Arte de tapa: Diseño Manuel T Zamora - Dibujo:arte_master

EDI

Revista Digital
Abril 2019 Vol.31
distribución gratuita

10 EDI AÑOS

ElDerechoInformatico.com

EDI

CONGRESO INTERNACIONAL DE DERECHO INFORMÁTICO

"desafíos legales y tecnológicos"

27/28 de Junio 2019
Lugar: Bolivar 177 2do piso

Auspicia: ASOCIACIÓN DE MAGISTRADOS CABA

MAFUCABA

APOYAN:

Adpl
Instituto Argentino de Derecho Procesal Informático

ADIAr
Asociación de Derecho Informático de Argentina

CIBERSEGURIDAD
<LATAM>

INDICE

Red Iberoamericana ELDERECHOINFORMATICO.COM (EDI)
EDICIÓN N° 31
DIRECCIÓN POSTAL: 9 DE JULIO 585 OF. 2 CP 9100
TRELEW / CHUBUT / ARGENTINA

LA RED EDI

INFORMACIÓN QUE SUENA BIEN

WWW.ELDERECHOINFORMATICO.COM

EDITORIAL

GUILLERMO M ZAMORA - DIRECTOR EDI

"No te quedes en el pasado, corre hacia el presente y crea un futuro."
- Anónimo

Si mal no recuerdo era un marzo de 2009, en una noche distraida se me ocurrió que un facebook de derecho informático era buena idea, así nació derechoinformatico.ning.com con un sentido de la estética que digamos dolía la vista, como todo salvador, cuando menos lo esperaba aparece un pibe ofreciendo su generosa contribución, (el "pibe" es uno de los más reconocidos abogados/informáticos del Derecho Informático en Argentina), su nomnbre es Marcelo Temperini, se ofreció a diseñar una estética más digerible, y por supuesto que dije que si!
Pasó el tiempo, y sobre fin de año, decidimos, migrar el dominio a un hosting propio, Marcelo que es una de las personas más capaces y trabajadoras

que he conocido dijo que si y diseño la primera versión de la Red y crecimos, y crecimos, y tuvimos nuestro diplomado, nuestra librería, nuestra revista, nuestros foros nuestros etc etc, aprendimos, conocimos gente, fuimos tomando vuelo propio, y Marcelo entendió que su lugar en ésta, su Red estaba cumplido, y avanzó al siguiente nivel poniendo su propia empresa, honestamente me sentí perdido, él se encargaba de todo, yo solo tenia alguna que otra idea que el desarrollaba, fue en el 2014, y ahí la Red dio otro salto, no mejor, pero si distinto, reformulé el concepto de su objeto y fines, siguió la revista, el diplomado, sumamos corresponsales en todo latinoamérica, comenzamos con los Congresos Internacionales, algunas campañas de concientización, cambiamos y cambiamos, y procuramos ser referentes de la materia lográndolo algunas veces y otras no, lo que importó siempre me parece, es que estuvimos y estamos después de 10 años y no es poco.-
Gracias a Marcelo, y a todos aquellos que están desde el principio y no me animo a enumerar por miedo a olvidar a alguno y que siguen acá, gracias a los que dejaron su huella y a los que aportaron desde su lugar, gracias a Uds que nos leen y nos dan ganas de seguir estando.-
Brindemos por 10 años o más!

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

APANDETEC
DERECHO Y NUEVAS TECNOLOGÍAS

LAW-TIC® Grupo Jurídico
www.lawtic.com.co

fundación Gema

ICE para el desarrollo

CONCIENCIA EN RED

YSC
YO SOY CURUNDÚ

AALCC
Asociación Argentina de Lucha Contra el Cibercrimen

PANAMÁ LIBRE DE BULLYING

UKUN
Aromas y Terapias

ODAID
Organización de Ayuda Integral para el Desarrollo

INTERACTUEMOS
DERECHO
TECNOLOGÍA
Y CIENCIA
@edukarenconpedesabilion
#interactuemosderechotecnologiayciencia

FORENSIC
DIGITAL EXPERTS

FUNDACIÓN EDUCACIÓN VIAL

MOVIMIENTO NUEVA GENERACIÓN
20 AÑOS

Centro de Investigación Nueva Escuela Panamá.

FUNDACIÓN
Creo en milagros

Fundación AGUA TIERRA

DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS

GLOBAL Brigades

FUNDACION latidos

eVenezuela.org

www.elderechoinformatico.com

Las redes sociales han sido creadas con el fin de que a través de las mismas sus usuarios interrelacionen[1]. No obstante esto, como en toda cuestión relacionada a lo social, es bien sabido que no siempre se interactúa en términos amistosos, o no agresivos al menos. El problema radica cuando se traspone la delgada línea de lo confrontativo, en un contexto razonable, a lo netamente agresivo, con una marcada intencionalidad destructiva hacia el otro.

Violencia Digital
La peligrosa práctica de los escraches

Abog. Rubén Avalos .

Es aquí donde la práctica del escrache, según palabras de Roberto Balaguer [2] "*es utilizada como defensa frente a un ataque. Pero es un arma de destrucción masiva y dependerá de la ética personal utilizarla o no*"

He aquí donde las redes sociales comienzan a ser utilizadas como antisociales, aportando ocasionalmente un medio poderoso para que personas que hayan sido, o no, víctimas de otra persona (otro ser humano, valga la redundancia) lo defenestren a diestra y siniestra.

Salvando las distancias con las hordas medievales, la diferencia radica en la Tecnología. El inconsciente colectivo hace su juego.

Que persona puede ser igual después de un ataque de este tenor, al margen de si es efectivamente o no responsable de lo que se le endilga.

Un caso desgraciadamente notorio es el de Agustín Muñoz, un joven barilochense, de 18 años de edad, acusado por una amiga de que la había abusado. Agustín se quitó la vida. A posterior la acusadora se disculpó por difamarlo. El grave daño estaba hecho.

Esto grafica la existencia de distintos vacíos:

[1]Obviamente el fin económico es el perseguido por la empresa.

[2]Psicólogo y Magíster en Educación con Especialización en Redes Sociales

El de la familia de Agustín y la sociedad, con un integrante menos por un absurdo. El de la educación de la joven, ella misma y su familia ya no volverán a ser lo mismo.

El de las personas que se plegaron a la manifestación y escraches, sin haberse interiorizado al menos si existía denuncia penal o intención de realizarla, han tenido una lección de la manera más dura, la vida de alguien que después tuvieron noticia de que era inocente.

Todos terminaron siendo víctimas de la vorágine del escrache. Uno en su vida, todos en su psiquis.

Por otro lado existen los vacíos institucionales por así decirlo: La empresa de la Red Social, por no desarrollar algoritmos para identificar cuando se utiliza su plataforma para estas prácticas similares a plaza de ejecución del medievo. Asimismo, a pesar de parecer un difícil camino, se debería sancionar a dichas empresas por no cumplir con el deber de Seguridad[3] e incluso el trato digno[4] que como empresa le correspondería, máxime interactuando en el Estado Argentino

El último pero no menos importante, El Estado Argentino a través de su cuerpo legislativo, debiera regular de manera más afectiva este tipo de acciones, cuando trasponen los límites del Derecho de Libertad de Expresión.

En el ámbito local mediante querella por calumnias e injurias es un mecanismo de acción, pero tiene un coste económico que debe sustentar quien se siente víctima.

A nivel penal, si no media al menos una amenaza, no encuadra en delito.

En Juzgados Contravencionales, en la Provincia de Santa Fe podría incurrir en el Artículo 64 de Código de Convivencia, Ley Provincial Nro. 13774 (Actos Turbatorios o Molestias).

Se puede reclamar Responsabilidad Civil en concepto de Daños y Perjuicios a la Imagen, Honor o Reputación de la persona.

Mientras tanto la persona agredida, de tener presencia en la red pasa a encontrarse en la red, pero enredada.

Nuevamente citando a Balaguer, la formación en ciudadanía digital debe ser una asignatura obligatoria en los

[3]Protección al Consumidor, Art. 5, Ley 24240 de Normativa de Defensa del Consumidor, entiéndase por salud, no solo la física, sino también la emocional

[4]Trato Digno, Art. 8 bis, Ley 24240 de Normativa de Defensa del Consumidor

colegios como lo fue en algún momento la instrucción cívica.

Más allá de lo expuesto es importante concientizar a las personas para lograr que la Red no se convierta en una telaraña.

Dr. Rubén Ávalos
Corresponsal Red Iberoamericana de Derecho Informático para el interior de Argentina

@eddakarencespedesbabilon

#interactuemosderechotecnologiayciencia

EKCB

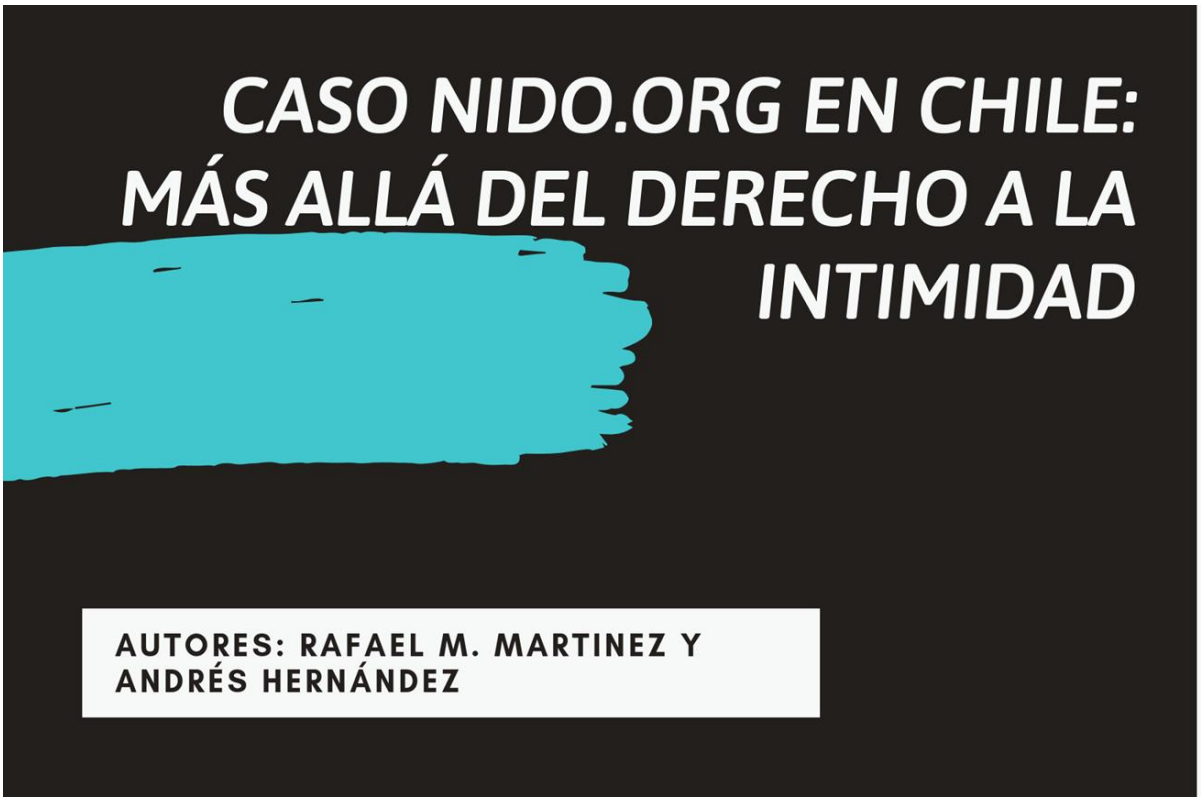
INTERACTUEMOS DERECHO TECNOLOGÍA Y CIENCIA

Una constante investigación del avance de las Tecnologías, unida a la pasión por el Derecho en interacción con la Ciencia. Nuestra bandera es la Concientización Digital, y esencialmente el respeto por los DDHH y la lucha contra la Violencia Digital en un trabajo altruista para bien del desarrollo socioeconómico y tecnológico de la sociedad a nivel mundial.

EDDA KAREN CÉSPEDES BABILÓN

Seguimos adelante con la "Concientización Digital"

https://www.facebook.com/EddaKarenCespedesBabilon/



NIDO funcionaba como un imageboard (tablero de imágenes) y en su contenido existían grupos que se dedicaban exclusivamente a compartir imágenes de mujeres; y a la vez la comunidad se organizó mediante canales a través de la aplicación de mensajería Telegram.

Tras revisar parte del contenido publicado y leer ciertas denuncias, es indudable que en NIDO se distribuyeron imágenes sin consentimiento de las personas que en ellas aparecen, pero también se debe resaltar que su fuente principal de contenido fue Instagram. Si bien Instagram es una red social legítima, con los años han surgido pequeños grupos de usuarios que se dedican a ofrecer servicios de carácter erótico y hasta cierto punto sexual.

Una de las actividades más rentables para este pequeño grupo de sexual entertainments es la venta de fotografías, videos e incluso videollamadas; a estos productos se les conoce como packs, pero obviamente esta actividad se presta para reventas y en muchos casos para intercambios entre los compradores.

En muchos casos el contenido de estos packs se hace público, volviendo a la persona objeto de ataques y críticas por parte de su entorno íntimo, llegando a veces al extremo del repudio familiar y la pérdida de trabajo.

Otro grupo de imágenes pertenecen a personas que sencillamente publicaron sus fotografías en traje de baño, ropa interior, etc. Este tipo de imágenes son muy comunes -pero no exclusivas- en cuentas que tratan de obtener cierto perfil público, con la idea de comercializar a futuro.

El tercer grupo de fotografías publicadas no fueron generadas con la intención de ser compartidas. Fueron imágenes producto de relaciones íntimas y privadas, que lamentablemente de manera legítima o no, cayeron en manos de alguna persona que las hizo públicas.

Obviamente hablamos de material gráfico íntimo con un alto contenido sexual.

La razón por la que hacemos esta distinción, es porque para el ámbito jurídico es sumamente importante distinguir tres elementos esenciales: a.) la forma en que se genera el contenido, b.) la intención con la que se genera el contenido y c) la forma en que se tiene acceso y posesión del contenido.

Usemos a Silvia como ejemplo:

Hipótesis 1: Silvia recibe la noticia que sus fotografías se encuentran publicadas en un foro donde se habla sobre su imagen : No se podría alegar una violación a su intimidad porque un sujeto descargó fotografías de su cuenta y distribuyó las mismas en un sitio web. Las fotografías fueron obviamente consentidas por Silvia. Asimismo, su intención es hacerlas públicas, es darse a conocer a través de esta imagen. El hecho que las fotografías se encuentren en otro servidor o servicio, no atenta contra su intimidad.

Hipótesis 2: Sus fotografías están siendo usadas por terceros para obtener beneficios económicos o de otro tipo : Si bien publicó las fotografías con la intención de que el público en general tuviera acceso a ellas, también es cierto que posee derechos de autor sobre su imagen, lo que le da una titularidad para protegerla y en

consecuencia decidir el uso que a dicha imagen se le da.

Descargar imágenes de redes sociales no es ilegal, pero su uso no autorizado sí puede ser controlado.

Hipótesis 3: Que las imágenes de Silvia sean utilizadas sin su autorización en algún medio o sitio web que promociona servicios sexuales : Esta práctica es más común de lo que las personas creen y es una de las más denunciadas por modelos e influencers de Instagram . Consiste en crear una cuenta falsa o sitio web con el objetivo de hacerse pasar por la persona que aparece en las imágenes y ofrecer servicios como venta de packs y en otros casos de escorts. En este caso Silvia sería posible víctima de difamación, injuria y escarnio público, ya que su imagen no solo se estaría usando para cometer fraude, sino que adicionalmente se perjudica su honor.

En el caso NIDO se registraron boards donde los usuarios publicaron imágenes de mujeres e incluían datos personales de contacto, así como sus direcciones de residencia. Se hicieron publicaciones donde daban a entender que la persona debía ser secuestrada con el único propósito de someterla a abusos sexuales; y en otros hilos afirmaban tener encargos de organizaciones criminales que les pagaban por cada víctima que les entregaran.

Como podemos inferir, todas estas personas fueron víctimas de un Doxing masivo con fines criminales. Obviamente estamos ante una situación donde no solo se violan derechos básicos de las personas como el derecho a la intimidad y al honor, sino que adicionalmente estamos en presencia de un grupo organizado con la intención de conspirar contra mujeres, bien sean adultas o menores de edad. El caso de estudio nos advierte que en la comunidad existían personas que simulaban hechos punibles, posiblemente buscando algún reconocimiento. Esto es alarmante, pues está psicológica y

sociológicamente demostrado que, la necesidad de una persona en búsqueda del reconocimiento del grupo, puede llevar a la materialización del delito, como en los casos de las pandillas callejeras, donde incluso el sujeto se somete asimismo a vejaciones.

Debemos superar esa errónea afirmación de que la violencia se presenta únicamente en estado físico. El simple hecho que se revelen datos íntimos, como la dirección de tu hogar con el objeto de agredirte, es violencia.

Si bien todo este escándalo es preocupante, igual debe llamar la atención de los usuarios de las TIC , quienes son los principales responsables de cuidar sus datos personales, especialmente cuando se trata de producir contenidos de carácter sexual. Es importante ser más conscientes a la hora de querer inmortalizar un momento tan íntimo por medio de dispositivos o medios electrónicos, ya que éstos tienen la lamentable particularidad de dejar rastros de su existencia, aun cuando los autores del contenido deciden eliminarlo.

Todas las personas tienen derecho de hacer en su intimidad lo que se les ocurra, ya que es un derecho fundamental, así como tienen la potestad de decidir que parte de su vida íntima quieran compartir o revelar.

Existen algunas prácticas muy habituales en la sociedad de la información que se han popularizado con el desarrollo de las TIC , y una de ellas se llama Sexting , y es aquí donde muchas veces nos convertimos en nuestro propio verdugo contra el derecho a la intimidad.

Hoy en día existe una práctica llamada Sexting. Esta se ha masificado increíblemente en las parejas, especialmente en las más jóvenes y en aquellas que por motivos migratorios se encuentran separadas por la distancia.

El Sexting , (sexo por texto o mensajes), consiste en el envío de contenido sexual, erótico o pornográfico a través de los medios de comunicación digitales o electrónicos, generalmente se realiza en un ambiente de confianza y lo más importante: con el consentimiento de las partes.

Para muchos es una práctica inofensiva, sin embargo, lo que debería ser un simple juego erótico y placentero puede provocar un caos sin precedentes si no se toman en cuenta las precauciones debidas. Practicarlo

no debe ser considerado algo indebido o dañino per se , a menos que el contenido generado trate de incluir personas que no han dado consentimiento para su difusión o producción, incluya menores de edad o sea enviado a menores de edad o a personas sin previa autorización.

En Venezuela no existe un tipo penal específico sobre la materia, sin embargo hay un conjunto de normas legales que podrían aplicarse, entre ellas están:

● Ley especial contra los delitos informáticos: Art. 22, sobre el Delito de revelación indebida de datos o información de carácter personal.

● Ley Orgánica sobre el Derecho de las Mujeres a una vida libre de violencia: Define el delito de acoso u hostigamiento, con pena de prisión de 8 a 20 meses.

Si decides generar para fines privado algún contenido de esta clase, debes tener en cuenta las siguientes recomendaciones básicas:

1. Si decides junto a tu pareja u otra persona tomar foto o grabar un video de sexo explícito, es preferible borrarlo una vez lo hayas visto y nunca expongas tu rostro.
2. No lo compartas con extraños o personas que apenas conoces virtualmente.
3. Instala antivirus o cualquier otra solución de seguridad que te permita asegurar que tu dispositivo esté libre malwares.
4. Utiliza aplicaciones seguras para el intercambio de material íntimo, principalmente aquellas que te garantice destrucción inmediata del contenido.
5. Si decides almacenar contenido íntimo en tus dispositivos, utiliza

programas para encriptar la información.

6. Evitar utilizar Wi-Fi públicas o desprotegidas para el intercambio de material íntimo. Pueden correr con la mala suerte de toparse con un ciberdelincuente.

7. Siempre mantén tapada la cámara web de tu PC o Laptop, no es ser paranoico, es ser preventivo.

8. Respeta la confianza de la otra persona que compartió su intimidad, no lo divulgues bajo ningún concepto.

9. Si eres menor de edad, NO lo hagas.

Para que una imagen o video íntimo llegue a Internet, es necesario primero crearlo, y es ese momento donde debes preguntarte: ¿Es necesario hacerlo? ¿Podría perjudicarme en mi relación de pareja, familia o trabajo? ¿Qué puedo ganar y qué puedo perder?

En fin, si tu imagen o video íntimo llega a Internet sin tu consentimiento, es importante y necesario que interpongas la denuncia ante los organismos policiales. No debes temer, y confiar en el trabajo técnico/investigativo de los cuerpos de seguridad que ya cuentan con Unidades de Investigación especializadas sobre la materia

TIPO DE PROGRAMA: Programa Ejecutivo

DURACION Y DEDICACION: El programa consta de 44 horas presenciales más un cierre de programa con una mesa de debate con speakers invitados.

FECHAS: 22 al 27 de julio del 2019

HORARIOS: Lunes a Viernes de 9 a 13 hs y 16 a 20 hs
Sabado de 9 a 13 hs y 14 a 15:30 hs (Mesa de Debate)

LUGAR DE DICTADO: Vicente López 1950 CABA

DIRIGIDO A:
Abogados – Comunicadores – Periodistas - Funcionarios públicos – Empresarios - Estudiantes avanzados
REGIMEN DE APROBACIÓN: Asistencia al 75% de los módulos.

E-MAIL DE CONTACTO: derecho@cudes.org.ar

TELÉFONOS: (11) 4803-6041 / Celular: 15-2738-7910 www.derecho.cudes.org.ar

¿Estamos en los umbrales de una nueva inquisición?

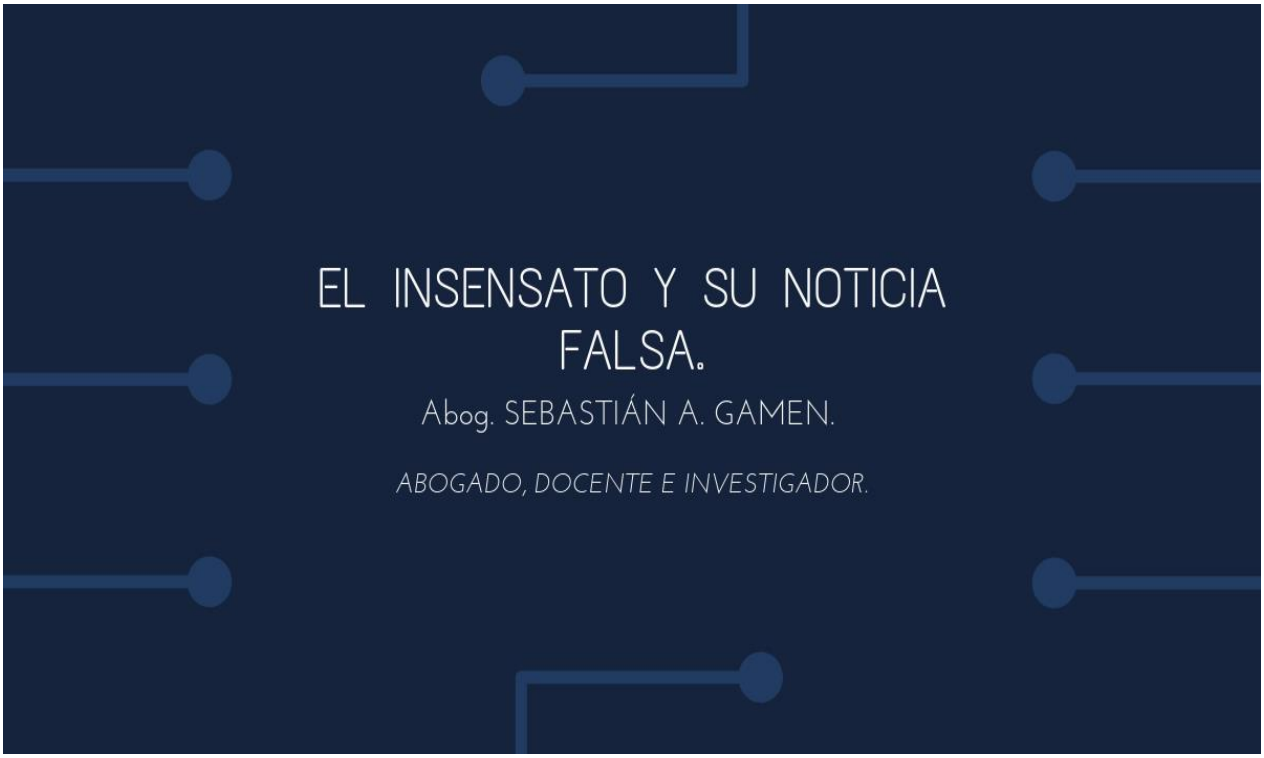
Muchas veces hemos escuchado que las cosas cambian para que nada cambie, un juego de palabras de una verdad absoluta que nos dejó Giuseppe Tomasi di Lampedusa. El poder político entendió muy bien eso.

En el siglo 21 el fenómeno de las noticias falsas nos está aturdiendo el pensamiento. Todo es falso, ¿o todo es verdadero? ¿Cómo distinguir?

El 08 de enero de 1642 abandonaba el mundo el insensato, el creador de la fake news más viralizada por la faz de la tierra, Galileo Galileu. Este personaje que trascendió a la posteridad tuvo la mala idea de decir que la tierra giraba alrededor del sol, poniendo en duda el geocentrismo. Esa noticia era “falsa” para la época y casi lo llevó a la hoguera. Se supo que escribió una carta amenizando sus dichos, y volviendo sobre sus pasos. Fueron 300 años después que se supo la verdad, y Galileo tenía razón.

Quise comenzar el artículo con un repaso de las teorías del insensato para poder pensar mejor en el problema que nos aqueja.

Fue hace muy poco (2014) que hubo una explosión en la medicina por las campañas anti vacunas. William Thompson, científico del Centro de control y prevención de enfermedades (CDC) de los Estados Unidos buscaba un nexo entre la vacuna triple viral y el autismo, investigación que nunca vio



la luz por falta de pruebas científicas. Estas investigaciones fueron tomadas por Brian Hooker, ingeniero bioquímico e padre de un hijo autista, y en 2014 publicó un paper afirmando que existía un vínculo comprobado. Para llegar a esa afirmación Hooker cometió errores estadísticos básicos. Inmediatamente fue desmentido por la misma revista que lo publicó. No obstante el daño ya estaba hecho. Se levantaron en todo el mundo campañas anti vacunación, que hasta el día de hoy se mantienen vivas. La posverdad en su máxima expresión.

El problema de las noticias falsas es grave, pero mucho peor podría ser la censura, y muchísimo más grave puede ser la autocensura.

El problema de las noticias falsas.

Antes de entender el problema de las noticias falsas, me gustaría definirlas. Se habla mucho de las noticias falsas pero, ¿realmente estamos entendiendo que son?

El diccionario Collins, define a las noticias falsas como "información falsa, frecuentemente sensacionalista, diseminada bajo el disfraz de reportaje de noticias"[5]. Por su parte, Cortez e Isaza nos dicen que

> Se trata de contenidos deliberadamente falsos que se publican en sitios web cuya apariencia intenta ser formal y auténtica. A veces el diseño del sitio y su URL suplantan un portal de noticias reconocido. El propósito claro es engañar al usuario. Generalmente estos contenidos se mueven en redes sociales a través de las cuentas propias de esos portales, ya sea de manera orgánica – mediante *likes*, *retweets* y compartidos de los usuarios– o con acciones promocionadas, es decir, pagando para que estos contenidos sean publicitados por las plataformas[6].

[5]Flood, Alison, "Fake news is 'very real' word of the year for 2017", *The Guardian*, 2 de noviembre de 2017, recuperado de https://www.theguardian.com/books/2017/nov/02/fake-news-is-very-real-word-of-the-year-for-2017 .en 03/03/19.

[6]Cortés C. y Isaza L., Noticias falsas en Internet: la estrategia para combatir la desinformación, Diciembre 2017. Universidad de Palermo.

En la definición que nos trae el diccionario de Collins nos topamos con el problema de definir información falsa, principalmente en la era de la posverdad. ¿Es falso todo aquello que no está científicamente probado?

¿Quién dirime lo que es falso y lo que es verdadero?

En la definición que nos acercan los autores Cortez e Isaza nos topamos con la expresión deliberadamente, que a los abogados nos trajo muchos dolores de cabeza. Además, los mismos autores complican aún más la situación cuando agregan que el propósito claro es engañar al usuario. Si retomamos los ejemplos que di al comenzar este artículo vemos que en ninguno de los dos supuestos hubo intención de engañar a nadie, simplemente se divulgó una información, tan simple como ello.

Voy a usar un tercer ejemplo para ver mejor lo complicado que resulta determinar la falsedad de una noticia en algunos supuestos.

En el año 2008 se informó que Barak Obama habría nacido en África y por ello se lo acusó de haber violado el juramento a la bandera que hiciese en la escuela, y asimismo de no poder ser presidente de los Estados Unidos. El escándalo fue bautizado como *Birthers*. Para contrarrestar esa noticia Obama divulgó la foto de su partida de nacimiento. Después de ello, en julio de 2009 el director del Departamento de Salud de Hawai dijo que los registros del nacimiento del presidente estaban archivados. En el año 2011 se divulgó nuevamente el certificado de nacimiento en la web de la Casa Blanca. Antes de este último hecho, el 45% de los ciudadanos norteamericanos ponía en duda la nacionalidad del presidente. Sorprendentemente, en enero de 2012 el porcentaje se mantenía en el 41%.

Es decir, a pesar de las pruebas contundentes sobre el lugar del nacimiento las personas seguían creyendo en la noticia falsa.
Pensemos en la inmensa cantidad de noticias que recibimos diariamente y que no necesariamente caen en el absurdo o en la obviedad de los falso, y descansan en una zona gris, confusa entre lo real y la mentira. Sin dudas, estamos frente a un problema muy pero muy grande.

Posibles soluciones.

Una de las primeras soluciones para detener el tsunami de noticias falsas es el propio control de los medios de divulgación.
La cadena de noticias BBC creo un equipo para identificar noticias falsas en todas sus formas. Lo que propone la empresa es chequear las informaciones más populares de las redes sociales, como Facebook, Instagram y Google. Además de su propio equipo, la BBC afirmó que está trabajando con Facebook en particular para ver cómo resolver el problema de las noticias falsas.

Los principales jugadores de internet también demuestran su preocupación. Google fundó la *Digital News Initiative*, que financia la organización Full Fact que se encarga de chequear las informaciones de manera automatizada.
En enero de 2017 Facebook anunció su propio proyecto (Journalism Project) que también busca detener la proliferación de noticias falsas.
Destacamos que la empresa Facebook fue la más golpeada por el escándalo de las noticias falsas, y la manipulación política de las elecciones en los EEUU. Esa preocupación se materializó en el trabajo con otras empresas, como ABC News, AP, Factcheck.org, PolitiFact e Snopes.
Tim Cook, CEO de Apple, dijo que las noticias falsas están matando la mente de las personas y que los gigantes tecnológicos deben trabajar para impedir la difusión.
Vale aclarar que los grandes jugadores de internet deberán tomar distancia de los negocios que hay detrás de las noticias falsas, especialmente el nicho de los click bait. Ello si desean realmente terminar con el problema.
Al margen del esfuerzo que están haciendo las empresas de internet por frenar las noticias falsas, no me simpatiza la idea de que sean ellos los verdugos de los contenidos. Internet

nació libre y debe mantenerse de ese modo.

Existen proyectos de ley en varios países que pretenden incriminar por la divulgación de las noticias falsas a quién la dice, a quienes las divulgan y a las redes sociales o plataforma que

facilita la publicación.

En ese sentido en Brasil hay un proyecto para considerar delito

> la actividad de producción y circulación de noticias falsas que tengan la intención de manipular la opinión pública, modificando el Código Electoral brasilero (art. 354 da Lei 4.737/1965), al prever como "infracción la creación y divulgación de noticias "que se sabe son falsas" y que puedan "distorsionar, alterar o corromper gravemente la verdad relacionada al proceso electoral". Ante su identificación, los contenidos deberán ser removidos en un máximo de 24 horas desde la notificación, sin orden judicial previa. En caso contrario, las empresas intermediarias de Internet serán responsables civilmente por incumplimiento[7].

La Coalición Derechos en la Red criticó fuertemente el proyecto por violentar la libertad de expresión en línea, "la idea de eliminación automática de contenido debe ser inmediatamente rechazada. El escrutinio judicial, tal como se prevé en el Marco Civil (de Internet), es fundamental para que la ponderación entre libertad de expresión y daños al honor ocurra de forma equilibrada por la autoridad judicial".

La solución judicial me interesa más, aunque no me convence del todo.

Volviendo a la historia del insensato vemos que un tribunal lo quiso llevar a la hoguera.

[7]Recuperado de http://www.observacom.org/organizaciones-sociales-rechazan-proyecto-de-ley-sobre-noticias-falsas-a-estudio-en-brasil/ el 04/03/19.

Nuevamente me criticarán por extremista, pero mi preocupación radica en los grises. Esas noticias cuya veracidad puede ser discutida son las que debemos dejar vivir, porque abortarlas prematuramente puede ser un crimen muy grande para la sociedad. Después de todo, censurar a los terraplanistas ni siquiera vale la pena.

Ahora, inmediatamente, para contener la proliferación de noticias falsas tenemos que apostar por la educación de los ciudadanos. Ellos deben ser los criteriosos, sus propios inquisidores 2.0 para discernir lo verdadero de lo falso, lo posible de lo irreal.

Conclusión.

Hay un abanico inmenso de noticias que son grises y por ello, categorizarlas como falsas sería apresurado, inapropiado y peligroso. La verdad que abrir la puerta de la censura sería lamentable para el progreso de la sociedad, sería retroceder varios años de libertad y volver a un control, insoportable para el siglo 21 que estamos viviendo.

Al comienzo de esta columna pensé en el caso de Galileo y para concluir me pregunto, ¿Quién podrá ser el insensato que censure a los insensatos?


eVenezuela
.org

Al plantearnos las preguntas, ¿desaparecerá el notariado con las nuevas tecnologías?, ¿Los nuevos servicios de certificación informáticos sustituirán al notariado anglosajón o latino?; analizando las anteriores preguntas, tenemos que recodar y se nos viene a la memoria la gran tradición y antigüedad de la propia institución, y como muestra tenemos a los *escribas* del Derecho Egipcio y aquellos *tabellones* o *tabulari*s del Derecho Romano; así como los *Tlacuilos* del Derecho Azteca, por lo que no obstante su antigüedad y su larga tradición, el mismo ha sido objeto de una larga, firme evolución y modernización.

Modernización generada, de manera obligatoria por las grandes transformaciones de la sociedad en virtud de las nuevas tecnologías, la inteligencia artificial y por supuesto de las redes sociales, primero por la sociedad de la información y posteriormente por la sociedad de redes, y más aun con la llamada web 5.0 y en especial los nuevos servicios de certificación informática.

Si recordamos la evolución de la web, tenemos que señalar que la evolución de la web, siguiendo a Infotecnarios http://www.infotecarios.com/estamos-listos-la-web-5-0/#.XHWb0ohKiUk

Web 1.0

Empezó en los 60´s, webs unidireccionales y no colaborativas; contenido solo en texto, solo lectura y páginas estáticas y por lo tanto una interacción mínima. El ejemplo más representativo es ELIZA, y posteriormente, surgió el HTML (Hyper

Text Markup Language), que traducido, es lenguaje de marcación de texto, .por lo que es una herramienta para que la computadora conectada a Internet interprete como visualizar el documento.

Por lo que debemos señalar como ventajas:

- Sencillo que permite describir hipertexto.
- Texto presentado de forma estructurada y agradable.
- No necesita de grandes conocimientos cuando se cuenta con un editor de páginas web o WYSIWYG.
- Archivos pequeños.
- Despliegue rápido.
- Lenguaje de fácil aprendizaje.
- Lo admiten todos los exploradores.

Y respecto a las Desventajas:

- Lenguaje estático.
- La interpretación de cada navegador puede ser diferente.
- Guarda muchas etiquetas que pueden convertirse en “basura” y dificultan la corrección.
- El diseño es más lento.
- Las etiquetas son muy limitadas.

Web 2.0

El término fue usado por primera vez por Darcy DiNucci en 1999 en un artículo denominado “Fragmented Future”; es la web puramente social, ya que enfatiza la colaboración online, en otras palabras un usuario/a más activo/a. Páginas web más accesibles, eficientes y dinámicas.

Incorporando la presentación en imágenes, texto, audio, etc., lo que implica la evolución de las aplicaciones digitales y por último, los formatos utilizados principalmente son Java script, PHP. Utilizado principalmente en páginas web. Es similar a Java, aunque no es un lenguaje orientado a objetos, el mismo no dispone de herencias. La mayoría de los navegadores en sus últimas versiones interpretan código Javascript, dicho código puede ser integrado dentro de nuestras páginas web. Para evitar incompatibilidades el World Wide Web Consortium (W3C) diseño un estándar denominado DOM (en inglés Document Object Model, en su traducción al español Modelo de Objetos del Documento).

Respecto a sus ventajas:

- Lenguaje de scripting seguro y

fiable.

- Los script tienen capacidades limitadas, por razones de seguridad.
- El código Javascript se ejecuta en el cliente.

Desventajas:

- Código visible por cualquier usuario.
- El código debe descargarse completamente.
- Puede poner en riesgo la seguridad del sitio, con el actual problema llamado XSS (significa en inglés Cross Site Scripting renombrado a XSS por su similitud con las hojas de estilo CSS).

Web 3.0

También llamada Web semántica, presenta las siguientes características: Uso de datos semánticos, adaptable a cualquier dispositivo, con contenido libre, destaca por los espacios tridimensionales, es muy importante la llamada computación en la nube, y ofrece búsquedas inteligentes y su principal aportación la importante evolución de las redes sociales.

Respecto a sus ventajas:

- Identificación de perfiles, aficiones, gustos, costumbres, conectividad, interactividad, usabilidad.
- Rapidez en las búsquedas.

Desventajas:

- Vulnerabilidad de datos personales.
- Bases de datos que recopilan información.

Web 4.0

Según Raymond Kurzweil, científico especializado en inteligencia artificial, la web 4.0 o también llamada Web ubicua, sería paralela al funcionamiento del cerebro humano y podría llegar un punto en el que por poner un ejemplo un smartphone podría reconocer y alertar a su dueño si llegará tarde a una reunión, tendiendo acceso a la información de su calendario, su geolocalización y tránsito en vialidades, es decir, se convertirá en un agente predictivo. Se pretende llegar a una red que no solo sea capaz de buscar y encontrar información, sino de brindar soluciones a partir de la información que le damos y de la que se genera en la red. Se fundamenta en cuatro pilares:

1. La comprensión del lenguaje natural y tecnologías Speech to text (de voz a texto y viceversa).
2. Nuevos modelos de comunicación máquina a máquina (M2M).
3. Uso de la información de contexto. Por ejemplo, ubicación que aporta el GPS, ritmo cardíaco que tu smartwatch registra, etc.
4. Nuevo modelo de interacción con el usuario.

Entre sus características principales encontramos: Uso de gafas especiales lo que permite dialogar de forma natural y en línea con una agente virtual inteligente, ahora se tendrá acceso a internet por medios de un “dispositivo, delgado, ligero, portátil y con muy alta resolución”, integrado en una serie de objetos y vehículos, el llamado internet de las cosas.

Respecto a sus ventajas:

- Interactividad.
- Captura la atención.
- Se pueden realizar pagos, trámites y en algunas escuelas existe el servicio de tareas y notas.

Desventajas:

- Dependencia, casi total, del sistema a la conexión de Internet.
- Vulnerables a ataques de virus, troyanos, espías, etc.

Web 5.0

Presenta y fomenta el uso de un dispositivo todo en uno. Se pretende identificar y categorizar emociones, buscando la realidad sensorial y lo más importante el desarrollo más tangible de la inteligencia artificial y en proceso de construcción y mejora.

Es importante señalar que desde la web 1.0 y hasta al web 4.0 se ha tenido una web emocionalmente neutra, pero a partir de la web 5.0 o también llamada web sensorial, está será encaminada a poder identificar las emociones de los usuarios, por medio de los dispositivos, productos y/o servicios, y sí… esto parece salido de la ciencia ficción pero cada vez más se mezclan y ese momento ya llegó y crecerá como en su momento florecieron otras características de la web, como el rastreo de frases emotivas en la web.

Ajit Kambil (Global Director of Deloitte Research, Boston, Massachusetts, USA) menciona lo difícil que es mapear las emociones, más no imposible y que con los dispositivos adecuados como pueden ser implantaciones neuronales, se pueden personalizar de tal manera, que causen ese impacto en las y los usuarios.

Respecto a sus ventajas:

- Modificar información en la página de forma rápida.
- Fácil navegación.
- medio económico de publicidad.
- Cuenta con un editor en línea para su uso.
- Cuenta con código fuente abierto y con licencia para su modificación.
- Permite un uso colectivo.
- Exposición al mundo entero a través de Internet.
- El presentador de la información tiene total control y autoridad de lo publicado.
- Es posible conocer e interactuar con muchas personas.
- Se permite realizar comentarios sobre la información.
- Elementos semánticos más concretos.

Desventajas:

- Uso de material que viola derechos de autor.
- Que se borre la información por parte de usuarios que no estén de acuerdo con el contenido.
- Uso abusivo y mala utilización de las herramientas.
- No existe supervisión de los contenidos.
- No son un medio profesional de información.
- Y se encuentra en construcción.

Al respecto, y con relación al Notariado, se tiene que señalar, que el notario es un profesional de derecho, dotado de capacitación especializada en la materia y con cuya intervención se logra la seguridad jurídica, a diferencia del notariado anglosajón, señalándose que sus diferencias son:

Notario Latino:

- Abogado/a o Licenciado/a en Derecho.
- Con procesos de designación, abiertos o cerrados según la regulación.
- Con ciertos impedimentos por lo que se garantiza su imparcialidad.
- Redacta el acto y ello lo hace auténtico, veraz y en algunos casos solemne.
- El documento se presume cierto.
- Existe colegiación obligatoria.
- El valor formal del acto jurídico se obtiene con la actuación Notarial.

Notario Sajón:

- No se requiere ninguna profesión
- No hay impedimento para desempeñar otras profesiones.
- La veracidad no se refiere al contenido del documento sino a las firmas, aunque el contrato sea privado.
- No hay presunción de certeza del documento, solo de las firmas.
- No existe colegiación.
- El valor formal se obtiene con la actuación judicial.

Con la evolución de las nuevas tecnologías deberíamos de analizar la pertinencia que las y los notarios deberán ser conocedor de las mismas, y más aún si estarían dispuestos a utilizar la inteligencia artificial e invertir en ella, o sea realizar las inversiones en tecnología, ya tenemos unos de esos usos, tales como uso de datos para la toma de decisiones, gestión de cobranza, herramientas para gestión de proyectos, facturación, control conocimiento de todo el proyecto y además considerando el costo que ello implica.

Sabemos de la existencia de Inteligencia Artificial capaz de interpretar casos y dar con la respuesta correcta acerca de cómo proceder, en asuntos legales, además es un reto, ya que las nuevas generaciones en especial la *millennials* exigen de los servicios notariales sea como ellos: globales, digitales, con avances de gobierno electrónico, dándole valor probatorio a las app, y todos los servicios con calidad, calidez, eficacia, eficiencia y sobre todo utilizando las grandes aportaciones que ofrece la tecnología. En conclusión, los nuevos servicios de certificación y registro podrán sustituir al notario anglosajón, pero sólo en parte a notario latino.

2019
La Red EDI

En crecimiento constante

EDI - La RedIBEROAMERICA

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

"E-WASTE" / "RESIDUOS ELÉCTRICOS Y ELECTRÓNICOS (RAEE)": EL LADO OSCURO DE LA TECNOLOGÍA

POR MA.EUGENIA LO GIUDICE

RAEE, qué son? qué costos medioambientales y sociales implican?, porqué urge la necesidad de legislación reguladora del tratamiento de los presupuesto mínimos de su gestión? Algunas de las muchas preguntas que generan este tema.

RAEE (ewaste o escrap) es acrónimo de Residuos de Aparatos Eléctricos o Electrónicos, riesgo generado por la sociedad actual. Se trata de desechos urbanos pero con un alto potencial de peligrosidad, según sea el tratamiento que se le aplicará a su disposición final.

Son el resultado mayormente de los productos ofrecidos por las Tics en una carrera consumista, que inunda los mercados, convocando el status del "ultimo confort" y en donde nativos digitales como inmigrantes digitales, reclaman insaciables aún más, introduciendo dos conceptos de "obsolescencia".

La denominada "obsolescencia percibida", que correspondería al consumismo anterior descripto y la "obsolescencia programada de los productos"[8]. En esta última la vida útil del producto es calculada por el fabricante o productor, desde el momento mismo que es diseñado, de tal forma que sea imperiosa su renovación o se lo deseche en un periodo de tiempo corto.

[8]Según la TV Española : "En 1911 se anunciaban bombillas con una duración certificada de 2500 horas pero en 1924 los principales fabricantes pactaron limitar su vida útil a 1000.

El cártel que firmó este pacto, llamado Phoebus, oficialmente nunca existió pero en 'Comprar, tirar, comprar' se nos muestran pruebas documentales del mismo como origen de la obsolescencia programada" http://www.rtve.es/television/documentales/comprar-tirar-comprar/ Recomiendo ver este documental para entender su idea.

Otra interesante premisa que apareja este tema, es la “economía circular”, moderándose el modelo de desarrollo económico sustentado en el consumo de materias primas, respondiendo a los conceptos de los Objetivos de Desarrollo Sustentable indicados por la ONU.

Encontrando su origen en los residuos domiciliarios universales, los RAEE dejan de ser amigables y se convierten al alcanzar su vida útil en peligrosos, de acuerdo al tratamiento que se les proporcione en su disposición final.

Se los define como chatarra o basura electrónica, residuos-e. En los países de habla hispana se promueve el uso del término RAEE como término oficial. La Unión Europea se refiere a ellos como WEEE (Waste Electrical and Electronic Equipment). Y la OCDE, 2001 (Organización para la Cooperación y el Desarrollo Económico) sugirió generalizarlos como “cualquier dispositivo que utilice un suministro de energía eléctrica, que haya alcanzado el fin de su vida útil”.

Según la Directiva sobre RAEE de la Unión Europea, 2002: “Todos los aparatos eléctricos o electrónicos que pasan a ser residuos …; este término comprende todos aquellos componentes, subconjuntos y consumibles que forman parte del producto en el momento en que se desecha”.

StEP (Solving the E-waste Problem)[9], 2005 se refieren a “la cadena en sentido inverso que colecta productos que ya son descartados por el consumidor que los da y repara para otros consumidores, para reciclarlos o procesarlos como otro tipo de basura.

Los RAEE se distinguen en tres líneas:

- Línea Blanca: frigoríficos, lavavajillas, lavadoras, hornos y cocinas.
- Línea Marrón: televisores, vídeos, equipos de música, etc.

[9]StEP (Solving the Ewaste Problem, iniciativa que nuclea a varios actores de las Naciones Unidas, gobiernos, sector privado e industrias bajo el objetivo de resolver este problema)

- Línea Gris: computadoras, periféricos y teléfonos celulares.(está es la linea generadora de la mayor parte

de los vertidos tecnológicos, sobre todo celulares por su prematura obsolescencia. Las baterías y plaquetas electrónicas de las laptops conforman los componentes con mayor potencial de contaminación).

A pesar de estos aspectos negativos expuestos, como contrapartida se destaca el concepto de "minería urbana". Nos referimos a la búsqueda de metales que se pueden recuperar desde los propios e-waste. Como ejemplo en un teléfono móvil se pueden encontrar hasta 46 tipos de metales. Metales de base (ejs.cobre, estaño, etc.), metales especiales (antinomio, cobalto, etc.) y metales preciosos (ejs. oro, plata, paladio, etc.).Y lo que los diferencia del cartón o del papel, reciclable de tres a ocho veces, es que los metales preciosos tienen un reaprovechamiento "infinito".

Cuál es la implicancia del riesgo generado por los RAEE? Por el año 2002 la "Basel Action Network"[10], ONG que trabaja para que no se exporten o envíen desechos peligrosos por parte de las naciones desarrolladas a naciones en desarrollo, presentó el "Exporting Harm", dejando al descubierto por primera vez, los envíos de basura tecnológica.

Realizó el estudio especialmente sobre Guiyu[11] (Guangdong, China) transformada en un gran basural, donde el 80% de los niños tenían altos niveles de plomo en sangre.

Replicándose ya luego otros informes, como los de la ONG "Greenpeace"[12], sobre e-waste en China y la India.

Actualmente cerca de 50 millones de toneladas de residuos electrónicos y eléctricos son desechados.

Los expertos del UNEP estiman que para 2020 el volumen de los residuos procedentes de ordenadores desechados habrá crecido un 500 por ciento en India con respecto a 2007; y

[10]Opera globalmente pero está radicada en Seattle, USA.

[11]Guiyu está formada por cuatro pequeñas aldeas, es conocida como el cementerio de desechos electrónicos más grande del planeta. Procedente principalmente de Estados Unidos, Canadá, Corea del Sur, Japón, de la propia China.

[12]Informe Recycling of electronic wastes in China and India. Workplace and enviromental contamination. Greenpeace Agosto 2005

en China y Sudáfrica, el 400 por ciento.[13]

Veamos sus efectos “negativos”.

En cuanto a la salud del ser humano su efecto negativo es directo. Pudiendo traducirse desde erupciones cutáneas, malestar de estómago, úlceras, problemas respiratorios, debilitamiento del sistema inmune, daño en los riñones e hígado hasta diversos cánceres, etc..

Mientras que su incidencia en el medioambiente es asimismo severa, al producirse el “percolados y/o lixiviados” [14]en la tierra o liberados a la atmósfera en procesos de mala incineración, liberandose furanos y dioxinas.

Asimismo existe un impacto sobre la minería por la demanda de minerales para la fabricación de diferentes aparatos tecnológicos. La fabricación de celulares y computadoras según la UNEP[15], consume el 3% del oro y plata extraída en el mundo, 13% del paladium y 15% del cobalto.

La escasez de minerales usados para la producción de los aparatos de la nueva tecnología , llevará a situaciones de extrema violencia social y un ejemplo de esto es lo que ocurre con el “coltán”[16], disparador de las guerras tribales que se desataron 1998. La “guerra del coltán o el oro gris”, ha provocado la muerte de 5,5 millones de personas (mayor cantidad de victimas fatales desde la segunda guerra mundial), donde el Congo con su 80% de reservas mundiales del mineral está

[13]De acuerdo al Boletin electronico del PNUMA – “La ONU insta a tomar medidas ahora contra la basura electrónica”, 22 – 02 – 10

[14]Según el CEAMSE de Argentina (Cinturón Ecológico Area Metropolitana Sociedad del Estado) llama lixiviado o percolado a los líquidos que se generan en el módulo de un relleno sanitario a raíz de la degradación de la materia orgánica y como producto de la infiltración del agua de lluvia que al atravesar o “percolar”, la masa de desechos, disuelve, extrae y transporta o “lixivia” los distintos componentes sólidos, líquidos o gaseosos presentes en los residuos dispuestos. El líquido lixiviado es sometido a un tratamiento que incluye dos etapas, un proceso físico-químico y otro biológico. El tratamiento ejecutado, es necesario para poder volcarlo a los cursos de agua cumpliendo con la normativa legal vigente.

[15]“Reccycling –from E=Waste to Resources”

[16]Mineral no renovable y escaso en las reservas natuales que sirve para la miniaturización caractarísticas de los dispositivos de los dispositivos electrónicos actuales., usados en plasma,celulares, dvd, industria aeroespacial, computadores, etc.

siendo oprimido por Ruanda y Uganda.[17]

Desde el punto de vista legal, cuáles serian los ámbitos de responsabilidad de los RAEE?

La atribución de responsabilidades de los RAEE se relacionan con "los principios generales de Derecho Ambiental, como el Desarrollo sustentable, el Principio preventivo, el Principio precautorio, quien "contamina paga", entre otros.

Pero asimismo existen principios propios aplicables a la gestión de RAEE, como por ejemplo:

Reducción en la fuente, Proximidad, Consideración del ciclo vital integrado. Extensión de la responsabilidad al ciclo de vida de todo el producto. Responsabilidad extendida del productor.

Los tipos de responsabilidad que competen al "productor" abarcan desde "Liability", Responsabilidad económica y física, Responsabilidad de información y de manejo de datos personales.

No podemos dejar de mencionar el concepto REP[18], en un marco de responsabilidades compartidas y con una visión "amplia". Asumido por las empresas, debe ser incentivado por los gobiernos, centrando la atención más allá del ciclo de vida útil del aparato y su destino final.

Este principio "REP" surgió como una propuesta de estrategia política, combinado con el principio de "Responsabilidad Individual del Productor", RIP.

Promueve el mejoramiento total del ciclo de vida de los aparatos eléctricos y electrónicos, por medio de la extensión de las responsabilidades del productor considerando como novedad, el ecodiseño.

La REP (Responsabilidad Extendida del Productor) se puede cumplir a través de sistemas individuales o colectivos, RIP (Responsabilidad Individual del Productor) o RCP (Responsabilidad Colectiva de Productores).

Entorno a los Sistemas Colectivos de Responsabilidad, se agrupan organizaciones, ORP, que son asociaciones basadas en el apoyo y compromiso de los fabricantes de aparatos electrónicos. Manejan parte o sistema completo de e-waste en sus países. Un ejemplo es la "Asociación Europea de Sistemas de Recolección para Residuos de Aparatos Eléctricos y Electrónicos", como plataforma, sin ánimo de lucro que nuclea 39 sistemas colectivos de e-waste en Europa.

No sé puede desconocer que un rol fundamental lo cumplen los consumidores. Por eso la importancia de políticas públicas de

[17]Encuentrese en los Anexos el articulo sobre las "Guerras tribales por el coltan, el lado oscuro de la tecnología"

[18]Presentado por primera vez en Suecia,1990, en un informe para el Ministerio de Medioambiente denominado "Modelos para la Responsabilidad extendida del Productor"

concientización dirigidos a ellos, que les hace presente, las conocidas “ 3Rs”, idea que nació en Japón como un esquema para aplicarse a la gestión de los residuos en general: Reduzca, Reúse, Recicle y que hoy se le suma: Reparar, Regular.

Con el reciclado de los residuos electrónicos logramos dos resultados positivos, evitamos la degradación en rellenos sanitarios o basurales que al lixiviar pueden contaminar suelos y napas. Y recuperamos materiales y metales que son cada vez más escasos, cuya necesidad de obtención a través de la minería, genera fuertes impactos negativos en el medioambiente.

Estado Legislativo de la Región

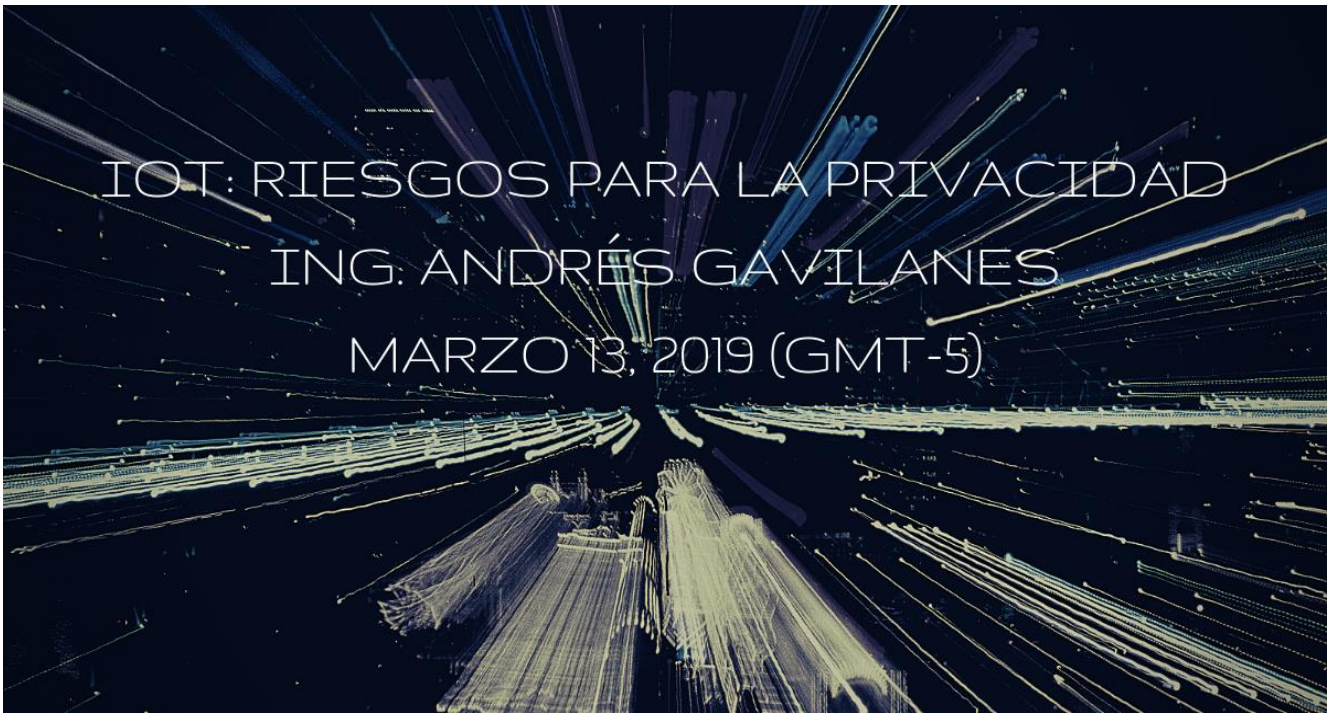
En términos generales se toma como modelo la Convención de Basilea y otras directivas europeas a nivel internacional.

Si no se cuenta con leyes sobre RAEE, son las leyes generales de medioambiente de cada país con las cuales se está tratando, pero es un imperativo la legislación especifica de acuerdo a lo expuesto.

Actualmente los países latinoamericanos que cuentan con legislación especifica son: Brasil, Chile, Colombia, Costa Rica, Ecuador, México y Perú. Argentina presentó su primer proyecto en el 2004 pero lamentablemente a hoy no ha sancionado ningún proyecto.

Conclusión

Analizado los efectos sobre el medioambiente, salud humana tanto como los impactos económicos y sociales, urge especial tratamiento de responsabilidad competente a los RAEE. Los Estados deben generar políticas públicas sobre concientización y sancionar legislación especifica sobre los presupuestos mínimos para la gestión de los mismos.



El futuro aguarda cambios sustanciales debido al internet de las cosas, más conocido por sus siglas en inglés como IoT (*Internet of Things, IoT*). IoT permitirá identificar comportamientos y estandarizará preferencias en el mundo que actualmente posee o carece de una conexión a internet, lo cual implica evaluar el impacto social de estas nuevas tecnologías emergentes, métodos y técnicas históricas al igual que actuales con el objetivo preservar la privacidad de datos personales.

La posibilidad de un mundo sin conexión a internet se mantiene en disminución, continuamente es menos probable. Cada día que pasa, se reducen espacios privados, cámaras y sensores aumentan constantemente, en consecuencia, encontrar soledad o espacios reservados es complicado. Es decir, IoT facilitará la identificación de personas, ya sea en espacios públicos o privados.

IoT, podría invadir hasta la privacidad emocional y corporal, dado que la proximidad de sensores posibilitaría a terceros recolectar estados emocionales a corto, mediano y largo plazo. Emociones y

Más que un blog.
Toda la actualidad jurídica.

información jurídica ágil, eficiente y relevante

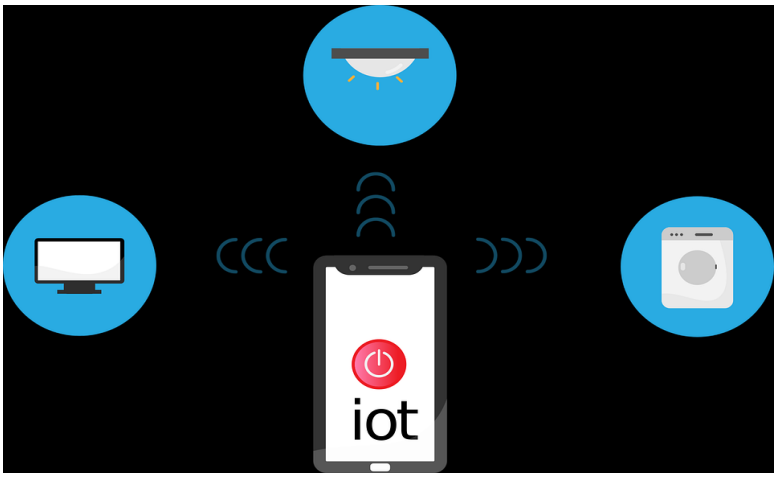
aldiaargentina.microjuris.com

Llámenos (5411) 5031-9300

microjuris.com
inteligencia jurídica

más transparentes y accesibles para organizaciones interesadas en recoger, analizar y explotar dichos datos personales.

Hoy en día, existen personas que exponen su vida personal vía redes sociales o blogs, incrementando la probabilidad de una recolección de datos omnipresente en el entorno humano. En otras palabras, mientras más aumenta la expectativa de las personas a ser observadas o



reconocidas en la web, disminuye la noción de invasión de su privacidad.

Los dispositivos IoT tienen un diseño amigable poco intrusivo, por ende estas

“cosas” se van tornando más familiares, provocando que con serenidad y consentimiento se revele información íntima. La mayoría de la gente podría olvidar la presencia de IoT o confiar plenamente en ellos, por consiguiente admitir a ser constante e impertinentemente monitoreados en sus ambientes personales y laborales, lo cual no hubiésemos aceptado en otros tiempos, medios o circunstancias.

IoT desafía lo convencional, así como la habilidad de las personas para afrontar dicho reto tecnológico.

Los hogares se volverían transparentes para los fabricantes de dispositivos inteligentes. Además, sí las políticas gubernamentales desconocen o evitan enfrentar el tema, tendríamos como resultado que los límites de protección de datos personales establecidos por marcos jurídicos, que se encuentra actualmente en socialización y debate, sean confusos o poco prácticos.

El mercado manipula el entendimiento de la población respecto a estos temas para evitar declinaciones o rechazos de condiciones o políticas de privacidad de sus productos o servicios.

Productos con características similares a IoT son comercializados como características inteligentes, poco se informa al consumidor sobre

la recolección de datos y comportamientos personales. Sociedades modernas se preocupan más por usabilidad que por seguridad de dispositivos digitales y electrónicos. IoT aumenta la vigilancia de la sociedad, reduciendo el control del propietario de sus datos, exponiendo a manipulaciones por parte de entes internacionales, razón por la cual será difícil lograr una consciencia plena en las personas.

Los principios de transparencia podrían ser mancillados por el internet de las cosas, IoT amenaza destruir los Derechos de Participación reconocidos en Principios de Prácticas Justas para Información de Estados Unidos (US Fair Information Practice Principles) y el Reglamento General de Protección de Datos de la Unión Europea (EU General Data Protection Regulation). Cabe mencionar que, los dispositivos IoT son imparciales, en otros términos, fueron concebidos netamente con fines comerciales; internet de las cosas engloba y promueve lógicas empleadas en las redes sociales, inversiones basadas en las interacciones de personas que utilizan internet y divulgación intencional de datos íntimos y reservados.

Sin embargo, excluir, eliminar o negar el uso o acceso a las nuevas tecnologías de la información y comunicación (NTIC) dista de ser una solución razonable, viable y realista; considerando que, coartaría el goce de las ventajas, así como los beneficios de las NTIC. En tal virtud, una solución factible es, desde la fase de diseño, desarrollo hasta la operación y eliminación, respetar la privacidad y protección de datos en todo el ciclo de vida de la tecnología. Esta idea es conocida como

privacidad desde el diseño (PdD). La PdD supone un conjunto de acciones que dependen de contextos concretos. Verbigracia, no se debería comerciar o utilizar comportamientos de conducción para crear diferentes tipos de seguros médicos o vehiculares o planear de algún otro modo

actividades acaecederas con fines lucrativos, pero se lo hace. PdD puede obligar a eliminar o reducir datos personales para evitar manipulaciones innecesarias, excesivas, abusivas o no deseadas. Por lo tanto, PdD puede ofrecer herramientas para que los propietarios de sus datos tengan el control idóneo sobre sus propios datos personales; aunque suene redundante, es crucial que se tomen en cuenta estos principios al elaborar estándares, buenas prácticas, arquitecturas de sistemas de información y comunicación y estructuras organizacionales de entes que gestionan datos personales. Los marcos jurídicos actuales deberían incorporar explícitamente el requisito de PdD, y no de manera indirecta o muy genérica, a fin de evitar el tratamiento ilícito de los datos.

“La civilización moderna es naturalista, mecanicista, su ritmo es el ritmo de máquinas, cada una de las cuales es una criatura de inteligencia para resolver problemas. Es un equilibrio inestable de fuerzas, cuyos patrones cambiantes requieren que la humanidad tenga cada vez más conocimiento y cálculo” (Everett Dean Martin, 1928)

El debate sobre la privacidad trasciende desde tiempos pasados fruto de avances técnicos. No obstante, en vista de la rapidez de los cambios tecnológicos contemporáneos que nos rodean es más imprescindible que nunca garantizar la profundidad, diversidad y calidad de los discursos, al igual que la literatura, sobre privacidad e intimidad de los datos.

Cabe mencionar que, lo largo del tiempo, IoT ha tenido muchos nombres. Por ejemplo, computación generalizada, inteligencia ambiental, comunicaciones máquina a máquina, computación ubicua, sistemas ciberfísicos, entre otros. Dichos términos nacen de varias realidades, contextos o disciplinas, a pesar de ello todos tienen el misma orientación, lo cual significa que existen continuos intentos para hallar un término pertinente y común que defina el fenómeno en mención.

Adicionalmente, se evidencia una cierta conciencia de las personas en el sentido de una rápida transformación hacia un mundo completamente monitoreado y conectado, por este motivo, IoT probablemente tendrá un impacto profundo. Como resultado, es importante prever las posibles acontecimientos. El mundo físico y digital evoluciona diariamente, tal como la noción de privacidad. Las posibles ramificaciones de los avances de la Internet de las cosas son motivo de profunda preocupación para muchas personas Estos nuevos retos deben ser encarados, caso contrario, IoT podrá afectar principalmente a la niñez, en consecuencia a sus padres, ergo a la familia, las responsabilidades en cuanto a proteger su intimidad y privacidad serán cada vez mayores.

A medida que el internet de las cosas sea más y más común, se podría prever que la niñez vivirá en un mundo monitoreado ubicuamente por entes con fines de lucro e instituciones gubernamentales, con total normalidad y permisividad.

Instituto Argentino de Derecho Procesal Informático

Donde la Informática y el proceso judicial se encuentran.

Visitanos en www.iadpi.com.ar

Resumen

Este artículo analiza los nuevos ciberdelitos incorporados al Código Penal peruano, nuevos delitos que también se cometen por medios electrónicos, para ello se define cada tipo penal. Posteriormente se reconoce sus elementos según la teoría del delito y finalmente se resalta la necesidad de considerarlos como un tipo de Violencia de género.

Palabras Clave

Ciberbullyng, Sexting Gromming, Sextorsión, delitos cibernéticos, violencia cibernética

1. Nuevos delitos informáticos en el Código Penal peruano

El Decreto Legislativo 1410 (1) promulgado el 11 de setiembre del 2018 incorpora al Código Penal peruano al Ciberbullyng o Ciberacoso (acoso), el Sexting, el Gromming (acoso sexual) y la Sextorsión (Chantaje Sexual), realizados a través de medios electrónicos, redes sociales u otra tecnología de información y comunicación. *Ver fig 1.*

Si bien estos delitos existían en la doctrina extranjera, el constante uso de la costumbre como fuente de Derecho obligó a que se positivice, colocando al Perú dentro de los países que sancionan estos nuevos delitos.

Surge la duda si esta ley forma parte del Derecho informático, ya que el término Delito Informático no aparece en ningún contexto de la norma, por lo que es recomendable ante este vacío utilizar el término de “Delitos cibernéticos” ya que tiene una similitud a la ley española LO 1/ 2004.

Aunque la denominación es secundario, lo primordial es que los legisladores tomen conciencia de adecuar normas que se adapten a nuestra sociedad de la Información y el conocimiento.

Fig. 1 NUEVOS DELITOS INFORMATICOS INCORPORADOS AL CODIGO PENAL POR EL DL 1410

Artículo Código Penal	Delito Informático	Acción	Finalidad	Medio empleado	Pena
151-A Acoso	Ciberacoso ó Ciberbullyng	De forma reiterada o no, continua, habitual vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona sin su consentimiento.	Alterar el normal desarrollo de su vida cotidiana de la víctima	Cualquier tecnología de la información o de la comunicación	1 -4 años e inhabi-litación.
				Agravante:	4 -7 años e inhabi-litación.
154-B Difusión de contenido sexual	SEXTING	Sin autorización difunde revela, publica, cede o comercializa materiales de contenido sexual de cualquier persona obtenida con consentimiento	Generar una difusión masiva del material	Imágenes, materiales audiovisuales o audios.	2 -5 años 30- 120 días multa.
				Agravante: Pareja o ex Uso de Redes Sociales.	3 -5 años 180 -360 días multa.
176-B Acoso Sexual	Grooming	Vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona, sin el consentimiento de esta.	Llevar a cabo actos de connotación sexual	Tecnologías de información o comunicación-	3 -5 años e inhabi-litación.
				Agravante:	4 -8 años e inhabi-litación.
176-C Chantaje Sexual	Sextorsión	Amenaza o intimida a cualquier persona	Obtener de ella una conducta o acto de connotación sexual.	Tecnologías de información o comunicación.	2 -4 años e inhabi-litación
				Agravante: Imágenes, materiales audiovisuales o audios que aparezca o participe la víctima.	3 -5 años e inhabi-litacion

2. La Violencia Cibernética

Estos delitos cibernéticos constituyen juntos un tipo de violencia de género no contemplado aún en la ley N°30364 (2) que podemos denominar VIOLENCIA CIBERNETICA, porque a través de medios electrónicos, redes sociales, se afecta exponiendo la intimidad de las mujeres y una forma de control sobre ellas, en cualquier etapa de su vida pudiendo derivar en el delito de feminicidio. (3)

4. El Ciber Acoso Cibernetico, Ciberacoso O Ciberbullyng

El acoso cibernético para el autor, es una modalidad de acoso, este no requiere que el fin sea sexual, aunque el acosador (sujeto activo) sea un mayor de edad sobre el acosado (sujeto pasivo), ni que si es un varón sobre una mujer, la condición es que el hostigamiento (acción) se realice a través de medios electrónicos (medio empleado) como internet, teléfonos móviles, redes sociales, más de una vez y cuyo daño (modalidad) que se cause sobre la víctima pueda llegar a perturbar su proyecto de vida, es conocido también como Ciberbullyng.

Cabe resaltar que a diferencia del acoso físico o bullyng que suele ser

El Derecho informático se interrelaciona así con otras disciplinas jurídicas,

Fig. 2 El Derecho informático se interrelaciona con otras disciplinas

muy común en los colegios por ejemplo, el daño se detiene cuando acaban las clases y se retiran a su hogar, sin embargo en el caso del ciberbullyng el menor se encuentra las 24 horas del día los 7 días de la semana expuesto a dichos actos hostiles porque en el ciberespacio no existe horario.

También puede darse el caso por ejemplo que estas dos figuras confluyan el ciberbullyng y el bullyng en un mismo escenario por ejemplo el salón de clases, por ello es necesario que las escuelas prohíban el uso de teléfonos móviles a los alumnos como parte de las políticas educativas a fin de proveer el mayor aprovechamiento de las clases y por salud mental.

El acoso cibernético para Kowalski y Agatston (4) es “entendido en un sen-

tido amplio, se refiere al acoso que incluye el uso de correos electrónicos, mensajes instantáneos, mensajes de texto e imágenes digitales enviadas a través de teléfonos móviles, páginas web, bitácoras web (blogs), salas de chat o coloquios online, y demás tecnologías asociadas a la comunicación digital"

En el artículo 151-A del Código Penal, el acosador vigila, persigue, hostiga, asedia o busca estar cerca a una persona de forma reiterada o no, utilizando las TIC (Tecnologías de Información y Comunicación).

El agravante de este delito se da por la condición del sujeto pasivo, aumentando a siete años de pena privativa de libertad, inhabilitación y multa, cuando: 1. La víctima es menor de edad, persona adulta mayor, en gestación o discapacitada. 2. La víctima y el agente tienen o han tenido una relación de pareja, convivientes o cónyuges, parientes. 3. La víctima y el agente habitan en el mismo domicilio, 4. La víctima es dependiente. 5. Hay relación laboral, educativa o formativa de la víctima

5. Difusión de imágenes, materiales audiovisuales o audios con contenido sexual.

Aunque el Sexting no es delito, es una práctica común entre jóvenes, también conocido como "sexo virtual", Este término inglés nace de la conjunción de dos palabras SEX y TEXTING, y consiste en compartir material erótico, sexual o pornográfico, video, conversaciones, fotografías, teléfono móvil, Whatsapp, sky,.

El Artículo 154-B del Código Penal sanciona con pena de cárcel de hasta 5 años al sujeto que trasmite sin autorización a terceros material de contenido sexual adquirido con anuencia, "consentimiento o acción de consentir" (5)

En lo que se refiere a la anuencia o consentimiento, que sucedería en el caso de que no se contara con la autorización, supongamos Juan necesita revisar su correo y solicita a su vecina que le preste su computadora, el aprovecha y se apodera de un video intima de ella sin su consentimiento y lo comercializa, se estaría incurriendo en otro delito como en el de violación de la intimidad personal o familiar.

En Corea del Sur país de gran adelanto tecnológico, este material se obtiene sin permiso de lugares públicas, que obligada a las mujeres coreanas, buscar en los baños que no se haya colocado una cámara y al gobierno ha iniciar una campaña disuasiva advirtiendo que las penas llegan hasta 5 años.

La agravante de este delito, no es por la falta de consentimiento por la víctima sino por el tipo de relación que tiene o haya tenido el acosador y el acosado una relación o la tienen o si son convivientes o esposos, y 2. Que sea difundido a través de un medio masivo como son las redes sociales, no se especifica si la conducta o acción es reiterativa, puesto que basta una sola publicación, para que pueda visto por miles de personas en un minuto. En el caso que la persona sin vínculo con el acosador sexual, se hace más permisible y menos sancionable este ilícito por no configurar como agravante.

6. El Acoso Sexual Cibernético o Grooming

El acoso sexual cibernético, es entendido como una modalidad del acoso sexual que se realiza utilizando (modo) cualquier tipo de Tecnología de Información y Comunicación transmitido (medio) a través de medios electrónicos.

Aunque el artículo 176-B segundo párrafo del Código Penal, no especifica que sea realizado a través de medios electrónicos es de suponer que estas tecnologías incluyen también a las redes sociales, entre otras.

Las agravantes del delito son además del artículo 151-A cuando

"6. La víctima tiene entre catorce y menos de dieciocho años."

7. La Sextorsión o Chantaje sexual Cibernético

El artículo 176-C del Código Penal sanciona a quien amenaza o intimida a una persona a través de las TIC (Tecnologías de la información y comunicación) a fin de obtener una conducta o acto de connotación sexual, penándose hasta con cuatro años de pena privativa de la libertad e inhabilitación.

Asimismo se agrava este delito cuando se amenaza con la difusión de dichas imágenes, videos y audios de contenido sexual protagonizados por la víctima.

Y aquí surge una observación que sucedería si por ejemplo el chantaje no

se da con fines sexuales sino por dinero. ¿Estamos frente a otra figura como la simple extorsión? Con ello podemos observar que el Chantaje sexual cibernético se configura por el contenido sexual del material, por el fin sexual con el que se chantajea, y por el medio de difusión masivo al que sería sometido tal información de imágenes, videos o audios.

Conclusión

1. La violencia digital debe ser considerada como una nueva forma de violencia contra la mujer.
2. Debe precisarse a fin de no caer en contradicciones doctrinaria la definición de cada tipo de delito.
3. Puede causar una impunidad el que se no especifique el tipo de medio empleado, porque para ser considerado un delito informático debe cumplir con los elementos de la teoría del Delito.
4. En algunos países aún no han concientizado la importancia de estos delitos en Latinoamérica razón por la cual debemos innovar en nuestra legislación.
5. Se requiere de implementación de normas sociales de prevención en escuelas, institutos, universidades a fin de que se evite el uso y abuso de estos medios electrónicos.

Referencia Bibliográfica

[1]Decreto Legislativo que incorpora el delito de acoso, acoso sexual, chantaje sexual y difusión de imágenes, materiales audiovisuales o audios con contenido sexual al código penal, y modifica el procedimiento de sanción del hostigamiento sexual

[2] Ley Nº 30364 Ley para prevenir, sancionar y erradicar la violencia contra las mujeres y los integrantes del grupo familiar

[3] Tristán, F. (2005) Feminicidio La violencia contra la mujer: Feminicidio en el Perú. Ymagino Publicidad S.A.C

[4] Kowalski, Robin, and Patricia Agatston. Cyber Bullying: el acoso escolar en la era digital, Editorial Desclée de Brouwer, 2009. Pag. 80.

[5]Diccionario de la lengua española. Edición del Tricentenario. Actualización 2018, accesado en https://dle.rae.es.

SOMOS EDI LA RED

EL CENTRO DE INFORMACIÓN

y contenidos
más grande iberoamerica

TWITTER: ELDERECHOINF

Somos

LA RED

AÑOS

junto a Uds

ELDERECHOINFORMATICO.COM

EL CENTRO DE FORMACIÓN E INFORMACIÓN MÁS GRANDE DE IBEROAMERICA