos más grandes del Derecho, es la implementación de la regulación "offline" al campo "online". Algunos expertos consideran que *"la gran cantidad de comunicación facilitada por Internet (por ejemplo, intensidad de la comunicación, número de mensajes) hace una diferencia cualitativa"*[1] en virtud de que más personas están expuestas, a través de diferentes plataformas, lo que dificulta la aplicación de los marcos legales como tradicionalmente se ha venido haciendo.

Si bien es cierto, las personas tenemos derecho a expresar y compartir nuestras ideas, sin prohibición alguna (Art. 19 de la DUDH[2]) también lo es que tenemos la obligación de respetar a la comunidad, pues sólo en ella podemos desarrollarnos plenamente (Art. 29). En este sentido, la libertad de expresión debe encontrar un contrapeso entre estas dos cuestiones.

Pero, más allá de estas discusiones legales que deben aterrizarse alrededor del mundo, antes de cargarle toda la responsabilidad a las "máquinas de pensar" que dedican sus carreras a buscar soluciones, todos podemos, desde los temas cotidianos como los que hemos mencionado arriba, hacer mucho. Cuando tengamos un *Smartphone* en nuestras manos, cuando estemos sentados frente a una computadora, o simplemente al tener una plática de sobremesa en un domingo familiar, vale la pena preguntarnos si estamos seguros de lo que estamos compartiendo: ¿Es verdad? ¿Aporta algo positivo? ¿Es útil? ¿No daña a nadie? ¿O es información de microondas para personas sin tiempo?

Autora: **Selene Peraza Rosas**
Consultora independiente, radicada en Lima, Perú. Se ha perfilado en temas de Reforma Procesal Penal desde 2008 en México. Es Maestra en Derecho con Orientación en Derecho Penal y Sistema Acusatorio, por la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León –UANL. Ha sido capacitada por diversas instituciones de México, Estados Unidos y Chile, tales como la Universidad Alberto Hurtado -UAH, el National Institute for Trial Advocacy -NITA, el Instituto Tecnológico y de Estudios Superiores de Monterrey –ITESM, entre otras. Trabajó como abogada en el Departamento de Investigación y Desarrollo Institucional de Renace A.B.P., fue asesora en la Comisión de Coordinación Interinstitucional para la Implementación del Sistema de Justicia Penal en Nayarit, y auxiliar para la implementación del Nuevo Sistema de Justicia Penal en el Poder Judicial del Estado de Nayarit. Trabajó en Jurimetría Iniciativas para el Estado de Derecho A.C., como coordinadora de información y análisis. Es consultora externa de la Agencia de los Estados Unidos para el Desarrollo Internacional –USAID, en donde ha trabajado para la campaña "Corre la voz… Hablemos de Justicia" del programa PROJUSTICIA y la organización México S.O.S.
Colabora para el Programa Nuevos Abogados para el Sistema de Justicia en México, de la Barra Americana de Abogados –ABA Roli México, siendo Juez de la Competencia Nacional de Litigación Oral. Ha sido docente en el Colegio Mexicano de Estudios de Posgrado y Económicos –Colegio Jurista, y en la Facultad de Derecho de la Universidad Nacional Autónoma de México –UNAM. Es becaria de la South School on Internet Governance –SSIG, por la Fundación Gertulio Vargas y el Centro de Capacitación en Alta Tecnología para América Latina y El Caribe, para la edición 2017 en Río de Janeiro, Brasil.

[1] JOVAN KURBALIJA, *An Introduction to Internet Governance*, 7th edition, DiploFoundation, Geneva, 2016. P. 207.

[2] Declaración Universal de Derechos Humanos

InFo-Lab: Laboratorio de Investigación y Desarrollo de tecnología nacional en Informática Forense

La Fiscalía General de Mar del Plata y la Universidad FASTA han trabajado en forma conjunta varios proyectos de investigación y desarrollo durante más de 10 años, es por eso que, para formalizar y afianzar el vínculo y a pedido de la Fiscalía General, el 29 de Mayo de 2014 mediante la Res 5/14 de la Procuración General se crea el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab), integrado por el Ministerio Público de la Provincia de Buenos Aires, representado por la Señora Procuradora General Dra. María del Carmen Falbo, el Municipio de General Pueyrredon, representado por el Señor Intendente Contador Gustavo Pulti y la Universidad FASTA, representada por el Rector, Dr. Juan Carlos Mena.

El laboratorio está integrado por investigadores científicos tecnológicos de las tres instituciones, que conforman un equipo multidisciplinario destinado a aportar soluciones a las problemáticas del Ministerio Público de la Provincia de Buenos Aires, potenciando las capacidades institucionales en un área de fundamental importancia para la ciudad y la provincia: la justicia penal.

Si bien los resultados de las investigaciones y desarrollos tecnológicos del laboratorio se aplicarán en el ámbito de la Provincia de Buenos Aires, se prevé la extensión de estos aportes a la totalidad de los Ministerios Públicos de la República Argentina a través del Consejo de Procuradores y del Consejo Federal de Política Criminal, dando un alcance nacional al trabajo de este equipo técnico provincial. Esto fortalecerá el desarrollo colaborativo de conocimientos, competencias y capacidades institucionales hoy imprescindibles en el ámbito de la investigación y la litigación penal, y permitirá la sustitución de productos extranjeros de apoyo a la investigación criminal por soluciones de origen nacional, con los consiguientes beneficios en términos de adaptabilidad, mantenimiento, costos, y autonomía tecnológica.

Proyectos de Investigación y Desarrollo Tecnológico

Los proyectos del InFo-Lab han sido acreditados por el Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación e incorporados al Banco Nacional de Proyectos de Desarrollo Tecnológico y Social.

A. Línea de trabajo INVESTIGA - Ambiente Integrado de Visualización y Análisis de Datos:

El proyecto INVESTIGA consiste en el desarrollo de un sistema informático que permita la consolidación de datos provenientes de múltiples fuentes en un ambiente único que facilite la visualización gráfica de conexiones y su análisis.

Este software ya se encuentra en uso a modo de prueba temprana, en los siguientes departamentos judiciales: Mar del Plata, La Plata, Zarate Campana, Morón, La Matanza, Mercedes, Quilmes, Bahía Blanca, Junín, Procuración General, San Martín y Trenque Lauquen.

Las pruebas tempranas tienen el objeto de detectar necesidades, demandas investigativas y potenciar el uso de la solución.

Asimismo, se han contactado con el InFo-Lab las siguientes provincias interesadas en INVESTIGA: Chaco, Jujuy, Santiago del Estero, La Pampa, Chubut, Entre Ríos y Ciudad Autónoma de Buenos Aires, a las cuales se les dio acceso a la versión de prueba instalada en el servidor de la Universidad.

Investiga se complementa con los siguientes proyectos:

- *"Visor Web INVESTIGA",* desarrollado en el ámbito de la Universidad FASTA como proyecto final de graduación de la carrera Ingeniería Informática. Permite incorporar al gráfico generado por INVESTIGA, elementos para colaborar en la litigación en juicio, tales como videos, imágenes, audios o textos.

- *"Big Data INVESTIGA",* desarrollado en conjunto con la UTN Regional Delta. Su objetivo es unificar y filtrar información útil en los casos en que se trabaja con gran cantidad de datos y relaciones, para graficar sólo laquellos que son relevantes.
- *"OSINT INVESTIGA",* desarrollado en el ámbito de la Universidad FASTA como proyecto final de graduación de la carrera Ingeniería Informática. Su objetivo es la búsqueda, recuperación, procesamiento y almacenamiento de información existente en fuentes de recursos abiertos accesibles desde la web, para integrarla con los otros tipos de datos y así anriquecer el análisis y graficación (ej.: armado de erfiles de personas sospechosas) .
- *"Workflows INVESTIGA",* en desarrollo. Tiene por objeto permitir la definición, ejecución y control de planes de investigación penal y flujos de trabajo, que se incorporan a INVESTIGA como centralizador de los datos investigativos.

B. Línea de trabajo Guías Normativas.

1. **Protocolo de Actuación en Informática Forense (PAIF-PURI®),**. Su objetivo fue la elaboración de una **Guía Integral del Empleo de la Informática Forense en el Proceso Penal** para ser adoptada y promovida por el Ministerio Público bonaerense como estándar oficial de trabajo, tanto para peritos informáticos como para investigadores judiciales. La Sra. Procuradora General mediante Resolución General Nro. 1.041/15 de fecha 30 de noviembre de 2015 solicitó su aplicación en los Departamentos Judiciales de Mar del Plata y Mercedes, con una evaluación por parte de los Ingenieros a cargo de las Oficinas Periciales correspondientes.
Bajo Resolución 483/16 de fecha 27 de junio de 2016 se resolvió la aplicación y observación de la segunda edición de la guía en el ámbito de todo el Ministerio Público de la Provincia de Buenos Aires.

2. **Guía Técnica para la Implementación de un Laboratorio de Informática Forense GT-LIF.**

Propone establecer los aspectos a considerar para el diseño, implementación y gestión de un laboratorio de informática forense, desde los aspectos estratégicos, institucionales, estructurales, de infraestructura, tecnológicos y de recursos humanos. Al brindar pautas para su creación, permitirá medir y evaluar la calidad de los procesos periciales dentro del laboratorio, sentando las bases para la definición de programas de calidad. Al contar ya el MPBA con la Guía Integral de Empleo de la Informática Forense en el proceso penal, el siguiente paso es la creación de laboratorios forenses que brinden las garantías necesarias para su aplicación, permitiendo gestar eficientemente la obtención de evidencias digitales válidas, relevantes, suficientes y confiables. Este proyecto está en desarrollo y se espera poder contar con esta guía en el año 2017.

C. Línea de trabajo Aplicaciones Forenses.

1. **Forensia en Equipos Móviles (FOMO)**, tiene como objetivo el desarrollo de un sistema informático que permita mejorar la capacidad de análisis de la información contenida en los dispositivos móviles, mediante el acceso a los datos extraídos por los Sistemas UFED.

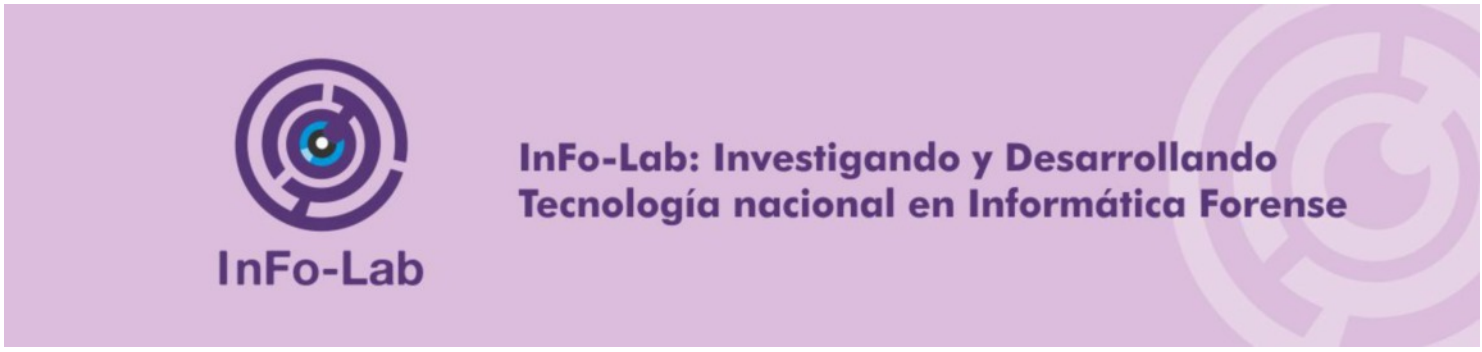
Cómo primer producto se trabajó sobre los sistemas operativos Android.

Este proyecto también ha derivado en la realización de un convenio de cooperación con la Universidad Nacional del Noroeste de Buenos Aires (UNNOBA), con sede en Junín (Convenio 18/15 PG) para la realización del módulo de extracción y análisis de datos forenses de equipos Windows Phone.

Los datos analizados podrán a su vez ser exportados a INVESTIGA, potenciando el análisis y graficación de este sistema.

2. Otros proyectos desarrollados en esta línea por el Grupo de Investigación de la Facultad de Ingeniería de la Universidad FASTA que están a disposición del Ministerio Público son: CIRA (Framework de File Carving) para la extracción forense de archivos eliminados, BIP-M (Análisis Forense de Procesos en Memoria), para el análisis forense de volcados de memoria volátil.

En cuanto a la extensión, servicios y transferencia, el InFo-Lab realiza tareas de investigación y desarrollo de tecnología en



Informática Forense brindando también asesoramiento general en esta disciplina así como también en la creación, implantación y evaluación de laboratorios técnicos forenses. También desarrolla soluciones de ingeniería ad-hoc. Además dicta el **Programa de Actualización Profesional en Informática Forense** destinado a profesionales de la informática interesados en la actuación pericial y que deseen capacitarse en los conceptos básicos de la Informática Forense, el Proceso Unificado de Recuperación de la Información (PURI®), la legislación aplicable y las técnicas y herramientas de software libre disponibles y recomendadas para la actuación pericial. De igual manera, se brindan capacitaciones y talleres adecuados a las necesidades de cada institución, y charlas abiertas al público en general sobre temáticas relacionadas.

Los profesionales del InFo-Lab participan periódicamente en distintos congresos y jornadas que se desarrollan tanto en el país como en el exterior, en los cuales se tratan temas de Informática Forense, Derecho Informático e Investigación Criminal. Ello no sólo promueve la actualización permanente y la difusión de la labor del InFo-Lab, sino que es también fuente de nuevas ideas. Contribuye además, a gestar redes de cooperación y alianzas estratégicas en el área las ciencias forenses.

El InFo-Lab y la relación Universidad-Estado

Todos los desarrollos del InFo-Lab están a disposición del Consejo Federal de Procuradores y del
Consejo Federal de Política Criminal.

Este laboratorio y sus proyectos son un aporte concreto de la Universidad al Estado, en pro de la mejora de la sociedad toda. La conjunción multidisciplinaria de actores académicos con los del poder judicial y ejecutivo, tanto en el plano provincial como municipal, demuestra que la colaboración Universidad-Estado, que tanto se promueve, es posible.

El InFo-Lab, inédito en su diseño y conformación mixta, es un ejemplo más, de los tantos que hay en el país, que honran la verdadera misión de la ingeniería: crear, con ingenio y compromiso, para mejorar la calidad de vida de la gente.

Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense *InFo-Lab*
Ministerio Público Fiscal Provincia de Buenos Aires. Universidad FASTA. Municipalidad de General Pueyrredon.
Universidad FASTA. Avellaneda 3341. Mar del Plata. Argentina.
info-lab@ufasta.edu.ar
(+54-223) 499-5200 3

LA RED EDI

INFORMACIÓN QUE SUENA BIEN

WWW.ELDERECHOINFORMATICO.COM

pengowin.com.ar/

PENGOWIN 4

Repositorio de herramientas para el uso en la seguridad informática

GOBIERNO

&

CUMPLIMIENTO

RESPONSABLE

ING FABIÁN DESCALZO

La importancia del factor humano

Autor: Fabián Descalzo

¿Todo se resuelve con la tecnología? ¿Por qué los directivos deben hablar más con sus empleados sobre seguridad? Según una investigación global de fraude, encargada por la consultora internacional Kroll y realizada por The Economist Intelligence Unit, se encuestaron a 768 altos ejecutivos de todo el mundo representando una amplia gama de industrias y funciones, cuya observación general es que el fraude sigue en aumento, donde tres cuartas partes (75 %) de las compañías informan que han sido víctimas de un incidente de fraude en el último año.

El resultado de la investigación revela que para el 81 % de las compañías encuestadas la mayor amenaza de fraude proviene de sus áreas internas, perpetrado por algún miembro de la propia organización. Este hecho representa un importante incremento frente al 72 % registrado en la encuesta anterior.

Las empresas encuestadas representan a una amplia gama de industrias, incluyendo Servicios Financieros y Servicios Profesionales, Comercio, Tecnología de la Información, Telecomunicaciones, Salud, Farmacéuticos y Biotecnología, Transporte, Ocio y Turismo, Bienes de Consumo, Construcción, Ingeniería e Infraestructura, Recursos Naturales y Manufactura, lo que indica que esta problemática no es privativa de una industria o pocas empresas.

Cuando hablamos de fraude la primera relación que hacemos está asociada a la estafa o robo económico, pero también debemos incluir aspectos relacionados con el robo a través de la pérdida de confidencialidad y privacidad de la información, y la coincidencia entre ambos aspectos es la necesidad de proporcionar directrices para la selección y especificación de controles de seguridad relacionados con el factor humano que sirvan para ser aplicados a cualquier proceso y sistema de información que deseemos sean más seguros y con una gestión de riesgos efectiva a través de facilitar un enfoque más coherente, comparable y repetible para la selección y especificación de los controles de seguridad de los sistemas y organizaciones de información y proporcionar un catálogo estable, pero flexible, de controles de seguridad para satisfacer las necesidades de protección de información actuales y las demandas de las necesidades de protección futuros basados en el cambio de las amenazas, los requisitos y las tecnologías.

Tengamos en cuenta que la pérdida de confidencialidad y privacidad de la información además de tener como consecuencia aspectos económicos adversos para la organización, también le crea expuestos legales y de imagen ante la comunidad, por lo que la creación de una base para el desarrollo de métodos y procedimientos para determinar la efectividad de los controles requiere que se discutan conceptos de gestión de riesgos asociados a los recursos humanos de toda la organización. Según lo mencionado por el Ministerio de Trabajo y Asuntos Sociales de España en el documento “NTP 537: Gestión integral de riesgos y factor humano”, la gestión de estos riesgos sobre la operación y funciones corporativas debe facilitar un efectivo control de todo tipo de pérdidas y a través de la cual, las personas, asumiendo que son debidamente respetadas por la estructura de la que forman parte, contribuirán notoriamente al logro de los objetivos empresariales.

Tal como lo sabemos, cada uno de los estándares aplicables a los sistemas de gestión contemplan el factor humano, tanto en aspectos relacionados con su capacitación y aptitudes técnicas como en su propia gestión del entorno de trabajo y sus responsabilidades en el cumplimiento legal y regulatorio. Las pautas determinantes para conseguirlo son la formación continua y la motivación del personal, que son elementos esenciales para conseguir un buen nivel de competencia profesional, crear pertenencia con la

organización y en consecuencia comprometerse con los objetivos de la misma.

Es precisamente a partir de esta concepción que una gestión adecuada de los riesgos ayudará a modelar una metodología para detectar cuáles son los aspectos esenciales en los que la mejora es más necesaria u oportuna sobre aquellos aspectos que pueden tener serias implicaciones en el éxito de una estrategia empresarial basada en las personas. La NTP mencionada puede ser tomada como guía para analizar la problemática que planteamos en este artículo, ya que establece que deben ser evaluados seis aspectos relevantes, que desde mi punto de vista pueden despertar potenciales riesgos a la organización, al igual que cualquier otro aspecto tecnológico o funcional:

•LIDERAZGO Y ESTRATEGIA, evaluado como factor clave para el potenciamiento y apoyo al desarrollo de competencias; revisión del método en la delegación de tareas, responsabilidades y autoridad; revisión de la definición de intereses estratégicos para la organización en prevención de riesgos.

•COOPERACIÓN, evaluando el desempeño del trabajo en equipo y la integración de los objetivos de grupo en los objetivos generales; así como la participación activa a todos los niveles y la facilidad en las relaciones funcionales e interdepartamentales.

•COMUNICACIÓN, revisando cada uno de sus canales (vertical bidireccional y horizontal), sus formas y la oportunidad de aplicación de nuevas tecnologías; evaluar los medios de transmisión de la información, sus tiempos y actualización.

•ORGANIZACIÓN Y CULTURA, evaluando su flexibilidad y adaptabilidad al cambio; revisando la

estrategia de la gestión por procesos frente a la gestión por funciones, para evitar que se solapen competencias decisionales ni funcionales; análisis del sistema de desarrollo y promoción de las personas en la organización; mejora continua y la toma de decisiones por la persona más próxima (autonomía decisional)

•FORMACIÓN, evaluando las actividades facilitan el compartir conocimientos; los programas de aprendizaje continuo y estratégica de aprendizaje

•TECNOLOGÍA, revisando la gestión de aplicación de nuevas tecnologías de la información y su aprovechamiento para la generación y gestión del conocimiento de los recursos humanos, y el cumplimiento legal y regulatorio desde sus funciones laborales.

Las definiciones antes expuestas, y la problemática entorno a los riesgos del factor humano, nos indican que el 2016 profundiza el desplazamiento en el enfoque adoptado por las diferentes regulaciones y estándares, cambiando su estrategia de revisión haciendo centro en la evaluación de la cultura de cumplimiento de las empresas y no simplemente en la evaluación técnica o funcional disociada de la gestión de sus recursos humanos.

Las entidades regulatorias han puesto sus ojos en la cultura corporativa y su relación con las prácticas de cumplimiento ampliando su enfoque en áreas tales como los controles internos y la gestión de riesgos evaluando entre otras cosas, qué tan bien las empresas han implementado procedimientos adecuados para minimiza los riesgos relacionados con toda gestión llevada a cabo por su personal.

Para todos los casos y ante cualquier situación, el riesgo del factor humano está siempre presente, por ello es necesario establecer una metodología cuantitativa en función de datos que representen el nivel de cumplimiento interno, representados en un proceso de medición que refleje en forma periódica el alineamiento a las políticas internas de la

organización y sus desvíos. También puede hacerse mediante encuestas internas a usuarios finales, con preguntas referentes a puntos vitales de las normas, para evaluar el nivel de conocimiento como instancia previa a evaluar el cumplimiento en los procesos. Con respecto a los indicadores, los mismos deben ser dinámicos en función de nuevas regulaciones o cambios en los procesos (lo que los hacen variables en el tiempo); además que también puedo establecer distintos niveles de indicadores en función del nivel de madurez de la organización, lo que también hace que puedan variar en el tiempo teniendo en cuenta el crecimiento futuro en el nivel de cumplimiento de la misma.

Como conclusión, no importa para que proceso usted esté implementando una gestión de riesgos. Lo importante es tener en cuenta en ella a las personas y sus funciones dentro del proceso, con el fin de determinar en forma temprana los controles y la metodología en que los va a llevar adelante y medirlos.

Fabián Descalzo

fabiandescalzo@yahoo.com.ar

Gerente de Servicios y Soluciones en el área de Gobierno, Riesgo y Cumplimiento (GRC) en Cybsec Security Systems S.A., con amplia 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.

GUÍA PARA HACER NETWORKING EN LINKEDIN Y TWITTER (PARTE I)

Autora: Carolina Marin

El networking es una pieza clave para conseguir el éxito en tu carrera profesional Crear y mantener los contactos en todos los trabajos por los que has pasado, así como intensificar los vínculos con otros profesionales, es imprescindible para mejorar profesionalmente. En este artículo te doy las claves para que puedas hacer networking utilizando las redes sociales ¿las protagonistas? Linkedin y twitter

¿Qué es el networking?

El networking consiste en establecer una red profesional de contactos que nos permita darnos a conocer, escuchar y aprender de los demás, encontrar posibles colaboradores, socios o inversores.

¿Para qué te sirve?

- Darte a conocer a ti o a tu estudio
- Reforzar relaciones con tus clientes
- Realizar nuevos clientes o socios.
- Conocer acerca del entorno laboral que te rodea

Linkedin, la red de contactos

La mayoría de los abogados tiene un perfil en esta red social, aunque solo se limitan a compartir contenido de terceros y pocas veces actualizan. Y sí, pareciera que Linkedin solo sirve para presumir nuestros estudios y habilidades. Déjame decirte que estás desaprovechando un espacio para hacer marca. ¿Qué necesitas para hacer networking en Linkeding? Para crear tu red de contactos, primero debes asegurarte de cumplir con las siguientes recomendaciones:

1) Completar todos los campos disponibles.
2) Crear una URL pública, trata de usar tu nombre tal cual, por ejemplo: https://www.linkedin.com/in/carolinamarinok/
3) No te olvides de tener una foto de perfil lo más profesional posible
4) Agregar habilidades
5) Procura escribir un texto corto en el extracto, no todo tu CV. Los dos primeros renglones son los más importantes, es lo que se ve a simple vista. Te recomiendo no más de 5 renglones.
6) Tomate 15 minutos todos los días, para contactar a otros. Piensa en tu target, colegas, crea tu comunidad de a poco.
7) Si no tienes blog o web, puedes usar la sección de notas de Linkedin, de hecho, si tienes blog también puedas usarla. Escribes

una parte del texto allí y dejas un enlace para que los contactos sigan leyendo el artículo en tu blog.

8) Comparte contenido de terceros

9) Una vez tengas todo en armonía, puedes agregar el enlace de linkedin a tu biografia de Twitter

10) ¿Sabías que también puedes agregar enlace de linkedin a tu perfil de facebook, ya sea personal o fan page?

Twitter, la red preferida de los speakers

Si eres un abogado que recorre instituciones, ciudades o países dando charlas, la red de microblogging se puede convertir en tu mejor estrategia. Puedo asegurarte que estar en Twitter va a llevarte a la gloria. ¿Qué puedes conseguir?

- **Networking**: al igual que linkedin, twitter es ideal para crear tu red de contactos.
- **Posicionarte:** Si bien lo puedes hacer desde todas las redes, Twitter te permite posicionar tu marca personal fuera de tus límites geográficos de manera más fácil.
- **Eventos:** La red de microblogging es ideal para cubrir cualquier tipo de evento, ya sea charlas, cursos, congresos.
- **Tendencia:** con una buena estrategia puedes lograr que todo un país hable de tu marca, ya sea un congreso, un libro o lo que fuere.
- **Tráfico:** llevar tráfico a la web de tu estudio o a tu blog personal.

Cómo lograr seguidores en Twitter

Si no tienes un perfil acorde y profesional es muy poco probable que consigas seguidores. El primer paso en tu estrategia es **causar una buena primera impresión**, de esta manera lograrás despertar interés en los demás. Los usuarios de Twitter necesitan saber:

- Quién eres
- De qué temas hablas
- En qué eres bueno

Es por ello que se vuelve fundamental completar tu perfil. Algunas recomendaciones:

- **Foto de perfil**: acá no sirve una foto de cuerpo entero o la foto de tu estudio. La foto de perfil es como la de tu DNI, solo tú y nadie más que tu debe estar en ella, en lo posible primer plano.
- **Foto de portada**: por favor, no pongas una foto tuya en primer plano, es muy narcisista. Vale poner una foto dando charla o si quieres de tu estudio. Puedes aprovechar el espacio para poner tu web y otras redes, pero sé minimalista, nada de textos largos o promociones.
- **Biografía**: sumamente importante completar tu bio. Una buena manera de saber qué poner es haciéndote la siguiente pregunta: **¿qué hago y con qué se encontraron los usuarios que me sigan?**
- **Actualización:** A nadie le gusta seguir a usuarios que escriben una vez a las quinientas, es un factor por el que pueden dejar de seguirte
- **Hashtag**: aunque se pueden usar en todas las redes, fue Twitter el que incursionó con las etiquetas ¿para qué sirven? Para posicionarte. Para que tu mensaje sea visto por usuarios, incluso los que no te siguen. No debes abusar de ellas. Lo recomendable es usar no más de tres por tuit. ¿Cómo elegir? Puedes usar una con el nombre de tu blog o estudio, (#EDI) otros por temática, por ejemplo: #Ciberbullying y otra por localización: #Argentina

Ahora que ya sabes cómo dar una buena primera impresión, lo siguiente es empezar a generar contenido atractivo en tus redes sociales, pero eso lo veremos en la próxima edición.

El caso de Andrea Noel: un abuso sexual y sus enseñanzas para el derecho informático.

Autor: Erick Lopez (México)

Al menos en México, el derecho informático sigue siendo visto por la mayoría de operadores jurídicos como una excentricidad. A pesar de que a partir de datos oficiales se calcula que alrededor del 60% de la población es usuaria de internet, las respuestas que el derecho ofrece frente a los retos que el mundo digital entraña son hasta ahora más bien pobres.

El abuso padecido por la periodista norteamericana Andrea Noel resulta ilustrativo de la pésima manera en que se actúa, desde un punto de vista jurídico-institucional, ante unos hechos que si bien en un primer momento no tienen una naturaleza digital, se vinculan estrechamente con temas propios del derecho informático por su desarrollo. Gracias a que la víctima ha contado recientemente su experiencia, las siguientes reflexiones toman como punto de partida su extenso relato[1].

Los hechos ocurridos.

Justo en el día internacional de la mujer de 2016 (08 de marzo), Andrea Noel fue agredida sexualmente en una de las colonias más gentrificadas de la ciudad de México. Mientras caminaba por la calle, un tipo se le acercó por atrás, le levantó la falda, le bajó su ropa interior y se echó a correr: apenas uno más de entre miles de casos de violencia contra las mujeres que se suscitan todos los días en un país eminentemente machista como México. Lo que empezó a dimensionar lo ocurrido de un modo distinto fue que Andrea luchó por obtener un video de lo ocurrido y lo subió a Twitter.

Según lo narra Andrea, tras ser atacada consiguió que el administrador de un edificio le diera acceso a un video tomado desde la cámara de vigilancia del lugar. Ella grabó con su teléfono lo que transmitía la pantalla pues no pudieron copiar el archivo a otro medio de almacenamiento. El breve video se hizo viral, generando tres tipos de respuestas: personas que mostraban apoyo y solidaridad, autoridades que se acercaron para ofrecer ayuda a fin de identificar al agresor, y una jauría de troles que a partir de entonces (y a lo largo de los siguientes meses) la amenazó con violarla y matarla. Poco más de un año después, el agresor sigue sin ser identificado.

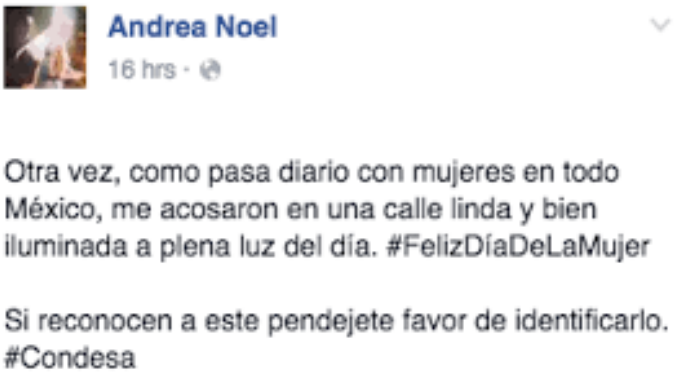
¿Cuál es la relevancia de estos hechos para el derecho informático? Me parece que los siguientes puntos ilustran bien una parte de los principales problemas que enfrenta este tipo de derecho.

a) La cada vez más inútil división entre el mundo *online* y el *offline*.

Cierto, existen fenómenos como los ataques distribuidos de denegación de servicio (DDoS por sus siglas en inglés) que no podrían existir fuera del entorno digital. No menos cierto resulta

[1] Andrea Noel, A viral sex crime saga of perverts, pranksters, and prosecutors, The daily beast, disponible en la dirección http://www.thedailybeast.com/articles/2017/03/18/a-viral-sex-crime-saga-of-perverts-pranksters-and-prosecutors.html

también que muchas de las afectaciones que sufre la gente, potenciadas por el uso de tecnologías de la información y la comunicación (TIC), son fraudes, acosos, injurias o amenazas que han existido desde antes de la irrupción de internet. En el caso de Andrea, el cobarde ataque callejero de un puñado de segundos de duración se transformó, a partir de la viralización del video en redes sociales, en un ataque continuo de meses de duración en el que el machismo aun imperante no dio sosiego a una mujer violentada tanto en la calle como ahora en su vida en línea*; a la violencia de género le es indiferente expresarse con un puñetazo o con un post amenazante, pues en ambos casos consigue su objetivo. El derecho ha actuado en ambas esferas con la misma incompetencia, resultando igualmente ineficaz para identificar y sancionar al atacante como para reaccionar de algún modo y tratar de proteger a Andrea de una hostilidad perenne en la red. Así, la violencia online y la offline no solo la han empujado a abandonar el país, sino también le hacen más difícil soportar una presencia en la red que, debido a su profesión, resulta particularmente indispensable para ella.*



b) La vigilancia masiva, ¿para qué sirve? Siempre con el pretexto de protegernos del terrorismo y toda clase de delincuencia, los gobiernos han inundado ciudades como la de México con cámaras de video, han creado leyes de retención de datos, han dotado a sus fiscalías com amplísimas facultades o han adquirido poderoso software de espionaje para infiltrar toda clase de comunicaciones privadas. Sin embargo, ese intrusivo andamiaje técnico-jurídico sigue siendo incapaz de cumplir con su supuesto cometido. En la ciudad de México, por ejemplo, el 2016 ha sido el año en que más homicios ha habido en los últimos 20 años, con una tasa de 10.78 asesinatos por cada cien mil habitantes, mientras que el robo creció un 26% en enero de 2017 comparado con enero de 2016[1].

Claramente, las promesas de la vigilancia masiva en cuanto a permitirnos vivir una vida más segura no han cristalizado en la ciudad de México, lo cual es comprensible si se pondera que las causas estructurales de la violencia (desigualdad, corrupción, educación deficiente, precariedad laboral, etc.) no suelen ser combatidas de verdad. ¿Qué estamos ganando, entonces, con esta vigilancia? Como lo narra Andrea, ella pudo obtener una grabación a partir de un servicio privado. Sin embargo, el acceso a las grabaciones obtenidas en las cámaras gubernamentales le fue vedado por varias semanas, lo que le impidió cooperar de mejor manera con las autoridades a fin de identificar al atacante (lo que a su vez provocó que por poco se

[1] Observatorio Nacional Ciudadano, Reporte sobre delitos de alto impacto enero 2017, disponible en http://onc.org.mx/wp-content/uploads/2017/03/mensual-enero-digital_VF.pdf

acusara a una persona inocente). Este suceso confirma así algo que para estas alturas ya debe ser claro: la vigilancia masiva es una herramienta sujeta al capricho, el arbitrio y la discrecionalidad de los gobernantes en turno, quienes en México como en casi toda latinoamérica no se caracterizan por su compromiso con el bienestar ciudadano.

c) La ineficacia policial y su falta de herramientas.

Recientemente, el alcalde de la Ciudad de México (un doctor en derecho) culpó al nuevo sistema penal acusatorio por el incremento de la delincuencia en la capital del país. Este sistema, en que predomina la oralidad e intenta reducir la discrecionalidad del pasado, entró en vigor en todo el país en 2016. Ciertamente, la falta de preparación de fiscales y policías de investigación está ocasionando que sea más factible que las personas acusadas sean dejadas en libertad, pues si no se genera evidencia sólida, correctamente recabada y preservada, las defensas tienen un camino fácil para erosionar las acusaciones. Pero esto no es un problema de los órganos jurisdiccionales, sino de falta de voluntad de los poderes ejecutivos (de quienes aun dependen las fiscalías) para generar instituciones de investigación sólidas.

Andrea Noel narra cómo en su caso las autoridades se pusieron en contacto desde el primer día por medio de twitter, un privilegio que casi ninguna mujer goza cuando es atacada sexualmente. Sin embargo, esa respuesta inmediata fue el único momento en que la institución investigadora actuó con debida diligencia, pues luego de la celeridad inicial inició el kafkiano calvario burocrático que no llevó a nada, excepto a un voluminoso expediente de 500 hojas sin ningún resultado. En el colmo del sinsentido procesal, la policía cibernética recibió la orden de investigar el origen del video disponible en youtube que la propia Andrea había grabado e, increíblemente, llegaron a la

conclusión de que "NO es posible determinar el origen del video".

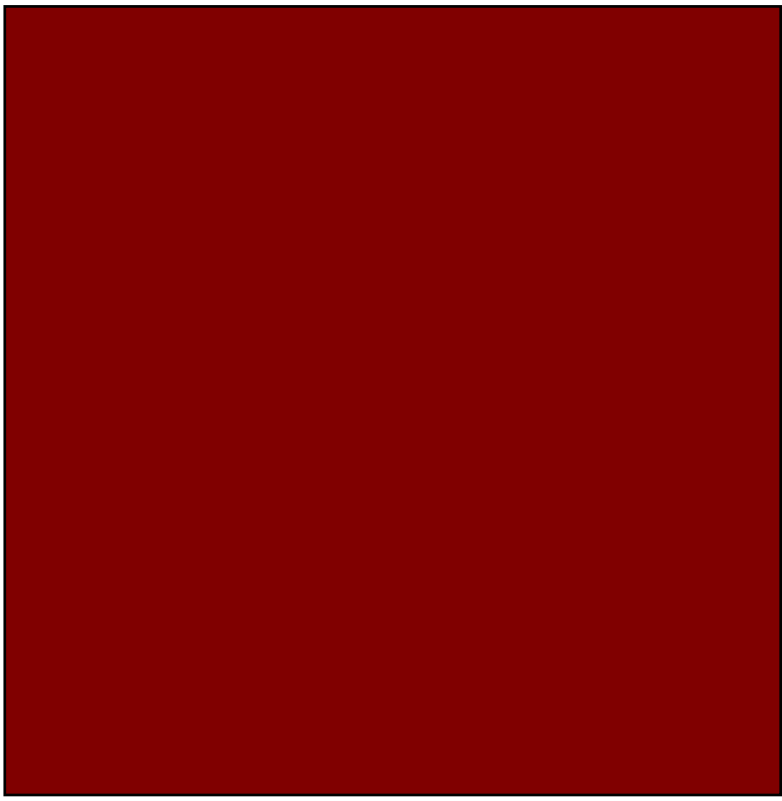
Por si lo anterior no bastara, cuando la fiscalía recibió por fin los videos de las cámaras de seguridad públicas, las obsoletas y desconectadas computadoras con que contaban no permitieron abrir los archivos. Cuando por fin un equipo pudo visualizar el video, no podía practicarse sobre las imágenes ni siquiera un zoom. Mal equipo, nulo software útil y una falta de conexión a internet para poder improvisar: un coctel desastroso.

d) El troleo online y la falta de respuesta institucional.

Desde luego, el problema de las amenazas en la red no es exclusivo de México y es en sí mismo un inagotable dolor de cabeza para todos los involucrados. Lo que en el caso de Andrea resulta incomprensible es que a pesar de que temía por su seguridad e informara a las autoridades del creciente hostigamiento que padecía en redes sociales (en donde recibía imágenes de su cuerpo decapitado, por ejemplo), los funcionarios le insistieron que volviera al país para proporcionar cierta información, porque, claro, la vida de alguien puede descarrilarse por algo ocurrido en línea pero no es posible coadyuvar con la autoridad a distancia por medio de por internet. Las semanas y meses transcurridos desde el ataque y la viralización del video provocaron que el daño mayor se continuara gestando en línea, y ante ello las autoridades optaron por el camino más socorrido en México: no hacer nada. En este caso, un activista ofreció una mejor perspectiva al relacionar varias amenazas a una red de unos 200 trolls vinculados a su vez con un periodista misógino. Sin embargo, el propio activista tuvo que huir a España al volverse luego él mismo un blanco de ataques por su labor.

A manera de conclusión. México, como muchos otros países de latinoamérica, cuenta con instituciones débiles que no saben o no pueden explotar las herramientas tecnológicas existentes o, peor aún, contribuyen a agravar los problemas derivados del uso de las TIC. Para crear una policía cibernética eficaz hay que empezar por contar con una policía eficaz. Si no tomamos en cuenta toda esta clase de factores o si pensamos los problemas propios del derecho informático olvidando que aún estamos muy lejos de solventar conflictos más "tradicionales", los expertos en esta rama del quehacer jurídico corremos el riesgo de apenas generar o aportar otra pieza aislada e incomprensible a un rompecabezas que de suyo resulta ya enredado y caótico. Andrea, y miles de víctimas como ella, no merecen esto.

Autor: Erick López Serrano. Maestro en Derecho y Tecnología por la Universidad de Tilburg, Holanda.



ELDERECHOINFORMATICO.COM

TODA LA INFORMACIÓN EN UN SOLO LUGAR

SOMOS EDI LA RED

EL CENTRO DE INFORMACIÓN

y contenidos
más grande iberoamerica

TWITTER: ELDERECHOINF