EDI

Revista Digital -Diciembre 2020

En esta edición

LOS DESTACADOS EDI DEL AÑO

2021

Edición nº 37 - ElDerechoInformatico.com

hammurabi digital

LANZAMIENTO

EL DERECHO INFORMÁTICO

GUILLERMO M. ZAMORA DIRECCIÓN

DERECHO INFORMÁTICO APLICADO.
DELITOS INFORMÁTICOS. PRUEBA DIGITAL.
ANÁLISIS JURISPRUDENCIAL

AUTORES

AGUIRRE - ARÁOZ FLEMING - ARCE
BRANCIFORTE - CASARES SUBÍA - DESCALZO
FRANK - IUALE - KOHEN - LOFEUDO - PARDINI
PEÑALOZA - PÉREZ CARRETTA
SALGADO MONTERROSA - SAUL - SUKENIK

DISPONIBLE EBOOK y LIBRO

hammurabi digital

Tu biblioteca legal, siempre disponible

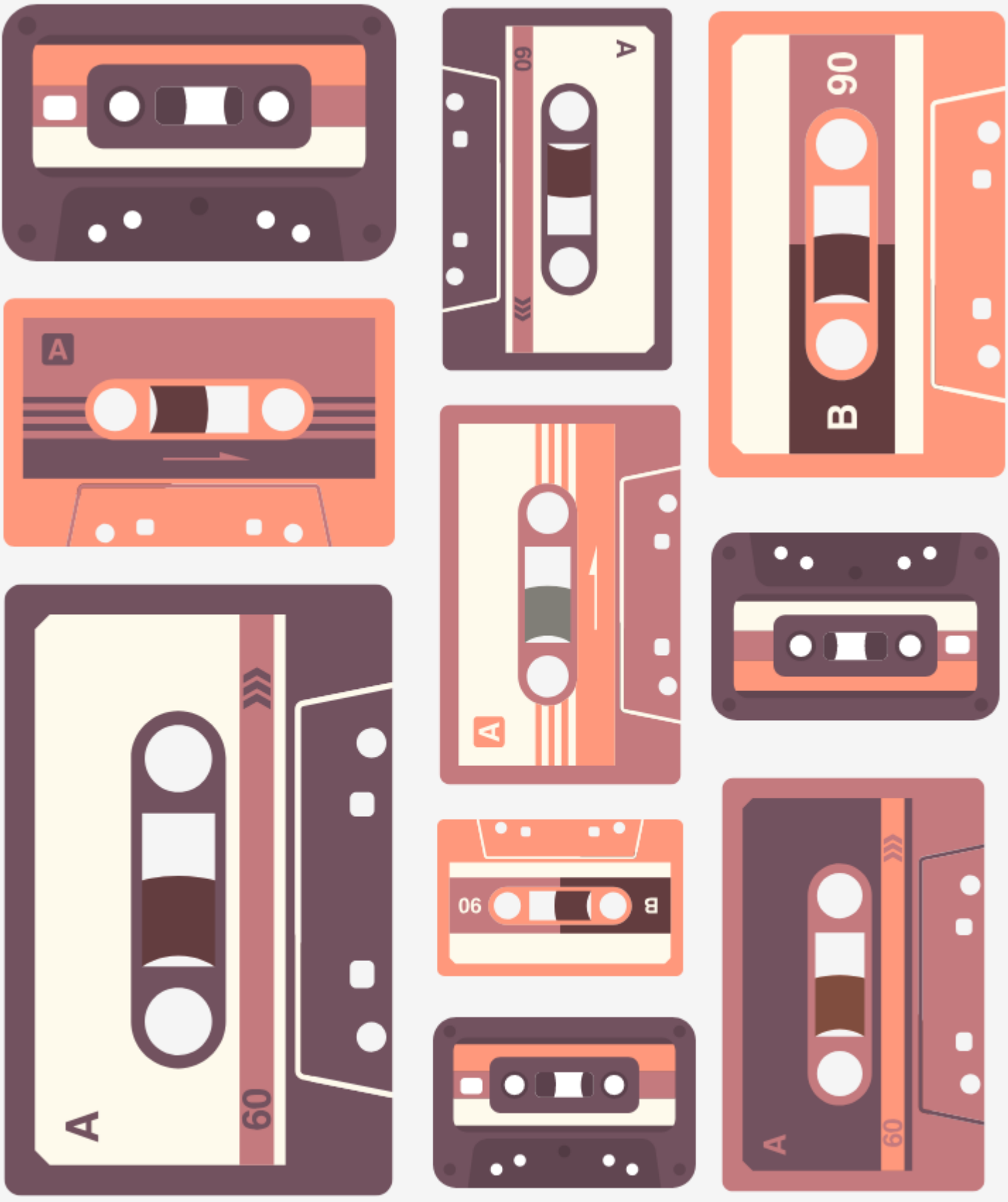
- Comprá ebooks y leelos las veces que quieras
- Desde cualquier dispositivo, a tu medida
- Planes de suscripción

www.hammurabidigital.com.ar

LOS DESTACADOS EDI

ÍNDICE

ELDERECHOINFORMATICO



LA RED EDI

INFORMACIÓN QUE SUENA BIEN

WWW.ELDERECHOINFORMATICO.COM

EDITORIAL

Estas ediciones son raras, la primera del año pero la última del que se fue, un momento de reflexionar, y de proyectar, contarles que pasó y que buscamos que pase... no se, como mínimo son raras.

No voy a contarle a nadie lo que fue el 2020, solo decirles que a pesar del mismo, no nos quedamos, seguimos haciendo y generando, buscando y encontrando, lleno de carencias y carente de plenitudes, fue un año contradictorio, pero sin discusiones, (casi), como sea, como haya sido, lo importante siempre es no quedarse, avanzar, crecer, reflexionar, y mirar el camino que queremos tomar, podría contarles de las campañas, los congresos, los libros, las revistas, las acciones que tendrán nuestra marca, pero no se si sirve de algo, hoy es hoy, con toda la obviedad de la afirmación, forjemos desde ahora el año que tenemos por delante, seamos generosos, comprometidos, sencillos, el resto viene solo.

En esta edición encontrarán LOS DESTACADOS DEL AÑO, sabemos que hay muchos más, sabemos que quizás haya algunos que también merecieran estar, pero recuerden, éste no es más que un juego donde buscamos dar el mimo que haga bien a alguien, quizás el año que viene le toque a alguno de los que leen estas líneas, dependerá siempre de Uds, como el creer firmemente en que tenemos todo un año por delante para hacer cosas, ser generosos, humildes, y sencillos, -

Feliz año

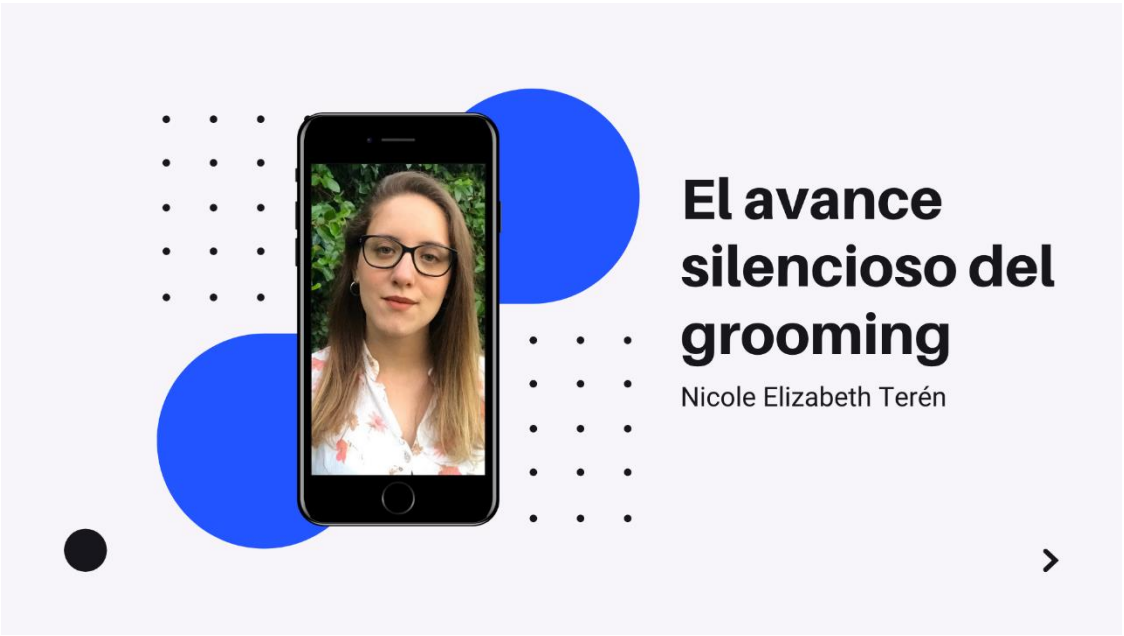
Guillermo M Zamora

La Red EDI

En crecimiento constante

EDI - La RedIBEROAMERICA

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



Como ya sabemos, el corriente año ha salido de todo parámetro de normalidad por la ya conocida pandemia causada por el COVID-19 que afectó a un nivel macro y mundial, en diferentes áreas, alterando la vida de muchas personas. Un aspecto que tuvo primordial relevancia fue el hecho de la búsqueda de una alternativa al relacionamiento personal diario, a la rutina que nos marcaba día a día, sea en el ámbito laboral, social o educativo. Por ello, la hiper conectividad se convirtió en un aspecto muy importante de nuestras vidas. La internet nos brinda innumerables beneficios, la tecnología en general nos trae soluciones que hace muchos años no existían, pero a la vez encontramos ciertos perjuicios que ocasiona esta red informática con la cual, a veces, debemos tener cuidado.

Una problemática que aumentó drásticamente durante esta pandemia, debido a la conectividad constante que marcó nuestra manera de comunicarnos y desenvolver nuestras actividades diarias, fue el delito de grooming. Los niños, niñas y adolescentes que tienen acceso a una computadora y a una conexión a Internet, debieron usar este medio para reemplazar las clases presenciales y que la enseñanza, tanto primaria como secundaria, pudiera llevarse a cabo a través de la pantalla, a pesar de la cuarentena y por el hecho de tener que permanecer en sus casas. En este marco comenzó a intensificarse (como venía ya sucediendo hace tiempo) el hecho de que personas adultas empleando un perfil falso o usando su propia identidad, llamados “groomers” aprovecharan esta circunstancia para contactarse con menores de edad para lograr el cometido de acosar o abusar sexualmente de ese menor.

Aquí surgió otra pandemia, aquella en la que la cuarentena se convirtió en el escenario ideal para que los groomers y que los casos de

grooming crecieran exponencialmente dejando víctimas de este delito a veces sin ningún resguardo.

Los niños, niñas y adolescentes pasan mucho tiempo en las redes sociales o plataformas de juegos y es allí donde se encuentran en peligro de caer en las manos de estas personas que se hacen pasar por alguien de su misma edad, o manifiestan verdaderamente quiénes son o, asimismo, puede haber casos en que el groomer puede ser una persona que los chicos conocen; de esta forma tratan de ganarse la confianza de los menores, manipulándolos y llegando a amenazas.

Esta problemática se acentúa aún más por el hecho de que muchas personas desconocen, tanto menores como adultos, sobre la existencia del grooming y que en muchos casos tienen la posibilidad de denunciar. Pero además es sumamente necesaria la educación sobre este tema que comienza en los hogares, en cada familia, en las escuelas, es primordial fomentar programas de enseñanza en áreas de la informática como así también en educación sexual. Los niños, niñas y adolescentes tienen derecho a que no exista ninguna injerencia indebida a su sexualidad o privacidad que pueda afectarlos trayendo consigo daños a veces irreparables, ya que el contacto del adulto con el menor por medio de una red social puede terminar en un encuentro personal llevando a consecuencias trágicas.

Si bien este hecho lamentable tiene cada vez más llegada a la gente a través de organizaciones no gubernamentales, educación en las escuelas o programas impulsados por los gobiernos, no debemos dejar de lado que la falta de conocimiento sobre este problema sigue latente, que muchos niños o niñas no saben cómo proceder ante una situación así que configura el grooming o se sienten solos y que sus padres a veces tampoco saben exactamente qué hacer o cómo actuar. Por lo tanto, es mucho el trabajo que queda por delante, existen muchos adultos que contactan no solo a un menor, sino que tienen muchas víctimas a las cuales acosar o abusar sexualmente.

Es evidente que en algunos países, como es el caso de Argentina, el derecho en relación con la ciencia informática necesita actualizarse, hay conceptos que no se encuentran regulados y con respecto a delitos como el grooming es indispensable que los legisladores y la sociedad en general conozca sobre ciertas materias que afectan, en este caso particular, a niños, niñas y adolescentes, que se encuentran en el camino de formación, por ello la educación es la clave en este asunto.

Se dice que el desconocimiento constituye una especie de complicidad ya que si los gobiernos no impulsan soluciones que apunten a revertir esta situación será muy difícil que la sociedad pueda en su conjunto, conocer cómo evitar que

siga avanzando este problema creciente que es el grooming.

Internet, como lo mencioné al principio, posee su lado bueno, con beneficios que pueden aprovecharse positivamente, pero a la vez cuenta con peligros que ponen en riesgo a muchas personas por el uso indebido e ilegal de ciertos sujetos. Por ello el derecho informático es clave en el camino a encontrar el remedio a estos problemas.

Asimismo creo que las escuelas deben seguir el ritmo de los tiempos modernos, implementando nuevas metodologías de enseñanza, amoldándose a las necesidades de los niños, niñas y adolescente de un mundo en donde la tecnología nos atraviesa y forma parte de nuestras vidas; por lo tanto se deberían actualizar los programas de educación formando en materias que actualmente no están presentes y que podrían ayudar a los niños a conocer sobre derecho, informática, sexualidad que son temas que se relacionan con un problema tan preocupante como lo es el grooming o el ciberacoso.

2020

ELLOS SON EDI

EDI











Hoy día la gran mayoría de los habitantes de este planeta lo primero que hacían al despertar en las mañanas era encender un cigarrillo o

Estamos en el tiempo de la tecnología, es su espacio. La tecnología es una de las expresiones de la actividad del ser humano

ir corriendo al baño. Hoy, estos hábitos cambiaron. Lo inmediato al cobrar conciencia es voltear al celular, revisarlo, y ver si su vida o el mundo ha cambiado gracias a estar “conectado”. La vida sin teléfono celular o red social es no vivir o vivir a medias. Lo pensamos sin decirlo.

El uso de la tecnología pasa imperceptible en nuestros sentidos, sin percatarnos que incorporamos en el Internet parte de nuestra vida, rasgos de nosotros mismos. Lo hacemos crecer aportando información para que crezca ese mundo virtual. Nosotros alimentamos al Internet sin saber que lo sabemos. Hablar, interactuar, enamorarse u odiar, vestirse, transportarse y pensar, ya no es monopolio de nosotros, lo compartimos con la tecnología.

referida a la producción de métodos o artefactos. Corresponde a la dimensión de la actividad humana que los griegos llamaban "póiesis", que podemos traducir como “hacer” y que se refiere a producir. Como tal, forma parte de la cultura. Proviene de la aplicación de la razón a determinados medios, en vistas a conseguir de manera eficaz algo útil. Como tal, está subordinada a las dimensiones más esenciales de la actividad humana, en la búsqueda de la verdad y del bien.

La incorporación de estos nuevos medios a la vida económica y social supone una serie de ventajas, como, por ejemplo, mayor eficiencia empresarial, aumento de elección de usuarios, así como nuevas fuentes de ingresos. Sin embargo, también se crean incertidumbres en el mundo

jurídico, por desconocimiento mismo de manejo del propio fenómeno. Uno de estos aspectos es el uso que le damos los usuarios a nuestros datos personales, referencias de nuestra propia vida al mundo digital y que determinarán como la tecnología nos va a influir al recibir "instrucciones adhoc" conforme a nuestro perfil de vida.

La tecnología en la época contemporánea ha adquirido dimensiones que plantean nuevos campos de conocimiento. Por lo que se refiere a la tecnología podríamos afirmar que lato sensu es un producto o solución conformado por un conjunto de instrumentos, métodos y técnicas diseñados para resolver un problema. Generalmente, se asocia la tecnología con el saber científico y la ingeniería; sin embargo, tecnología es toda noción que pueda facilitar la vida en sociedad, o que permita satisfacer demandas o necesidades individuales o colectivas, ajustadas a los requerimientos de una época específica; cabe considerar lo expresado por el científico irlandés John de Bernal, al hacer referencia a los primeros utensilios y herramientas de la época primitiva en su obra La Ciencia en la Historia [1]:

"…Los utensilios son una extensión de los miembros del cuerpo humano: la extensión del puño y de los dientes, con la piedra, del brazo, con el garrote, de la mano o la boca con el saco o la sesta; o un nuevo tipo de extensión por la proyección del cuerpo, como cuando se arroja una pierda con determinado propósito".

Cabe recordar el estudio visionario del jurista Marcos Kaplan [2] en la década de los ochenta del siglo pasado, en su obra Ciencia, Sociedad y Desarrollo:

> "La cultura asume las funciones de conservación, de la multiplicación y complejización del saber, del saber hacer y del lenguaje. Pautas mentales y esquemas conceptuales están en relación simbólica con la experiencia de grupos e individuos y de las sociedades respectivas, a las que expresan, influyen y modelan.

Interpretando al autor, es un enriquecimiento permanente de conocimiento que permite resolver problemas concretos.

La cultura, declara Harari, tiende a aducir que solo prohíbe lo que es antinatural, pero desde una perspectiva biológica, nada es antinatural. Todo lo que es posible es, por definición, también natura [3]l. Y un comportamiento antinatural no existe

La recomendación de la Comisión Europea sobre digitalización y accesibilidad en línea y preservación

[1] De Bernal, John. *La Ciencia en la Historia*. UNAM. México 1979. Pág.84.
[2] Kaplan Marcos. *Ciencia, Sociedad y Desarrollo.* UNAM. 1887. Pág.70
[3] Harari, Yuval, Noah. De animales a dioses. Edit. Debate. México 2018. Pág. 168

digital de material cultural (2011/711/EU) [4] es el único instrumento europeo que aborda todo el ciclo de vida digital del patrimonio cultural desde la planificación, monitorización y financiación de la digitalización hasta el acceso en línea y la reutilización y la preservación digital

En su numeral 8, se consigna su fin:

(8) La digitalización es un medio importante para ampliar el acceso al material cultural y fomentar su uso. La acción concertada de los Estados miembros para digitalizar sus respectivos patrimonios culturales daría mayor coherencia a la selección de este material y evitaría duplicaciones en la digitalización.

El diccionario para juristas de Palomar de Miguel, define a la cultura como el resultado de cultivar los conocimientos humanos y de afinarse las facultades intelectuales del hombre por medio del ejercicio [5].

Carlos Aguirre, inicia el debate de la cultura al explicar, en palabras de Morin, hoy la sociedad enfrenta una pugna entre quienes promueven el cambio a lo desconocido, hacia lo abstracto, hacia algo distinto de lo trabajado, pero con la certeza de saber que más que un futuro cercano, nos referimos a un presente inminente [6]; ya que ellos por temor a lo desconocido los científicos, se encuentran en su etapa de esplendor. Nuestra realidad no pasa

Ocurre que cuando las formas tradicionales de pensar y resolver cuestiones cambian y las nuevas formas logran imponerse al modelo dominante, nos encontramos ante un cambio de paradigma. Ahora bien ¿Por qué se producen estos cambios de paradigma? [7], la historia de la ciencia se caracteriza por contar con largos periodos de estabilidad a los que se denominan ciencia normal. Estos periodos de estabilidad finalizan cuando son desequilibrados por cambios explosivos que abren paso a nuevas teorías. A estos cambios explosivos de Kuhn, los “llama revoluciones científicas”. Esto es los cambios de paradigma son motivos de las revoluciones científicas.

Nuestra realidad, reflexiona Aguirre, no pasa sólo por lo tangible, sino que la plataforma de conocimiento también se ha trasladado a lo virtualidad, al ciberespacio, una nueva realidad diferente con nuevos paradigmas [8]

Castells entiende por cultura el conjunto de valores y creencias que dan forma, orientan y motivan el comportamiento de las personas. El propone una nueva sociedad, la

[4] Recomendación de la Comisión Europea de 27 de octubre de 2011 sobre la digitalización y accesibilidad en línea del material cultural y la conservación digital.
[5] Palomar de Miguel, Juan. *Diccionario para juristas*. Ediciones Mayo, México, 1981. Pág. 357

[6] Aguirre, Carlos. *Apuntes de la nueva economía y gobernanza en internet, para comenzar a entender la nueva realidad.* Edit. Lex. Córdoba. Pág. 73.
[7] *Ibdem* pág. 81
[8] *Ibdem*. Aguirre. Pág. 88

sociedad red, global y trabaja con una multiplicidad de culturas ligadas a la historia y geografía de cada área del mundo. Lo que caracteriza a la sociedad red es la contraposición de la lógica de la red global y la afirmación de la multiplicidad de identidades locales [9].

Una sociedad red es aquella cuya estructura social, nos dice Castells está compuesta por redes activadas por tecnologías digitales de la comunicación y la información basadas en la microelectrónica, entendiendo la estructura social como los acuerdos organizativos humanos en relación con la producción, el consumo, la reproducción, la experiencia y el poder expresados mediante una comunicación significativa codificada por la cultura.

En este sentido Giddens[10] señala que en las sociedades premodernas coincidían el espacio y el lugar puesto que las dimensiones espaciales eran dominadas por la presencia, el estar ahí en el lugar físico y en la modernidad se separa el espacio del lugar al fomentar las relaciones entre los ausentes localizados a distancia de cualquier situación de interacción cara-a-cara.

La cibercultura un término concebido por Lévy [11] designa el conjunto de las técnicas (materiales e intelectuales, de las practicas, de las actitudes, de los modos de pensamiento, y de los valores que desarrollan conjuntamente en el ciberespacio.

Tres principios, nos dice Levy [12], han orientado el crecimiento del ciberespacio [13]:

La interconexión, capacidad de transmisión, el provocar una mutación en la física de la comunicación al pasar de la noción de canal y red a un espacio englobante. Todo espacio se convierte en canal interactivo y dirige la cibercultura a una telepresencia generalizada se constituye la humanidad en continuo sin frontera. los abonados a internet (estudiantes, investigadores, universitarios, comerciales siempre en desplazamiento, trabajadores intelectuales independientes, etc.) viajan probablemente más que la medida de la población. El tercer principio de la cibercultura es la inteligencia colectiva, constituye más un campo de problemas que una solución, es un campo abierto de problemas y búsquedas prácticas.

Se sube a la ola de Bauman.

[9] Castells, Manuel. *Comunicación y poder*. Edit. Siglo XXI. México 2012. Pág. 65
[10] Guiddens, Anthony. *Consecuencias de la modernidad*. Alianza editorial. México 2004. Pág. 30
[11] Lévy, Pierre. *Cibercultura. La cultura de la sociedad* digital. Edit. Anthropos-UAM. España, 2007. Pág. 1
[12] *Ibidem*, 99-103

[13] El carácter irrelevante del espacio físico ha llevado a acuñar el termino ciberespacio, creado por el novelista William Gibson, en un relato breve llamado Burning Chrome, posteriormente fue desarrollado en la novela neuromante en 1984, y se refiere a una alucinación mediante la cual se podía sentir como real un espacio que en realidad es generado por un ordenador y no tiene una correlación con la realidad física.

El advenimiento de la instantaneidad, declara Bauman, lleva a la cultura y a la ética humana a un territorio inexplorado, donde la mayoría de los hábitos aprendidos para enfrentar la vida han perdido toda utilidad y sentido [14]. Los hombres y mujeres de hoy quieren olvidar el pasado y ya no creen en el futuro

Nuestro mundo según nos dice Humberto Eco – nace con el acceso de las clases subalternas al disfrute de los bienes culturales y con posibilidad de producir estos últimos mediante procedimientos industriales. Vivimos en una sociedad de masas media (medios de comunicación de masas) y la situación conocida como cultura de masas se produce en el momento histórico en que estas entran como protagonistas de la vida social. Las masas han impuesto su lenguaje y su estética propias. Sin embargo, su manera de divertirse y su modo de vida no vienen de las capas inferiores de la sociedad, sino que proceden del código de modelos culturales burgueses.[15]

La sociedad de hoy es de consumo, en ella la cultura, al igual que el resto del mundo experimentado por los consumidores, se manifiesta como un depósito de bienes concebidos para el consumo, todos ellos en competencia por la atención insoportablemente fugaz y distraída de los potenciales clientes, empeñándose en captar esa atención más allá del pestañeo [16]. Tal como señalamos al comienzo, la eliminación de las normas rígidas y excesivamente puntillosas, la aceptación de todos los gustos con imparcialidad y sin preferencia inequívoca, constituye la estrategia de comercializar el arte.

Nuestra civilización capitalista post-industrial se apoya en el consumo, y bajo este lema se halla cualquiera de sus manifestaciones. La cultura, el arte, la ciencia se consumen casi como si fueran comestibles...”

La cultura en este sentido, siguiendo a Viser, puede concebirse como el proceso y la estructura a través de las cuales se construyen y regulan los usos de los espacios y los tiempos públicos y privados, colectivos, físicos y también imaginarios [17]. En todas las sociedades, la cultura ha sido la depositaria del tiempo, tanto del tiempo pasado-futuro como del presente, y por ende la fuente del reconocimiento del ser y de la identidad de cualquier sociedad.

Internet no modifica la forma en la que los ciudadanos se relacionan, sino que más bien, aumenta las posibilidades de comunicación entre ellos

En la primer revolución tecnología del siglo XX, comenta Labastida[18],

[14] Bauman, Zygmunt. *Modernidad liquida*. FCE. México 2019 Pág. 137
[15] Eco, Umberto. *Los movimientos pop*. Salvat Editores S.A., Barcelona 1973. P. 41
[16] *Ops. Cit.* Bauman. Pág. 19
[17] *Ops. Cit.* Viser
[18] Labastida Contreras Arturo, profesor de filosofía de derecho en diversas universidades, articulista y abogado socio en LHA S. C.

los medios masivos de comunicación se caracterizaron por congelar la realidad y repetir indefinidamente los contenidos, por su parte la revolución digital del siglo XX y XXI, implica una tecnología en la que los contenidos simplemente fluyen en un tiempo indefinido. En nuestros días sigue presente la contradicción que se ha dado en los procesos de comunicación, entre el conocimiento y el individuo, figurando como antípodas la autonomía individual y la posibilidad de la manipulación del individuo a través de la comunicación que se genera y recibe. Y en medio de estas dos, se genera sin querer la forma de expresión y sentir del ser humano.

Es difícil concebir, nos reitera Bauman- una cultura indiferente a la eternidad, que rechaza lo durable. Es igualmente difícil concebir una moralidad indiferente a las consecuencias de las acciones humanas, que rechaza responsabilidad por los efectos que esas acciones pueden ejercer sobre otros.

Homo faber es una locución latina que significa “el hombre que hace o fabrica”, - siguiendo a Labastida- entraña a la misma tecnología, como un elemento que por antonomasia, define la esencia misma de lo humano y la cultura como uno de sus productos; por otra parte el concepto de *Homo creator* expresa la idea de que la especie humana tiene la capacidad de evolucionar y crear para satisfacer sus necesidades concretas. El ser humano va diseñando su futuro en la línea del tiempo, utilizando los conocimientos, habilidades y destrezas del pasado, recreando lo aprendido para construir su realidad en el presente. Bajo el anterior supuesto, podemos aseverar que el entorno digital, está cambiando a las sociedades humanas, de modo que es de esperarse, en el futuro un nuevo tipo de homo sapiens evolucionado, en un contexto de nuevas relaciones socio-jurídicas hasta hoy insospechadas. No hay que olvidar que en el mundo jurídico contemporáneo han aparecido instituciones jurídicas, que son producto del impacto de las revoluciones tecnológicas, incluida la digital.

Conclusión si se me permite:

Cuando inicie el primer semestre en la universidad, lectura obligada fue introducción al estudio del derecho de García Maynes. Se explicaba la diferencia entre norma moral y jurídica. La cultura es una expresión, perceptible, exterior, no vinculante jurídicamente; pero insinúa modos de comportamientos sin obligarlos[19]. Contra el relativismo moral, hoy día, existe los valores universales, tales como el principio de la universalidad de los derechos humanos. Vázquez

[19] Nos dice el maestro García M. El derecho refiérase a la realización de valores colectivos, mientras la moral persigue la de valores personales. Habermas J, en este sentido expresa que las únicas normas que pueden afirmas ser válidas son las que reciben la aprobación de todos los afectado, en su calidad de participantes de un discurso práctico

y Serrano [20], exponen que los derechos humanos son exigencias éticas justificadas especialmente importantes por lo que deben ser protegidas eficazmente a través del aparato jurídico. El problema que no se advierte es que la naturaleza humana no se presenta de forma evidente ni explicita y eso deriva en reconocer a los derechos humanos como derechos morales. La realización de los derechos civiles y políticos sin el goce de los derechos económicos, sociales y culturales resultan imposible. Todos los derechos humanos y libertades fundamentales son indivisibles e interdependientes [21]. Se enfatiza la palabra indivisible.

Los modos, hábitos que hacemos o dejamos de hacer son ya influenciados por los aparatos electrónicos que usamos como si fueran una "extensión de nosotros" sin reflexionar. Aunado al control indirecto de los intereses mercantiles que se ocultan en internet que disponen o crean nuestros gustos o necesidades y hacen preguntarme si no golpean nuestro derecho humano a la dignidad, expresión e información.

Del impacto de la evolución tecnológica en el mundo del derecho, podemos dar cuenta de la aparición misma del derecho informático y de su tránsito doctrinal hacia el derecho de las nuevas tecnologías, que influye en la generación de ramas de la práctica jurídica. Producto de esta revolución digital es una nueva cultura jurídica cada vez más dinámica; es categórico el hecho notorio que estamos en el preludio de una nueva cultura, que sin duda requerirá del orden jurídico para darle el debido cause bajo la impronta de los derechos humanos.

Hoy toda expresión material e inmaterial debe ser rápida, útil, bella y debe satisfacer las necesidades del grupo local o mundial, si no, no tiene valor la misma obra o su autor por más común que sea. Siendo innegable que los procesos tecnológicos contemporáneos están en una revolución permanente como no se había visto en centurias anteriores.

Sin duda estamos en la Genesis de una nueva humanidad y orden mundial del que somos optimistas, ya que considero que las nuevas tecnologías sentaran las bases de la cultura y humanismo del futuro.

Alejandro Loredo Alvarez, abogado litigante y especialista en derecho de nuevas tecnologías, articulista, socio del despacho LHA, S.C.

[20] Los principios de universalidad, interdependencia indivisibilidad y progresividad. Apuntes para su aplicación práctica. Instituto de Investigaciones Jurídicas. UNAM

[21] ONU. Resolución 32/130, 1997.

2020

ELLOS SON EDI

EDI

[22] **Universidad Continental**

daniel.pena@upn.pe
Perú

RESUMEN: La cuarta revolución industrial en que vivimos, en donde la hiperconectividad, y latencia es una característica de la posmodernidad, ha traído consigo no sólo el aprovechamiento y maximización de nuestras oportunidades en el ámbito personal, académico y laboral, sino también ha rebasado las conductas desviadas punibles y no punibles, provocando que el Estado responda a la propuesta de su criminalización para controlar estos comportamientos delictivos que perturban la vida en sociedad y el adecuado desarrollo bio-psico-social de los ciudadanos a través del tipo penal: *"stalker" y "cyberstalker"* (acoso y acoso a través de la nuevas tecnologías de información o comunicación), para lo cual es necesario abordar su perspectiva criminógena, para su prevención y sanción.

PALABRAS CLAVE: Posmodernidad, stalker y/o cyberstalker, Nuevas Tecnologías de Información y Comunicación (NTICs); Criminología y Derecho Penal.

SOCIEDAD DE LA INFORMACIÓN Y CONDUCTAS DELICTÓGENAS

Recordemos que, en el siglo XXI, se ha *posicionado el "homo digitalis*", como eje de la funcionalidad planetaria, unidos a ello, los cambios sociales, transformaciones ya provocados por la digitalización, convergencia y globalización de las redes informáticas y como indica **Campos, P. (2016:30)***: "Engloban a todas las herramientas que procesan y guardan información como la televisión, la radio, el dispositivo móvil, la computadora e internet. Todos y cada uno de estos aparatos son utilizados por las empresas, en los hogares e instituciones para realizar sus actividades cotidianas".*

En este escenario **Del Rosal, B. (2009:02),** refiere que desde finales

[22] ***Abogado & Sociólogo. Magíster en Derecho Penal por la Universidad Nacional Federico Villarreal. Segunda Especialidad en Derecho Informático. Profesor de Derecho Penal en la Universidad Privada del Norte – Lima - Perú; Miembro del Comité Científico Internacional del Instituto Iberoamericano de Criminología Aplicada IBERCRIMA-España y Miembro de la Comisión Consultiva de Criminología del Ilustre Colegio de Abogados de Lima (2019). https://orcid.org/0000-0001-6070.***

de los ochenta y noventa, las legislaciones penales de la mayoría de países occidentales, han experimentado una serie de transformaciones, vertiginosas y aparentemente muy profundas, en cuanto a los principios sobre los que parecen inspirarse, que han hecho que la doctrina: penal, penológica y criminógena, hayan centrado de forma muy peculiar su atención en tratar exclusivamente en describir sus rasgos distintivos, sino sobre todo, de adivinar cuál es el modelo de política criminal, que sobre el delito, la pena ,el delincuente y la víctima, se sustentan esas modificaciones.

Sin embargo, la persecución penal será eficaz si el Estado capacita a los operadores jurídicos sobre los aspectos dogmáticos y doctrinarios de estos nuevos tipos penales, garantizando el debido proceso y el equilibrio entre los intereses de la sociedad y la ley penal bajo el irrestricto respeto de los derechos humanos.

PERSPECTIVA CRIMINÓGENA EN EL DELITO DE "STALKER Y CYBERSTALKER "

Ante las novísimas formas de delincuencia que se asocian al creciente aumento de usuarios en internet, donde la hiperconectividad es una característica irrefutable, haciéndonos ultra vulnerables, desde la criminología y victimología, se deben profundizar el estudio y análisis de los factores criminógenos ante la carencia de una definición legal de acoso físico y virtual, facilitando la comisión de actos ilícitos, constituyendo un *"tinglado de impunidad"* para sus agresores.

En consecuencia, advierte **Agustina, J. (2009:01),** el espacio virtual genera una atmósfera de anonimato que protege, promueve y alienta nuevos modos de atentar contra personas e instituciones.

Ahora bien, *"stalker"* es una palabra que cada vez más obtiene un mayor auge y utilización en la lengua española, es un anglicismo. Proviene del verbo en lengua inglesa "*to stalk" que equivale a "acosar", "espiar" o "perseguir",* traduciéndolo al castellano. Al ponerle el prefijo *"cyber"*, nos referimos al acoso mediante soportes tecnológicos, en específico en entornos digitales, que invaden nuestro día a día, para describir la acción propia de acosar vía redes sociales o comunicación bidimensional a una persona, siendo entre las más populares: ***Facebook, Twitter, Instagram, Twitter, Snapchat*** etc.

Sin embargo, suele tener elementos definitorios, explica **Palop, M. (2018:91)**: Debe tratarse de un patrón de conducta insidioso y disruptivo, incluyendo todas las conductas mencionadas en el artículo 151-A del C.P. peruano: (…) *"El que de forma reiterada, continua o habitual y por cualquier medio, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona sin su consentimiento" (…); "aun cuando la conducta no hubiera sido reiterada,*

continua o habitual. Por lo tanto, sin la anuencia de la víctima; que esta comunicación o aproximación asfixiante y no querida sea susceptible de generar algún tipo de repercusión en la víctima *(desasosiego, temor, angustia, cambio de hábitos personales)*; y no interesa si es repetitivo o no el número de conductas de acoso para ser considerado delito.

Asimismo, el término *"stalker",* sostiene **Lorenzo, S. (2015:06)** en la acepción materia de nuestro ensayo, ha sido objeto de diversas conceptualizaciones. Por lo cual, lo define como *"conducta reiterada e intencionada de persecución obsesiva respecto de una persona, el objetivo, realizada en contra de su voluntad y que le crea aprehensión o es susceptible de provocarle miedo razonablemente"*.

PERFIL DEL STALKER Y/O CYBERSTALKER

Debemos partir de la premisa que cualquier persona es un *"stalker", y/o "cyberstalker"* en potencia y sabemos también que por lo general pasará desapercibido. La ciencia de la conducta humana (*Psicología*), lo define como *"síndrome de acoso apremiante"* y es analizado del mismo modo por la sociología y psiquiatría, criminología; y sus consecuencias punitivas por el derecho penal, siguiendo la clasificación de Mullen, Pathé y Purcell, citado por **Becerra, E. (2015:13)**

STALKER RESENTIDO: El propósito fundamental de sus conductas patológicas, es asustar y afligir a la víctima debido a un sentimiento de rencor y resentimiento hacia *"él o ella"*, por cualquiera que sea el móvil que lo inspire. **TORRAS, J. (2017:03).**

STALKER DEPREDADOR: El acechador vigila a su víctima, habitualmente con fines de índole sexual, hasta que encuentra la ocasión perfecta para atacarla, siendo precavido y tolerante para perfeccionar su *"circuito de acoso"*, siendo las redes sociales sus fortalezas para preservar su anonimato.

STALKER RECHAZADO: Este acosador espía con sentimientos resentidos o con el fin de retomar una relación (*amorosa, laboral, amistosa, etc*) que la víctima ha roto y que desesperadamente quiere retomar convirtiéndose en una *"obsesión".*

STALKER PRETENDIENTE INEFICAZ: Este tipo de acosador suele tener poca capacidad de comunicación y de interrelacionarse con otras personas y comprende de forma errónea el hecho de tener los mismos gustos, actividades o aficiones con la víctima, hasta llegar al punto de obcecarse con ella.

STALKER DESEOSO DE INTIMIDAD: El insistir por una relación amorosa e íntima con la víctima es el esencial aliento de este tipo de *"stalker y/o cyberstalker"*, que ve en la otra persona el mito de su *"media naranja"*, que en su psique siempre ha buscado y anhelado, aunque no tenga una relación estrecha ni profunda con la víctima, creando en su mente patológica, una relación de dependencia aflictiva que

lo atormenta y pondera su ansiedad. **Llamas, E. (2016-2017:07).**

CONCLUSIONES

PRIMERA:

El delito de *"stalker" y/o "cyberstalker",* posee un componente psicopatológico. El Acoso, junto con las demás conductas delictivas del presente siglo XXI, pretenden intimidar a la víctima; de forma reiterada, continua o habitual y por cualquier medio las vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con ella sin su consentimiento, de modo que pueda alterar el normal desarrollo de su vida cotidiana, y valiéndose de cualquier tecnología de información y comunicación, aun cuando la conducta no hubiera sido reiterada.

SEGUNDA:

Sólo conociendo la etiología y dinámica holística del delito del *"stalker* podremos afrontar su problemática punible y no se agota con la sola integración al catálogo penal, debemos decirlo: no es suficiente, y se debe procurar que no se convierta en un derecho penal simbólico, sino favorecerlo con su estudio dogmático, doctrinario y casuístico. En esas condiciones, contribuiremos a su control y sanción efectiva, destronándolo del manto de impunidad de las *"cifras oscuras"* que otorga ventajosamente al *"cyberstalker",* la inteligencia artificial.

REFERENCIAS BIBLIOGRÁFICAS

1.- AGUSTINA SANLLEHÍ, José, *"La Arquitectura digital como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual".* Euskera: International e-Journal of Criminal Science, Artículo 4, Número 3, Universidad del País Vasco, 2009. Recuperado de: https://www.ehu.eus/ojs/index.php/inecs/article/view/262

5.- BECERRA VECINO, Ester, *"El delito de Stalking"*. Trabajo Final de Grado en Derecho. Dirigido por la Dra. Núria Torres Rosell. Tarragona: Universitat Rovira I Virgili, 2015. Recuperado de: https://blocking.esforos.com/viewtopic.php?t=32

7.- CAMPOS XOOL, Pamela, "*Delitos Informáticos en México y sus formas de Prevención".* México: Revista Electrónica: Visión Criminológica-Criminalística-Sección: Tópicos Latinoamérica, 2016. Recuperado de: https://es.scribd.com/document/389435644/Articulo09-Delitos-Informaticos-en-Mexico-y-Sus-Formas-de-Prevencion

9.- DEL ROSAL BLASCO, Bernardo, *¿Hacia el Derecho Penal de la Postmodernidad? Granada:* En Revista Electrónica de Ciencia Penal y Criminología, Nº11-08. 2009. Recuperado de: http://www.criminet.ugr.es/reepe

13.- LORENZO BARCENILLA, **Silvia**, *"Stalking El nuevo delito de acecho del art.172 ter del Código Penal. Aproximación al cyberstalking".* Barcelona: Universitat Oberta de Catalunya. Master Universitario en Abogacía. Junio del 2015.Recuperado de:

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/44681/6/slorenzobaTFM0615memoria.pdf

14.- LLAMAS PINTO, Erika, *"El delito de Stalking"*. Trabajo de fin de Grado. Almería: Universidad de Almería. Curso Académico: 2016-2017. Recuperado de: http://repositorio.ual.es/bitstream/handle/10835/6478/14470_TFG%20STALKING.pdf?sequence=1&isAllowed=y

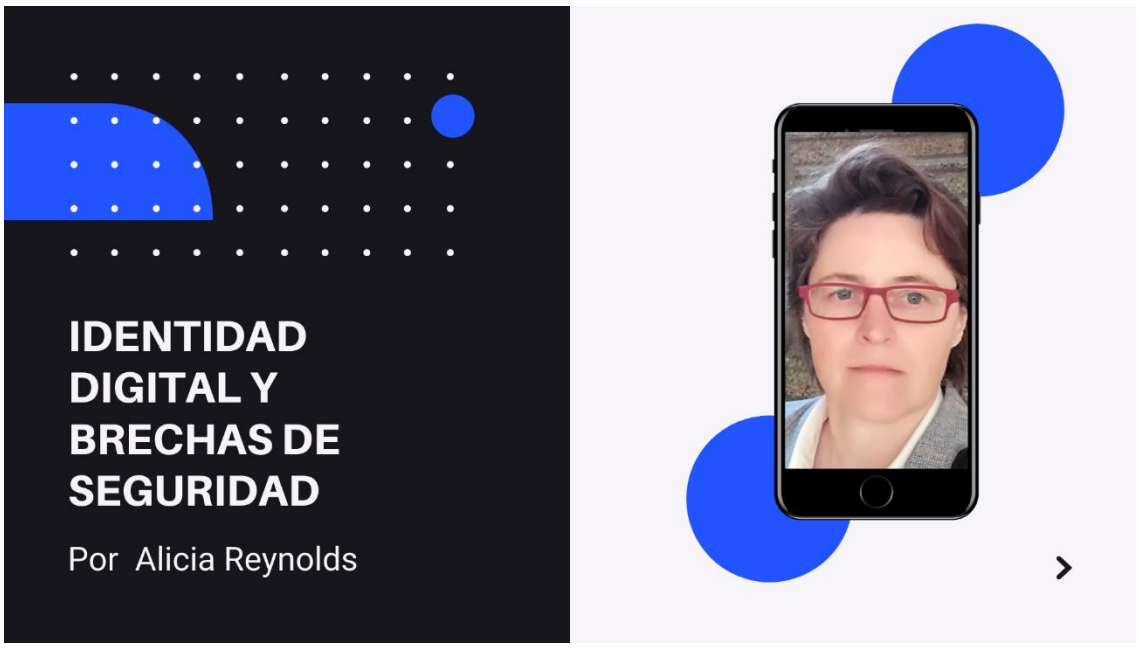
18.- PALOP BELLOCH, Melania, *"La falta de regulación del artículo 172 ter en el supuesto de reincidencia del agresor de violencia de género"*. Madrid: Revista Internacional de Derecho de las Comunicaciones y Tecnología: Derecom Nº 24, marzo - septiembre 2018.Recuperado de: http://www.derecom.com/derecom/

26.- TORRAS COLL, José, "*El Delito de Stalking. Breves consideraciones".* Madrid: LEFEBRE. Tribuna 24 de junio de 2017.Recuperado de: https://elderecho.com/el-delito-de-stalking-breves-consideraciones

2020

ELLOS SON EDI

EDI



23

Introducción

A medida que avanzamos hacia la Industria 4.0 o Cuarta Revolución Industrial[24] y se realizan mas transacciones de forma digital, la representación digital de la propia identidad se ha vuelto cada vez mas importante, esto es aplicable tanto, a los seres humanos, a los dispositivos, al igual que la inteligencia artificial, entidades digitales, robots y a los recursos naturales. Humanos y dispositivos por igual, requieren de una identidad verificable y confiable necesaria para acceder, interactuar y realizar transacciones con otros. Acreditar identidad, es el primer paso de cada transacción, entre dos o más partes tanto en el mundo físico como en el digital. Desde la provisión de servicios financieros hasta la identificación emitida por el Estado. Tal identidad para las personas humanas, constituye un prerrequisito fundamental para poder acceder a servicios esenciales y, participar en sistemas económicos, sociales y políticos. Entonces ¿qué es una identidad digital? ¿qué sucede con las fuga o filtraciones de datos personales? ¿Debería ser obligatorio notificar los incidentes de seguridad? Éstas son algunas de las preguntas a las que se da respuesta en un artículo mas complejo denominado:*"Identidad Digital*

[23] Abogada. Posgrado en Cibercrimen y Evidencia Digital (UBA). Miembro del equipo de investigación de Legislación, Doctrina y Jurisprudencia del Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales (OCEDIC) de la Universidad Austral. Técnica en Hardware de PC (THPC) Microsoft OEM certified y Técnica en Redes Informáticas (TRI), Microsoft OEM certified. Titular del desarrollo: Abogacía Digital http://abogaciadigital.ar.

[24] El concepto *"Cuarta Revolución Industrial"* fue acuñado por Klaus Schwab, fundador del Foro Económico Mundial, en el contexto de la edición del Foro Económico Mundial 2016.

concepto legal emergente en el contexto del ciberespacio y las brechas de seguridad" del cual aquí, se comparte una acotada presentación.

I. Identidad y Datos personales

Expresa la Declaración Universal de Derechos Humanos en su artículo sexto:*"Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica."*

Atributos de la personalidad jurídica, son aquellas propiedades o características de identidad propias de las personas humanas o jurídicas como titulares con derechos. Son inherentes, únicos, inalienables, imprescriptibles, e irrenunciables y que se conforman con el nombre, capacidad, domicilio, nacionalidad, estado civil y patrimonio.

Analizando las definiciones que ofrece la Real Academia Española[25], podemos entender a la identidad como el conjunto o universalidad de datos personales de un sujeto en un tiempo determinado. Según la Corte Interamericana de Derechos Humanos, el derecho a la identidad *"puede ser conceptualizado, en general, como el conjunto de atributos y características que permiten la individualización de la persona en sociedad y, en tal sentido, comprende varios otros derechos según el sujeto de derechos de que se trate y las circunstancias del caso. (..)"*.En otras palabras, la identidad es la conciencia de una persona de esa universalidad, que la hace única por lo que configura un Derecho Humano, y por tanto, el bien jurídico tutelado sería la persona.

En contraposición a lo expresado, la ley de Protección de Datos Personales[26], permite el comercio de algunos de los datos personales que conforman la identidad de las personas. Y, por tanto, esos datos personales serían bienes. En consecuencia, la identidad puede ser entendida como una universalidad de datos personales donde algunos tendrían el carácter de bienes y otros no.

I.1. Identidad Digital

Una identificación digital habilita operaciones y transacciones para el movimiento de personas, fondos, bienes, datos y otros recursos y al mismo tiempo, los sistemas y mecanismos de identidad digital ofrecen la promesa de una mayor eficiencia, seguridad y confianza, a través de un conjunto de atributos electrónicos como plantillas biométricas, registros de navegación y trazabilidad. La identidad digital tiene como objetivo, permitir la identificación de una entidad tanto en línea como remotamente por medios electrónicos, a través de la explotación de atributos cibernéticos

[25] 2. f. Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás. Y 3. f. Conciencia que una persona tiene de ser ella misma y distinta a las demás.

[26] Ley 25.326, sancionada en Octubre 4 de 2000.

como huellas digitales. Pero, ¿qué es la identidad digital?

Como consecuencia del uso de las nuevas tecnologías, principalmente Internet, muchos de los datos de las personas se han convertido, prácticamente, en datos de acceso público. Este fenómeno se ha incrementado con el uso masivo de las redes sociales (Lezcano, 2010). Cuando un conjunto de datos personales se asocia a una persona en un marco digital, algunos lo llaman erróneamente "identidad digital" (Sullivan, 2011).

Cuando hablamos de identidad digital no implica una sola fuente de información, sino una combinación de múltiples atributos ¿Cualquier forma de información vinculada a cada uno de nosotros resultaría en un *"atributo de identidad digital"?* Prácticamente no hay límites en la cantidad de atributos que pueden definirnos, pueden ser indivisibles (datos biológicos) o también acumulativos (datos históricos). Por ejemplo, hay muchos atributos de identidad digital biométricos, como el aspecto de nuestra cara, patrones de voz, etc. Además de otros atributos de identidad digital, como nuestros nombres, o la dirección actual también puede definirnos socialmente.

I.2. Identidad Digital en Argentina

La identidad digital es fundamental dentro del contexto de la Sociedad de la Información. Analizar el marco jurídico aplicable al ciberespacio en nuestro ordenamiento jurídico, centrando la problemática en el derecho de identidad digital confluye en dos temas jurídicos e informáticos de significativa actualidad: la protección jurídica de los datos personales y la regulación de las firmas y certificados digitales.

El RENAPER[27] a través del Decreto 744/2019 autorizó a emitir en forma adicional a la tarjeta, la credencial virtual del DNI para dispositivos móviles inteligentes. Ésta credencial virtual debe contener un certificado encriptado y firmado digitalmente y su validación se realiza a través de la aplicación *Mi Argentina*[28]. El uso de ésta credencial virtual es posible por medio de la validación en el Sistema de Identidad Digital[29] (SID).

[27] La ley 13.482 creó el Registro Nacional de las Personas (Renaper), es el organismo estatal que realiza la identificación y el registro de las personas físicas que se domicilien en el territorio o en jurisdicción de Argentina.

[28] Validación en Mi Argentina https://www.argentina.gob.ar/miargentina/app

[29] *"El SID es un sistema seguro y confiable de validación de identidad que respeta la privacidad de los datos y fotos suministradas por el ciudadano. La biometría de rostro es un modo de identificación legalmente válido y adaptado a las nuevas tecnologías según los términos de la ley 17.671 y su reglamentación decreto 1501/09."* https://www.argentina.gob.ar/sid/preguntasfrecuentes

En 2018, la legislatura de la Ciudad Autónoma de Buenos Aires aprobó la reforma del Código Contravencional incorporando el *"Capítulo V - Identidad Digital de las Personas"* con las siguientes contravenciones: 1) Difusión no autorizada de imágenes o grabaciones íntimas, 2) Hostigamiento digital, y la 3) Suplantación digital de la identidad. Esta última figura permite inferir en la interpretación de los legisladores porteños sobre qué atributos de identidad afectados, configurarían una suplantación de la identidad en el contexto digital: 1) la imagen ¿cualquier imagen? y, 2) los datos filiatorios de una persona.

En el orden nacional, aún hoy no se encuentra tipificada como delito la suplantación de la identidad digital, ni el robo o su usurpación, como tampoco la explotación de identidades digitales, esta última conducta, está vinculada con las violaciones de datos personales masivas, caso "Weleakinfo.com[30]".
La propuesta prevista en el Proyecto de Reforma del Código Penal de la Nación para la suplantación de la identidad, art. 492, no hace a referencias a atributos de la identidad sino directamente utiliza el término "identidad" ¿Debe leerse en un sentido rudimentario de afectación y utilización de *datos personales digitalizados* vinculados a la identidad física? o ¿debería interpretarse como abarcativo de la identidad digital? Si así fuera, ¿totalizaría todas las identidades en internet vinculadas a la víctima?, o ¿deberíamos separar entre identidades electrónicas y digitales?

II. Brechas de Seguridad - Ciberataques

Una brecha de seguridad, conocida nativamente como *data breach* (violación de datos), *information leakeaged* (información filtrada) o *data spill* (derrame de datos) wikipedia la define como: *"un incidente de seguridad en el que los datos confidenciales, protegidos o confidenciales son copiados, transmitidos, vistos, robados o utilizados por una persona no autorizada para hacerlo. Las violaciones de datos pueden involucrar información financiera como una tarjeta de crédito o datos bancarios, información de salud personal, información de identificación personal, datos biométricos, secretos comerciales de corporaciones o propiedad intelectual."*

Breve aclaración, una violación o acceso ilegítimo a un sistema informático o dato informático (art. 153 bis CPN) no implica necesariamente una violación de datos personales y, en determinados supuestos, un incidente de seguridad de datos personales no implica rigurosamente un acceso ilegítimo o un ciberataque, sino que, tal filtración podría acaecer

30 https://nationalcrimeagency.gov.uk/news/weleakinfo-com-site-hosting-stolen-credentials-taken-down-after-international-operation

por fallas en la seguridad negligentes o ignoradas. La ley 26.388 sólo aportó o modificó conductas dolosas, no culposas, a excepción del art 255.

II.1 Obligación de Notificar o Denunciar Brechas de Seguridad

En el modelo español de protección de datos personales, los operadores que explotan redes públicas de comunicaciones electrónicas o que prestan servicios de comunicaciones electrónicas disponibles al público tienen la obligación de notificar a la Agencia Española de Protección de Datos (AEPD) las brechas de seguridad que sufran cuando supongan la pérdida, destrucción, alteración o acceso ilegítimo a datos de carácter personal. Asimismo, el operador deberá notificar también la violación al abonado o particular sin dilaciones indebidas. Las demás empresas, distintas a las referidas del sector de las comunicaciones electrónicas, no están habilitadas para notificar sino que están obligadas a denunciar dicha afección sufrida sobre los ficheros que están obligadas a custodiar. En caso de que la brecha no haya afectado a datos personales, solo las empresas que formen parte de las infraestructuras críticas del estado podrán, si lo desean, informar al CNPIC español.

En Argentina, no hay tales y claras obligaciones ante un incidente de filtración de datos personales. Tampoco contempladas infracciones administrativas. Sin olvidar que, como se menciona más arriba, las brechas de seguridad "intencionales" configuran delito y, para el caso de que se dieran brechas de seguridad por violación de un sistema, dato informático o base de datos personales en el ámbito de una entidad estatal, sus funcionarios y empleados públicos resultarían obligados por ley a denunciarlas.

No obstante, los vacíos legales, el Congreso Nacional sancionó en el año 2017, la ley 27.411 de adhesión al Convenio de Budapest, sellando un compromiso de adecuación legislativa y de cooperación internacional para la persecución de los delitos allí estipulados, previéndose la obligación de designar un punto de contacto localizable (red 24/7), con el fin de garantizar, una asistencia inmediata en las investigaciones de delitos vinculados a sistemas y datos informáticos, como para la obtención de evidencia digital, con miras en maximizar eficacia en las investigaciones penales en entornos digitales.

Conclusión

Una identidad oficialmente reconocida es un derecho humano básico. La brecha digital y las brechas de seguridad expanden una enorme grieta entre la realidad de los individuos que viven en países desarrollados, de los que viven en países en vías de desarrollo. Nuestros datos son nuestra identidad y para potenciar lo humano, debemos potenciar la identidad. Entiendo que, en la medida que avance la infraestructura tecnológica adecuada de Identidad Digital, se hará más clara su autonomía respecto del régimen de

Protección de Datos Personales. Es decir, podría ocurrir, que la migración a una tecnología sólida y autosuficiente a través del uso de Inteligencia Artificial termine garantizando ciberseguridad paulatinamente, creándose así, un sistema de confianza en una entidad supra humana superadora técnicamente, a los discutidos y descuidados sistemas actuales de identidad fragmentados, como a los tensos y vulnerables regímenes de protección de datos actuales, en el estrecho camino del proceso evolutivo hacia la civilización digital.

Bibliografía

- DUPUY, Daniela (Dirección), y KEIFER, Mariana (Coordinación), (2018) "Cibercrimen II", Editorial IB de F. Montevideo-Buenos Aires.
- PARADA, Ricardo y ERRECABIRDE, José, compiladores, Suplemento Especial "Cibercrimen y delitos informáticos" (2018), 1° Edición, Editorial Erreius.
- SULLIVAN, Clare Linda (2011) "Digital Identity - An Emergent Legal Concept." Australia: University of Adelaide. Press. Disponible en: http://ssrn.com/abstract=1803920.
- ADC Digital, Área Digital de la Asociación por los Derechos Civiles (2017), "Desafíos de la biometría para la protección de los datos personales: Reflexiones sobre el caso SIBIOS".
- LEZCANO, José María. “Las redes sociales en Internet. Herramientas para la comprensión de un fenómeno en progreso”, En: XI Congreso Nacional y I Latinoamericano de Sociología Jurídica: Multiculturalismo, Identidad y Derecho. Buenos Aires: Argentina, 7, 8 y 9 de octubre de 2010. Actas. ISBN 978-987-25475-1-6.

Hablemos de Cyberbullying […]

A los fines de dar inicio a este artículo, co-instrumentado por dos abogadas dominicanas, establecidas en Estados miembros de la Unión Europea (España y Francia respectivamente) y que se encuentran vis à vis a una realidad distópica e íntimamente relacionada al desarrollo de las nuevas tecnologías de la información i.e. TIC y la protección de la data personal. Las cuales estudian, un subproducto de esta rápida evolución de las TIC. Este es uno de los peores fenómenos de ese desarrollo: ***El Cyberbullying***, como si se tratara de una de las maldiciones liberadas de la mismísima Caja de Pandora.

I. La génesis del *cyberbullying*

Hace cinco décadas Olweus (1970) comenzó a estudiar de forma sistemática el fenómeno del maltrato entre iguales en el ámbito escolar, siendo ampliamente reconocido como un pionero de la investigación sobre el acoso escolar, en la actualidad se conoce más de este acto de violencia, a esta evolución en los estudios sobre el *bullying.* Debido a las diferencias vistas en la forma de maltrato mediante el uso de la tecnología, aportó nuevas modalidades de *bullying*, acoso, abuso y hostigamiento, a través, de las nuevas tecnologías se le conoce como: *cyberbullying*.

El *cyberbullying* es un acto muy publicitado pero poco conocido por la mayor parte de la sociedad, estos hechos ilícitos, implican un incremento de las acciones agresivas a través de las TIC, sin embargo los profanos en la materia, cuando se habla de *cyberbullying*, deducen que se trata de meros insultos y amenazas, que ya han traspasado, hace años, los muros del espacio físico.

No se debe confundir: *cyberbullying* con *ciberacoso*. El cyberbullying se

da entre dos iguales, es decir entre niños o adolescentes, en el ciberacoso o acoso cibernético están involucrados adultos.

A. Modalidades de *cyberbullying*

Se ha observado un rápido desarrollo y utilización de nuevas modalidades de *bullying*, una de éstas es el *cyberbullying*, que posee varias categorizaciones conforme a los comportamientos identificados por el estudio de INTECO Y ORANGE (2010);

- *Cyberbullying* pasivo: La víctima recibe mensajes o llamadas de otros chicos o chicas agrediéndola.
- *Cyberbullying* activo: el victimario acosa a algún compañero a través del móvil u otros recursos electrónicos afines.

La literatura ha detectado la existencia de perfiles relacionados con las personas que participan en estas acciones, o bien las sufren, ya sea de manera física o en el medio tecnológico, y por lo general, muestran elementos coincidentes:

- El acosador/*bullie*: Persona que normalmente tiene problemas como falta de autoestima, y que se siente bien manifestando su fuerza, su tiranía y hostigamiento sobre otros.
- La víctima: Son aquellas personas que individual o colectivamente han sufrido un daño.
- Los espectadores: Individuos que presencian una situación de acoso, ya sea en persona o en línea, es un espectador. Esto puede incluir personas conocidas y desconocidas.

B. Elementos que tipifican al *cyberbullying*

Los delitos conformes a su naturaleza tienen elementos que vienen tipificados desde su nacimiento. El *cyberbullying*, como un delito relativamente nuevo, existe de forma general como manifestación de cualquier tipo de metodología de comunicación electrónica que solo se encuentra limitada por la pericia tecnológica y la imaginación de los menores acosadores. A partir de lo establecidos citamos algunos ejemplos concretos (Flores 2008):

- “Colgar” en Internet una imagen comprometida (real o efectuada mediante fotomontajes), datos delicados, que pueden perjudicar o avergonzar a la víctima y darlo a conocer en el entorno de relaciones de la víctima.
- Dar de alta, con foto incluida, a la víctima en un site donde se trata de votar por la persona más fea, a la menos inteligente, y cargarle de “puntos” o “votos” para que aparezca en los primeros lugares.
- Crear un perfil o espacio falso en nombre de la víctima, donde se escriban a modo de confesiones (en la primera persona) determinados

acontecimientos personales, demandas explícitas de ontactos sexuales, etcétera.

II. Los Menores de edad frente al *cyberbullying*

La aparición de Internet y los sistemas informáticos implicó un antes y un después en el *modus operandi* de las personas para acceder a las informaciones.

Según el Dr. Eloy Velasco, juez español, en su libro *Los delitos cometidos a través del Internet cuestiones procesales,* explica que se trata de "ataques al bien jurídico de la privacidad con concepto que incluye la intimidad", que va más allá, pues abarca todas las modalidades protegidas en el artículo 18 de la Constitución Española, (el honor, la intimidad personal, la familiar, la propia imagen, el domicilio, el secreto de las comunicaciones o el uso correcto de la informática (Velasco Núñez, 2010).

Tenemos la obligación de proteger los menores de edad victimas de *cyberbullying*, estos sufren daños psicológicos y en su mayoría a la hora de actuar ante la justicia se toma en cuenta la protección de datos de los menores que no salga a la luz ninguna información relevante que ponga en evidencia el menor causante de este ciberdelito, se va actuar de acuerdo al lado que te encuentres, si de victima o victimario.

A. Cyberbullying: Menor de edad hacia Adulto

El adulto que acosa por internet a otro adulto es **ciberacoso**, los menores que se atacan entre si es **cyberbullying**. Pero, **¿El menor que acosa por medio de las TIC un adulto como se llamaría y juzgaría?**

En el código penal español ni el ciberacoso, ni el cyberbullying están tipificados como tal, son fenómenos modernos y prácticamente nuevos, y este , es entre otros el uno de los principales problemas que se plantea. El legislador ha dejado estos ciberdelitos que sean juzgados como una adaptación de los artículos establecidos que puedan lesionar la integridad de la persona, dejando un vacío jurídico en lo que es la ley y la brecha digital, el menor es el más indefenso en estas situaciones porque suele sufrir en silencio los ataques.

En España, en los casos de los menores de edad que cometen un ciberdelito; se aplicará lo establecido en la Ley Orgánica de la Responsabilidad Penal de los Menores (LORPM) estableciendo una edad (14 a 18 años), que por la naturaleza del período vital de los menores, y que la psicología evolutiva singulariza, permite castigar y en su caso dar una respuesta socioeducativa eficaz, a la luz de la imputabilidad penal.

Consideramos que si una persona infringe la normativa legal debe asumir las consecuencias legales correspondientes, respetando los derechos humanos y fundamentales, **la responsabilidad penal debe ser personal sin importar la edad**.

B. Posición de la Unión Europea

Iniciamos con una problemática, si un acto ilícito que se comete por medios de las TIC no tiene definición exacta, el legislador, victima, ciberdelincuente y población en general está ante un delito que no sabe si es delito o es un juego.

La Unión Europea en lo adelante (UE) reconoce la importancia de proteger a los niños en relación con el uso de la tecnología y aunque no existe una definición comúnmente acordada de cyberbullying a nivel de la UE, el fenómeno ha sido descrito por las instituciones de la UE en el contexto de diversas iniciativas. La falta de una definición especifica acordada de cyberbullying a nivel de la UE, puede dar lugar a que estos actos ilícitos, realizados a través del internet queden impunes.

El Convenio Europeo para la protección de los Derechos Humanos protege y promueve derechos fundamentales que son aplicables a todas las personas incluyendo a entre ellos el derecho al respeto a la vida privada y familiar y la libertad de expresión, de acuerdo con lo establecido en el convenio sobre la ciberdelincuencia este garantiza la seguridad en la internet aunque respecto al cyberbullying no lo específica. De otra parte el Convenio de Lanzarote considera que los estados deben ampliar la penalización de los delitos sexuales que se comente en línea.

En general la UE no ha logrado instrumentar la normativa especifica que cada estado miembro cumpla con lo relacionado al cyberbullying es un problema de gestión en todos los Estados miembros el hecho de que cada país tiene diferentes culturas jurídicas y la edad pertinente para que un menor pueda juzgarse ante la justicia varía.

III. Quid del Reglamento General de Protección de Datos (RGPD) vs *El Cyberbullying*

La CNIL (La commission nationale de l'informatique et des libertés) la autoridad administrativa francesa e independiente que se encarga de velar por que la tecnología de la información esté al servicio del ciudadano y no atente contra la identidad humana, los derechos humanos, la privacidad o las libertades individuales o públicas, está preocupada por el número de quejas que recibe por casos de *cyberbullying*, 30 quejas en el espacio de 6-7 meses.

Como señalado, dentro del Derecho Internacional General, no existen normas muy claras que hagan referencia específicamente al *cyberbulling*. Sin embargo, el artículo 19 de la Convención de las Naciones Unidas sobre los Derechos del Niño (Adoptada y abierta a la firma y ratificación por la Asamblea General en su resolución 44/25, de 20 de noviembre de 19) sobre la protección de todas las formas de violencia es aplicable al acoso en línea**.**

A nivel regional, el Consejo de Europa ha adoptado una serie de medidas jurídicamente vinculantes

relacionadas con el acoso en línea. La UE, ejerce un papel complementario en este ámbito. Razón por la que no se ha instrumentado un Reglamento, el cual tendría un efecto directo respecto a los Estados miembros.

De otro lado, la Unión europea, dentro de su marco jurídico dispone de directivas, debemos recordar que las directivas, dentro del orden jerárquico de las normas de la UE no disfrutan de este *"efecto directo"* pleno de los reglamentos, ya que las mismas requieren de una: ley o decreto para transponerla a sus legislaciones nacionales, en ocasiones con importantes modificaciones, ver la jurisprudencia emblemática **Van Gend en Loos de 1963.** Actualmente, existen las directivas relacionadas al tema y ambas vigentes:

- Directive 2012/29/EU of the European Parliament and of the Council 2012.
- Directive 2011/93/EU of the European Parliament and of the Council 2011. Esta Directiva ha sido aplicada por todos los Estados miembros, excepto Dinamarca.

Y en vista, de que nos encontramos con esta marea de actos jurídicos de la UE, pero con las mismas problemáticas: **¿Cómo enfrentar el *cyberbullying* dentro de la UE de manera coherente?** Y la próxima pregunta sería: **¿Cuál es el rol del RGPD en todo esto?** Exploremos.

A. RGPD: Escudo protector contra el Cyberbullying

El Reglamento prevé normas específicas para los niños, que pueden ser menos conscientes de los riesgos que entraña el tratamiento de datos personales. Según el Reglamento, el consentimiento para el tratamiento de los datos de un niño debe ser dado o autorizado por el titular de la responsabilidad parental.

Esta disposición contenida en el artículo 8.1 del RGPD: *"El tratamiento de los datos personales de un niño se considerará* ***lícito cuando tenga como mínimo 16 años****. Si el niño es menor de 16 años, tal tratamiento únicamente* ***se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño****, y solo en la medida en que se dio o autorizó. Los Estados miembros* ***podrán establecer por ley una edad inferior a tales fines****, siempre que esta no sea inferior a 13 años"[...]*

¡Voilà! *Les nuances* del RGPD, que a pesar de ser un reglamento, funciona en ciertas disposiciones como una directiva i.e. Que cada Estado miembro, puede modificar ciertas disposiciones para adaptarlo a su marco jurídico. Volvemos a las incoherencias para atacar el tema, ya que cada Estado miembro determina la edad mínima para el tratamiento de los datos personales de un niño/a. e.g. En Francia a partir de los 15 años un menor de edad puede dar su consentimiento para el uso de su data sin autorización de

sus padres, mientras que en España es 13 años!

El RGPD introdujo un: "derecho al olvido" que permite a las víctimas solicitar la eliminación de sus datos personales. Esto previsto en el artículo 17: *"El interesado tendrá derecho a obtener* ***sin dilación*** *indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad*;*

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento" […]

El artículo 17 constituye un guardián para todos los niños víctimas de *cyberbullying* ya que les daría la posibilidad de solicitar la supresión de los datos personales puestos a disposición en línea. Su rol es fundamental en la protección de los niños y jóvenes contra el *cyberbullying*. En virtud de lo explicado anteriormente, si se reúnen datos personales por medios electrónicos, quienes los reúnan y publiquen esta información sobre terceros deberán solicitar su **consentimiento**. Por consiguiente, este marco es plenamente aplicable a todos los casos en que existe *cyberbullying*.

B. El Affaire Mila y la Competencia de las jurisdicciones francesas: cuando la víctima (s) y victimario (s) son menores de edad

1. El Affaire Mila es un caso de *cyberbullying* en Francia, muy controversial. Inicia enero de 2020, cuando Mila, una adolescente de 16 años, criticó virulentamente el Islam en la aplicación social: Instagram, luego de rechazar los avances de un usuario de Internet, que más tarde se convirtió en lesbófobo y la acusó de racismo.

El caso llegó a una dimensión nacional y creó numerosas reacciones polarizadas en las esferas: política, mediática y religiosa, con especial énfasis en los temas de la islamofobia y la "noción de blasfemia" la cual no existe, en el derecho francés. Al unísono, se abrieron dos investigaciones judiciales: una contra Mila por incitación al odio -que fue desestimada, esto relativo a su primer video- y la otra sobre las amenazas contra ella.

Un junio de 2020, dos jóvenes (menores de edad) fueron acusados y procesados en relación a la investigación.

2. Aquí observamos, una posición muy severa (la cual consideramos pertinente) de los cuerpos del orden francés. En materia delictual, el tribunal competente, son los

Tribunales Franceses, esto en virtud de los artículos 689 del Código de Procedimiento Penal y 113-2 del Código Penal francés. Esto, relacionado al lugar donde se produjo o puede producirse el hecho dañoso. Sin embargo, en la Internet, el hecho dañino puede producirse **en todos los lugares** en que la información se ha puesto a disposición de los usuarios de la Internet.

En consecuencia, la víctima de *cyberbullying*, en Francia, puede presentar el caso ante el tribunal de su elección:

- El tribunal del lugar donde vive el acusado;
- La jurisdicción del lugar del hecho dañoso o la jurisdicción en la que se haya sufrido el daño.

Para el Tribunal de Justicia de la Unión Europea- **TJUE** "el criterio de materialización del daño [...] confiere competencia a los tribunales de cada Estado miembro en cuyo territorio el contenido publicado en línea y accesible o ha sido accesible".

Las víctimas de *cyberbullying* no sólo podrán llevar su caso a los tribunales franceses, sino que también podrán recurrir a la legislación francesa, aunque los artículos o comentarios ofensivos **no estén escritos en francés.**

La Ley Avia: ¿Salvaguarda o Problemática?

Y aquí hace su entrada, la ley Avia ¿una luz de esperanza en Francia? Para muchos, representa a la diosa Temis, protectora de la justicia; sin embargo para el Consejo Constitucional, no. Este, censuró gran parte de su contenido.

Recordemos que en Francia, la noción de blasfemia fue eliminada de su legislación por la ley del 29 de julio de 1881 sobre la libertad de prensa. Además, en Francia por ejemplo se puede insultar a una religión, sus figuras y símbolos, pero está prohibido insultar a los seguidores de una religión.

La ley del 24 de junio de 2020 creada para combatir el contenido de odio en la Internet, conocida como "ley Avia", fue un proyecto de ley presentado por la diputada Laetitia Avia. Es una ley francesa, de inspiración alemana. Específicamente la ley: **Netzwerkdurchsetzungsgesetz - NetzDG** para abreviar, la cual obliga a las mayores redes sociales, aquellas con más de dos millones de usuarios alemanes, a acabar con el discurso de odio "descaradamente ilegal" dentro de las 24 horas de ser reportado. Ambas muy criticadas, ya que para muchas organizaciones y juristas representan un peligro para la libertad de expresión.

No podemos atacar en stricto sensu, el tema del *cyberbullying* en un solo artículo. . Ni las mentes más iluminadas del derecho de la Unión europea han podido llegar a un consenso para luchar contra este terrible fenómeno. Pero trataremos, de presentar algunas recomendaciones para dar inicio a pasos más firmes para combatir esta problemática.

- Es necesario asegurarse que las conductas del ciberacoso y cyberbullying se constituyan claramente, como **delitos tecnológicos, donde se debe** distinguir la opinión de una persona y los comentarios ofensivos que su único objetivo es denigrar y hacer daño a otra persona. Ojo con el "derecho a la blasfemia" como está integrado en el espacio europeo.

- Existen plataformas dentro de la UE, que muchos no conocen que están ya trabajando para aconsejar y educar a padres e hijos en este tema. e.g. The EU's network of Safer Internet, Hans Martens es el Director del programa: **EU Insafe Network of Safer Internet Centres**.
- La creación de una guía (interactiva, online) de actuación que pueda orientar a los padres, tutores, menores y centros educativos.

Proveer al menor de edad (niños y adolescentes) con charlas, talleres, eventos y que se incluya como contenido dentro del programa escolar, dándoles a conocer las ventajas y desventajas de las TIC, así, como sus consecuencias.

Como primera conclusión a nuestras premisas desarrolladas, podemos resaltar que la intención de colocar el reflector hacia el cyberbullying, es que las voces de las víctimas se escuchen. Se debe educar a la población, para que se conviertan en "whistleblowers" i.e. denunciantes informados, cuando sean espectadores de *cyberbullying*. Al momento, no podemos asegurar si el cyberbullying seguirá creciendo, pero los estudios recientes demuestran que probablemente si.

"Sólo hace falta un clic, para arruinar la vida de un niño/a"

Bibliografía

Avocats, Cahen Murielle (Marzo 2016) Le Cyberharcèlement Moral. Recuperado de: https://www.murielle-cahen.com/publications/cyber-harcelement.asp

Colosimo, Anastasia (Noviembre 2018) Le blasphème en France et en Europe : droit ou délit ? Entrevista. Recuperado de: https://www.institutmontaigne.org/blog/le-blaspheme-en-france-et-en-europe-droit-ou-delit

Consejo de Europa (2001a). Convenio sobre la ciberdelincuencia. Informe explicativo. Serie de tratados europeos (185), Budapest. Recuperado de: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403

Consejo de Europa (2001b). Convenio sobre la ciberdelincuencia. Serie de tratados europeos (185), Budapest. Recuperado de: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=-09000016802fa41c

Código Penal de España (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal).

Código Penal Francés (Art. 113-2) Recuperado de: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006417187&cidTexte=LEGITEXT000006070719&dateTexte=19940301

Código de Procedimiento Penal Francés (Art. 689) Recuperado de: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006577249&cidTexte=LEGITEXT000006071154&dateTexte=19811111

Cyber Security News (Junio 2020) Ciberacoso y Cyberbullying. Recuperado en: cybersecuritynews.es

European Commission (Mayo 2020) Safer Internet Centers. Recuperado de: https://ec.europa.eu/digital-single-market/en/safer-internet-centres

EUR-LEX (Mayo 2020) El Reglamento General de Protección de Datos-RGPD (2016/679). Recuperado de: https://eur-lex.europa.eu/legal

Flores J (Abril, 2008). Ciberbullying. Guía rápida. Descargado el 13 de septiembre de 2010 de http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/ciberbullying-guia-rapida.shtm.

France Tv Info (Enero 2020) Affaire Mila. Recuperado en: https://www.francetvinfo.fr/societe/religion/religion-laicite/affaire-mila-on-vous-raconte-l-histoire-de-cette-lyceenne-descolarisee-apres-avoir-recu-des-menaces-de-mort-pour-ses-propos-sur-l-islam_3813029.html

INTECO Y ORANGE 2010 (Abril 2020) Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles. Recuperado de : http://www.pantallasamigas.net/pdf/estudio_sobre_seguridad_y_privacidad_en_el_uso_de_los_servicios_moviles_por_los_menores_espanoles.pdf.

Legifrance (Junio 2020) Loi AVIA N° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet. Recuperado de: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000042031970&dateTexte=&categorieLien=id y http://www.assemblee-

nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet

Kowalski, R., Limber, S. y Agatston, P. (2010). Cyber Bullying: El acoso escolar en la era digital. Bilbao: Desclée de Brower. (Original publicado en 2008).

Méndez Rodríguez, L. (s.f.). Las nuevas caras de la ciberdelincuencia . *Las nuevas caras de la ciberdelincuencia .* Universidad Camilo JosÉ Cela , Madrid .

Olweus, D. (1970) Conducta de acoso y amenazas entre escolares. Madrid: Morata. Recuperado de: https://books.google.com.co/books?id=S0wSk71uQz0C&printsec=frontcover&hl=es#v=onepage&q&f=false

Parlamento Europeo (Junio 2020) The Policy Department for Citizen's Rights and Constitutional Affairs (2016) Cyberbullying among young people. Recuperado de: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Serrano, Angela (2013) Indicadores para Detectar el Ciberbullying. Directora del Máster en Resolución de Conflictos en el Aula UCV “San Vicente Mártir”. Recuperado de: https://online.ucv.es/resolucion/detectar-el-ciberbullying/

Smith (1991) The Silent Nightmare: Bullying and Victimization in School Peer Groups. Paper. London: Annual Congress British Psychological Society. Recuperado de: https://www.researchgate.net/profile/Peter_Smith34/publication/284679049_The_silent_nightmare_Bullying_and_victimization_in_school_peer_groups/links/59fb24e9aca272347a1d0f1e/The-silent-nightmare-Bullying-and-victimization-in-school-peer-groups.pdf

Velasco Núñez, E. (2010). Delitos Cometidos a través del Internet

PRIVACIDAD HACKEADA: BIG DATA EN LA VIDA COTIDIANA Y EL USO DE DATOS PERSONALES EN LOS MEDIOS DE LA TECNOLOGÍA.

William Lima Rocha

31

Nos proponemos abordar discusiones sobre privacidad y el uso de datos personales en los medios de la tecnología o el ciberespacio, que permite acceder a oportunidades rápidas entre el registro de la información y el tiempo para llegar a ella, conduciendo a la búsqueda de una adecuada exposición de ideas y la elaboración de debates sobre la insatisfacción o inseguridad de la vigilancia y el control. sociales, como barreras en el acceso a la información, violación de la privacidad, al darse cuenta de que el escenario tecnológico actual es un gran activo para llegar a la información.

Hay una distinción entre privacidad y datos personales. Sin embargo, sí resulta conveniente aclarar que en Europa, el derecho a la protección de los datos personales tiene reconocimiento legal como derecho distinto al derecho a la privacidad. Varias constituciones nacionales contienen previsiones distintivas en este sentido y, más aún, la Carta de los Derechos Fundamentales de la Unión Europea, adoptada el 7 de diciembre de 2000, establece una clara distinción entre uno y otro derecho. Mientras que el artículo siete consagra el derecho la vida privada y familiar, el artículo ocho reconoce que toda persona tiene

[31] Autor: William Lima Rocha - william.rocha@globo.com | https://www.linkedin.com/in/william-rocha-b487654/ Estudiante de Doctorado en Ciencias Jurídicas - UCA (Universidad Católica Argentina), Magíster en Derecho Económico Empresarial - UCA (Universidad Católica Argentina). Especialista con MBA en Derecho del Consumidor y de la Competencia por la FGV / RJ. Miembro de la Comisión de Protección al Consumidor y de la Comisión de Protección de Datos y Privacidad de OAB / RJ. Socio de Terra Sarmento Rocha Advogados y Fiscal Adjunto del Registro Mercantil del Estado de Rio de Janeiro - JUCERJA).

derecho a la protección de los datos personales que le conciernan.[32]

Los efectos del derecho a la información no solo están contenidos en el ámbito de la legislación común, ya que este derecho se eleva al nivel de los derechos fundamentales. Por tanto, no concierne solo al orden privado de los sujetos, sino que irradia en la consideración pública del campo indisponible de la ciudadanía activa, según la concepción contemporánea que la ve no solo en el ejercicio del derecho frente al poder político, sino frente al poder económico.

La información se ha convertido en un activo legal esencial, para las vidas individuales más simples y para las empresas y naciones más poderosas. El progreso tecnológico crece, pero también lo hacen los peligros de la falta de respeto a los derechos humanos.

El acceso a Internet permite el ejercicio de varios derechos humanos fundamentales y se convierte en un elemento central en la formación de la ciudadanía de las personas. De hecho, el ejercicio de este derecho fundamental es el resultado de uno de los efectos de la globalización: el "acceso en tiempo real a la información disponible".

La búsqueda de información se vuelve adictiva y competitiva para la inclusión socio-digital, así como para demostrar poder y superposición en la red de relaciones.

La puesta a punto de la información en tiempo real, fenómeno de la globalización, implica conocimiento y deseo de productos, incluso antes de su distribución en el mercado, estimulando una demanda inmediata a ser satisfecha por la oferta resultante de la piratería, competencia desleal, comercio ilícito o consumo inconsciente.

Según Marco Schneider[33], "el gran arte, entonces, sería la purificación de lo no esencial, de lo accesorio, para centrar nuestra atención y sensibilidad en lo que, en el fondo mismo de la inmediatez, la trasciende". Purgar el deseo consumista de productos o de acceso a la información sería el gran tónico del uso consciente de mantener o no necesidades sociales.

Los medios digitales permiten que la acción social colectiva participe en debates que tienen como objetivo potenciar la conciencia ciudadana sobre los derechos sociales y civiles con identificación racional para el ejercicio del voto en la elección de líderes o entender el origen e interés de las normativas legales que nos afectan en la día a día.

El acceso a la información es un derecho fundamental, considerando

[32] Accesible en http://www.europarl.europa.eu/charter/pdf/text_es.pdf

[33] SCHNEIDER, Marco . A Captura do Gosto como inclusão social negativa: por uma atualização crítica da ética utilitarista. Sinais Sociais, v. 5, p. 82-109, 2011. 3 Accesible en: http://www.sesc.com.br/wps/wcm/connect/5254eb81-39a4-4a4b-bb92-6710645bf424/17.pdf?MOD=AJPERES&CACHEID=5254eb81-39a4-4a4b-bb92-6710645bf424

que es sumamente importante para los seres humanos, está íntimamente relacionado con la dignidad de la persona humana, el acceso a información de calidad actúa positivamente en la protección y desarrollo de toda la comunidad, contribuyendo a la realización y mejora de otros derechos. El acceso debe corresponder a la utilización de medios legítimos y ajustes al régimen de información.

El uso irrestricto de las redes sociales como plataformas digitales (Instagran, Twitter, Periscope, Facebook, Skype, LinkedIn, etc.) sirve para la autoexposición de los usuarios de la world wide web, en universos egocéntricos, como suele ocurrir sin análisis de costos, beneficio de la provisión de información, porque más que compartir enlaces e información personal y hacer nuevos amigos, las redes sociales funcionan como diarios virtuales en tiempo real. Publicaciones comunes de personas que narran la rutina diaria, se quejan del trabajo, muestran la ropa del día, la comida o muestran su ubicación: hechos o actos en el lugar de trabajo, gimnasio, universidad, hospital o en el club. Por no hablar de los variados "selfies" en aspectos sentimentales o de ostentación material o "belleza".

Netflix lanzó el documental "Privacidad Hackeada"[34] en su catálogo. La película echa un vistazo entre bastidores al escándalo que rodea a Cambridge Analytica, Facebook y la elección de Donald Trump en Estados Unidos.

El caso llamó la atención en todo el mundo cuando reveló que la compañía británica utilizó datos personales de los usuarios de Facebook para dibujar perfiles psicográficos de la población estadounidense y crear anuncios dirigidos a grupos de indecisos. Esta práctica habría tenido una influencia decisiva en la carrera electoral estadounidense (y de otros países).

El documental sigue la saga de David Carroll, profesor de la Parsons Schoolof Design de Nueva York, que decide luchar en los tribunales por sus datos. Al descubrir que su información (junto con la de más de 50 millones de usuarios) se utilizó para influir en las elecciones, recurre a la ley del Reino Unido para recuperar sus datos.

La historia también sigue el viaje de Carole Cadwalladr, periodista de The Guardian, quien investigó y publicitó el escándalo, y la ex empleada de Cambridge Analytica Brittany Kaiser, quien apareció en el parlamento inglés para denunciar todo el plan.

Los problemas de Cambridge Analytica comenzaron cuando su ex director de tecnología, Christopher Wylie, un canadiense, dijo a la prensa que la compañía había comprado datos de millones de usuarios de Facebook sin su consentimiento. Los datos se obtuvieron a través de una aplicación

[34] Accesible en: https://www.netflix.com/br/title/80117542

de perfil psicológico desarrollada por un investigador de la Universidad de Cambridge, explicó Wylie, y que permitió el acceso a la información no solo de quienes usaban la herramienta, sino también de sus amigos.

Según los informes, los datos recopilados se entregaron a Cambridge Analytica, incumpliendo los estándares de Facebook. Wylie informó que la información obtenida se utilizó para perfilar a los votantes y dirigirles propaganda política personalizada y noticias falsas. Esto les permitió, según Wylie, influir en las elecciones estadounidenses y, también, a través de empresas relacionadas, en otros procesos electorales, como el referéndum del Brexit.

El saldo final es de conocimiento público: además de perder alrededor de $ 50 mil millones en valor de mercado, Facebook ha pasado por una de las crisis de imagen más graves de su historia y se le ordenó pagar una multa de $ 5 mil millones por exponer datos de terceros.

La presión de la opinión pública llevó a Mark Zuckerberg a comprometerse con una serie de cambios en la política de privacidad de la red social (los resultados aún no han convencido a gran parte del mercado). Cambridge Analytica, mientras tanto, finalizó sus servicios en mayo del año pasado.

Más que una advertencia para los usuarios de plataformas digitales, “Privacy Hacked” refuerza los peligros de una afirmación que ya se ha convertido en una máxima del mundo digital: cuando el servicio es gratuito, los datos del consumidor suelen ser el producto final.

El fenómeno de big data (denominación genérica de todo lo que refiere a enormes cantidades de datos y su tratamiento), és una denominación que se utiliza para referirse a enormes cantidades de datos que pueden ser almacenados, unidos y analizados, trae consigo la posibilidad de encontrar información, tendências de consumo y conocimientos que no hubieran resultado óbvios y la toma de decisiones automatizadas mediante el uso de algoritmos.

El big data[35] retrata una nueva forma de capturar, analizar, almacenar, extraer valor de una gran cantidad de información, permitiendo, entre otros, la toma de decisiones automatizada, el aumento de la eficiencia empresarial y gubernamental, la creación de nuevos modelos de negocio y la generación de riqueza sustancial. además de ahorrar valiosos recursos[36].

[35]GOMES, Rodrigo Dias de Pinho. Big Data: Desafio à tutela da pessoa humana na sociedade da informação. 2ª. ed. Rio de Janeiro: Lumen Juris, 2019. p. 29.

[36]GOMES, Rodrigo Dias de Pinho. Big Data: Desafio à tutela da pessoa humana na sociedade da informação. 2ª. ed. Rio de Janeiro : Lumen Juris, 2019. p. 9.

Se pretende saber cómo se tiene el ciberespacio, que permite acceder a oportunidades rápidas entre el registro de la información y el tiempo para llegar a ella, lo que lleva a la búsqueda de una adecuada exposición de ideas y elaboración de debates sobre la insatisfacción o inseguridad de la vigilancia. y control social, como barreras de acceso a la información, violación de la intimidad, reconociendo que el escenario tecnológico actual es un gran activo para llegar a la información.

Con el debate sobre la democracia digital y el uso de la información en medios tecnológicos digitales, se espera comprender los aspectos sociales, culturales y políticos del régimen de la información, así como desarrollar la capacidad y competencia de información crítica. También busca verificar cuáles son los límites regulatorios de “internet” en cuanto a privacidad, acceso, neutralidad, vigilancia y seguridad.

Es necesario encontrar un equilibrio entre el acceso a la información, la regulación y los derechos existentes en la relación jurídica en cuanto a la recogida de datos masivos del interesado, realizando un juicio ponderado entre la autonomía de la voluntad y la libertad de contratar, traducido por el principio de libre iniciativa y el derecho a la intimidad y protección de los datos personales, cumpliendo la Protección de Datos un papel muy importante en este sentido.

2020

ELLOS SON EDI

EDI

APANDETEC
DERECHO Y NUEVAS TECNOLOGIAS

DIRECCIÓN NACIONAL
DE REGISTRO DE
DATOS
PÚBLICOS

ASOCIACIÓN DE
ESCRIBANOS DEL URUGUAY

"El gran motor del cambio es la tecnología".
Alvin Toffler

Nadie imaginó que este 2020, sería un año atípico, raro, distinto, un año que nos doblegó, nos puso de rodilla, hizo que pongamos a prueba nuestra fe y nos llevó a reevaluar todo, desde la vida personal, los negocios, la educación, la medicina, la angustia, la soledad, la excitación, la depresión, el desempleo y el surgimiento de nuevos modelos productivos. Un año que nos robó sueños, familiares, amigos y conocidos y nos obligó a pensar en cómo será nuestra revancha en el 2021.

Sin duda un año que hizo que nos reencontremos con nosotros mismos, con la familia que, aunque ahí estaba, la desconexión era tal que ya no nos conocíamos unos a otros y ahora, tuvimos que vernos nuevamente cara a cara, conversar, reencontrarnos y re- conocernos, pues quién hubiera pensado que este año que en el calendario chino es el año de la "Rata" sería tan digno de un calificativo similar.

COVID -19, nos llevó a parar el balón, levantar la mirada y observar la cancha, nos mostró que era momento de despertar, no fue la manera más sutil, pero a veces hace falta un fuerte sacudón para hacernos entrar en la realidad.

La principal medida adoptada fue el encierro, no ha sido fácil sobrellevarlo pero nos ha enseñado a recobrar la paciencia, a ser resilientes, a tener que aceptar esta nueva realidad y sobretodo nos llevó de cierta forma al pasado ya que tuvimos la necesidad de re aprender a comunicarnos cara a cara, suena raro, pero la tecnología nos ha hecho tan esclavos que habíamos olvidado lo que son las relaciones humanas, volver a sentir un abrazo, conversar alrededor de una mesa o simplemente sentir la calidez del hogar, de la familia junta y completa, eran cosas que hace mucho las habíamos dejado atrás por un mensaje de texto, un mensaje de whatsapp o simplemente una videollamada.

Mantenernos en casa no ha sido sencillo, hemos tenido que adaptarnos a nuevos hábitos, pero sin temor a equivocarme el golpe más duro ha sido el económico que muchas familias han tenido que soportar. Muchas compañías (grandes, medianas y pequeñas) se vieron en la necesidad de cerrar sus operaciones, era insostenible seguir operando sin que haya una dinámica económica fluida, otras empresas consideraron aplicar medidas alternativas como reducir jornadas y por tanto reducir salarios y sueldos y otras han tratado de sacarle provecho a la situación incorporando herramientas tecnológicas que les ha permitido seguir activas en el negocio.

Antes de vivir este confinamiento quizás muchas empresas y profesionales no veían la necesidad de implementar nuevas herramientas, sin embargo, la actual realidad los llevó a reevaluar y a caminar a pasos agigantados a una medida que consideraron muy lejana, otras actualizaron lo que ya disponían y otros simplemente se quedaron atrás.

Aplicaciones como Glovo, Rapi, Tipti han conseguido su BOOM, pues al no poder salir de casa y requerir abastecernos ha hecho que este tipo de negocios basados en aplicaciones móviles sean de inmensa ayuda ya no solo con productos de primera necesidad, sino también con temas de papelería, tecnología, regalos, ferretería entre otros, si bien es cierto, ya las restricciones han ido cambiado poco a poco y de cierta forma estamos retomando algunas actividades, los servicios de "delivery" se han ganado un lugar muy importante en la dinámica de la economía, y aunque si bien es cierto nada nos exime a no ser posibles candidatos de contagio, al menos tenemos una opción menos riesgosa que el salir de casa si no deseamos.

El confinamiento o cuarentena (mal llamada ya que hace rato sobrepasamos los 40 días de aislamiento) también tiene otra cara, y es que hoy más que nunca nuestra privacidad, intimidad e incluso manejo de nuestra información personal está más expuesta, el despegue de plataformas como Jitsu, Zoom, Teams, han hecho que sea más sencillo llevar a cabo algunas actividades laborales, académicas e incluso familiares y personales, pero al mismo tiempo han abierto un ventanal de vulnerabilidad, el trabajo, el colegio, la universidad entraron de lleno a la intimidad del hogar, no es raro ver a perro o gato caminando mientras estamos en una videollamada, o un niño gritando, o algún familiar que se cruza no siempre con sus mejores galas y es pues parte esta realidad, la invasión directa a nuestra vida familiar queda expuesta sin filtros.

Sumado a eso, tenemos también situaciones que preocupan, niños y jóvenes que se encuentran mas tiempo del habitual conectados a los distintos dispositivos, y no cabe duda que esto no ha sido "desatendido" por personas inescrupulosas, la exposición de los chicos a posibles situaciones de vulnerabilidad como el envío de videos o fotos haciendo ejercicios, a modo de tareas, que exponen de manera directa a los menores son algunas de las cosas que han llamado la atención, aunque

lo mas impactante ha sido escuchar comentarios de padres que aducen que no tiene importancia porque los menores “no están desnudos”, “es solo un deber”, “uy se quejan por todo”, esto, solo nos deja ver la poca información y el desconocimiento que aún existe alrededor del manejo de la tecnología y los riesgos que esta sugiere, ya que en algunos casos estamos entregando a niños y jóvenes en bandeja de plata a predadores que no pierden la menor oportunidad para atacar y sacar provecho.

En entorno laboral, con el teletrabajo también ha traído cola, el abuso con relación a las horas que exigen de trabajo las empresas a sus colaboradores y el uso de “amenazas” se ha vuelto un común denominador la presión psicológica con el uso de frases como “deberían ponerse la camiseta” “la empresa los necesita” “agradezcan que aún tienen trabajo”, ha sido la excusa perfecta para abusar en esta modalidad laboral, incluso olvidando el derecho que tienen sus colaboradores a la desconexión.

El campo del bienestar también ha buscado de alguna manera sostenerse, no ha sido fácil, pero han buscado la mejor forma de mantener sus actividades, para muchos fue difícil pararse frente a una cámara y empezar a dar clases, pero estos esfuerzos han sido bien recibidos por la gente que ha buscado una ruta de escape en estos nuevos modelos de acceso a diversas actividades y de esa forma cuidar su salud física, mental y emocional.

Como ya lo dijimos antes, esta nueva realidad ha impulsado al uso de herramientas tecnológicas incluso en sectores que se mantenían algo reacios a hacerlo, pero hasta los más necios tuvieron que adaptarse y eso le paso al sistema gubernamental, debido a que se vieron en la necesidad de poder garantizar el acceso a los usuarios a todos sus servicios.

Entornos como el legislativo y judicial han visto y palpado el gran beneficio que ha traído en especial el uso de firmas electrónicas, que si bien es cierto la norma existe del año 2002, tuvimos que esperar mas de 18 años para verla es en su pleno apogeo, y bueno al fin valió la pena que nos hayan tildado de locos en aquel entonces cuando proponíamos la ley (2002).

La tecnología llegó para quedarse e imponerse, pese a que poco a poco la restricción de quedarnos en casa se ha ido desvaneciendo será difícil volver atrás, muchos padres están están analizando opciones como “home schooling” o modalidades virtuales, para sus hijos, las empresas están re evaluando sus estructuras, y actividades, ya que dadas las pérdidas no será fácil volver a las jornadas completas y sueldos completos, por tanto mantener colaboradores bajo sistemas de teletrabajo puede resultar más beneficioso.

Hoy más que nunca nos damos cuenta que profesiones orientadas al desarrollo de aplicaciones, seguridad de la información, seguridad informática, análisis de big data, marketing digital, community manager, diseño, entre otras, han cobrado fuerza y muchos las han volteado a ver como una opción con visión ya no de futuro sino de

presente, ya que el futuro que nos piso los talones y como siempre nos tomó desprevenidos.

Todos sabemos que este 2020, será un año para recordar, evaluar, analizar y que se convertirá en una fuente inagotable de experiencias, tomar el aprendizaje que este proceso nos deja será la mejor herramienta para que podamos volver a flote en este próximo 2021, que en el calendario chino es el año del “Búfalo”, es decir, fuertes e imponentes. -

TOKENIZACIÓN DE ACCIONES EN LA LEY DE MODERNIZACIÓN A LA LEY DE COMPAÑÍAS DEL ECUADOR

Darío Echeverría Muñoz.

INTRODUCCIÓN

Antiguamente, los tokens consistían en fichas con un valor determinado que reemplazaba al dinero fiduciario en ciertas sociedades, quienes, con sus usos y costumbres, acordaban el intercambio de bienes y servicios.

En la actualidad, los avances tecnológicos han abierto un mundo de posibilidades para brindar mayores facilidades en nuestras labores diarias, dentro de estos desarrollos está la tecnología de la cadena de bloques (*blockchain*) en principio concebida para soportar las criptomonedas, y consiste en una base de datos descentralizada con un registro único, consensuado y distribuido en varios nodos de la red. De esta forma, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores para crear un nuevo tipo de bases de datos.

Su creciente interés ha permitido emular de forma eficiente el funcionamiento del dinero digital, para en lo posterior ser utilizado con otros propósitos acreditativos, es así como el token en la actualidad consiste en la representación digital de un valor emitido por una entidad pública o privada que funge como unidad de medida y reserva de valor para su intercambio y transacción.

TIPOS DE TOKEN

A pesar de que hay una serie de diferentes modelos de tokens esparcidos en el mundo y con distintos nombres que se refieren a lo mismo, estos son agrupados en tres categorías principales:

- ***Security tokens:*** consisten en valores digitales cuyo contenido esencialmente económico proporciona derechos y obligaciones respecto de los activos que tienen como fuente subyacente, entre estos se ubican las acciones, instrumentos de deuda entre otros.

- ***Utility tokens:*** estos activos digitales conceden a sus titulares acceso a un producto o servicio con la finalidad de obtener beneficios económicos. Está orientado a ofrecer una utilidad concreta en una plataforma o aplicación, otorgando derechos de uso o goce en determinados proyectos.
- ***Payment Tokens:*** o tokens de pago, se utilizan como un medio de pago e intercambio alternativo. A diferencia de las monedas fiduciarias tradicionales como el dólar estadounidense, el euro o el yen japonés, no son de curso legal y carecen de respaldo gubernamental, ya que su principal objetivo es ser una herramienta descentralizada para la compraventa de bienes y servicios sin intermediarios tradicionales, el ejemplo más característico de este token es el bitcoin.

TOKENS EN ECUADOR

El éxito del token ha permitido que sus distintos usos logren adaptarse a las necesidades actuales que su estructura permite implementar, es así como en Ecuador la Disposición General Cuarta de la reciente expedición de la Ley de modernización a la Ley de Compañías, estipula[37]:

> *«Las acciones de una compañía anónima o de una sociedad por acciones simplificada podrán estar representadas por certificados tokenizados. Las demás especies societarias no podrán representar sus acciones, participaciones o cuotas sociales en certificados tokenizados.*
> *Para los efectos de esta Disposición General, se entenderá como certificado tokenizado a la representación de las acciones en un formato electrónico que cumpla con las siguientes condiciones:*
> *a) Que la información se encuentre organizada en una cadena de bloques o en cualquier otra red de distribución de datos o tecnología de registro y archivo de información virtual, segura y verificable; y,*
> *b) Que la información verificada a un certificado tokenizado pueda ser transferida electrónicamente.*
> *El tenedor del certificado tokenizado podrá transferirlo a una tercera persona. La notificación de la cesión de un certificado tokenizado deberá ser enviada a la correspondiente red de distribución de datos que hubiere sido implementada para la emisión de los mencionados certificados tokenizados. Esta notificación será efectuada por el cesionario al representante legal, para lo cual utilizará su firma de red.*
> *Para los efectos previstos en esta Disposición General, se*

[37] (Ley de modernización a la Ley de Compañías, 2020)

entenderá como una firma de red a una cadena de caracteres alfanuméricos que, al ser transmitida por el remitente a la correspondiente red de distribución de datos u otra tecnología de registro y archivo de visualización virtual, propone garantías razonables al receptor acerca de la posesión del remitente de la llave criptográfica asimétrica, asociada con la red de distribución, que proteja la identidad digital de su portador.

Se entenderá como cadena de bloques o blockchain a la tecnología de registro y archivo virtual que organiza los datos de los bloques encadenados cronológicamente por una función algorítmica encriptada y confirmada por un mecanismo de consenso. Esta tecnología será distribuida y confirmada por un mecanismo de consenso. Esta tecnología será distribuida, encriptada y verificable en tiempo real. Una vez agregada la información, los registros de la cadena de bloques serán inmutables.

A pesar de su validez interpartes, la transferencia de un certificado tokenizado surtirá efecto contra la compañía y terceros a partir de su inscripción en el Libro de Acciones y Accionistas organizado en una cadena de bloques o cualquier otra red de distribución de datos o tecnología de registro y archivo de información virtual, segura y verificable.»

Esta disposición legal permite que las acciones ya no sean respaldadas solamente en certificados físicos, las compañías anónimas y las de sociedades por acciones simplificadas (SAS) tienen la potestad de implementar sistemas *blockchain* para respaldar la información de sus accionistas de forma virtual, segura y transparente.

Por otra parte, la ley expedida en su Disposición General Tercera otorga la potestad a que los libros sociales tengan respaldo electrónico o digital, esto para asegurar la información en un sistema viable que permita su distribución y resguardo a favor de la compañía.

Además, el Art. 2 de la Ley de Comercio Electrónica, Firma Electrónica y Mensajes de Datos[38], otorga validez jurídica a cualquier mensaje de datos con la misma calidad que un documento escrito con todos sus efectos legales.

Una de las características que la Disposición General Tercera de la Ley de modernización a la Ley de Compañías resalta para la implementación virtual de los libros

[38] (Ley de Comercio electrónico, firma electrónica y mensajes de datos, 2002)

de acciones y accionistas, es la equivalencia funcional, cuyo principio se sustenta en el Art. 5 bis de la Ley Modelo de la CNUDMI sobre Comercio Electrónico[39]:

> *«No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.»*

Este importante principio consiste en atribuir eficacia jurídica o mismo valor legal a los mensajes de datos, documentos y firmas electrónicas que la ley consagra para los documentos escritos, esto implica en trasladar la funcionalidad tradicional a los medios electrónicos o virtuales con la finalidad de resguardar la seguridad de las partes ofreciendo confianza, seguridad y transparencia.

Es decir que las acciones implementadas por medio del *blockchain* o cualquier tecnología telemática, deben guardar concordancia con el sustento físico que le otorga valor jurídico para su correcto desenvolvimiento, por ende, las acciones deben contener los requisitos mínimos que estipula la Ley de Compañías en su Art. 176[40]:

> *«Los títulos de acción estarán escritos en idioma castellano y contendrán las siguientes declaraciones:*
> *1. El nombre y domicilio principal de la compañía;*
> *2. La cifra representativa del capital autorizado, capital suscrito y el número de acciones en que se divide el capital suscrito;*
> *3. El número de orden de la acción y del título, si éste representa varias acciones, y la clase a que pertenece;*
> *4. La fecha de la escritura de constitución de la compañía, la notaría en la que se la otorgó y la fecha de inscripción en el Registro Mercantil, con la indicación del tomo, folio y número;*
> *5. La indicación del nombre del propietario de las acciones;*
> *6. Si la acción es ordinaria o preferida y, en este caso, el objeto de la preferencia;*
> *7. La fecha de expedición del título; y,8. La firma de la persona o personas autorizadas.»*

Por último, en el ámbito del mercado de valores, el avance tecnológico ya tuvo su efecto por escrito desde el año 1993; y actualmente conforme lo dispone el Libro 2 del Código Orgánico Monetario y Financiero: “Ley de Mercado de Valores”, cuando las acciones son negociables en el mercado bursátil, sus títulos deben ser desmaterializados, esto consiste en

[39] (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 1996). Pág. 5

[40] (Ley de Compañías, 1999)

la sustitución del soporte físico por anotaciones en cuenta, las cuales poseen la misma naturaleza y conllevan en sí, todos los derechos, obligaciones, condiciones y otras disposiciones que contienen las acciones en soporte cartular.

El sistema de anotación en cuenta corresponde a un conjunto de normas y principios contenidos en la Ley de Mercado de Valores y la normativa secundaria expedida por la Junta de Política y Regulación Monetaria y Financiera, que otorgan sustento legal y rigen la representación, registro y circulación de valores negociables a través de notas contables electrónicas, siempre bajo la custodia, administración y gestión de una entidad autorizada a brindar estos servicios el cual le corresponde al Depósito Centralizado de Compensación y Liquidación de Valores.

En este último caso, asegurar la transferencia y negociación de las acciones tokenizadas por medio de anotaciones en cuenta, es otro reto susceptible de debate jurídico, financiero y operativo para determinar si otros títulos valor son sujetos de ser tokenizados, y si su procedimiento de negociación debe ser implementado conforme las directrices que varios organismos han establecido para el caso de las STO (*Security Token Offering*) o ICO (*Initial Coin Offering*) además de sus posibles efectos y viabilidad dentro del mercado de valores.

Por lo pronto con lo establecido en la Disposición General Cuarta antes citada, el Ecuador se convierte en uno de los pocos países que ha incorporado una norma viable para implementar por medio del *blockchain*, un soporte seguro, eficiente y transparente para custodiar, transferir y administrar la información de sus accionistas, además de facilitar su transferencia e identificación ágil segura y sistematizada, además de soportarse a la vanguardia tecnológica legal que el mundo ha implementado en estos últimos años.

2020

ELLOS SON EDI

EDI

ASADETICS

Asociación salvadoreña de derecho de las nuevas tecnologías

JURISTAS

adiar

Una asociación en todo el país

ABOGADO DIGITAL.TV

HONDURAS Cibersegura

OGDI.ORG

Observatorio Guatemalteco de Delitos Informáticos

Conciencia en Red

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

ELDERECHOINFORMATICO.COM

LOS DESTACADOS DEL AÑO 2021

Abogado/a - Organización - Cuenta en red social - Aporte académico - Informatico/a - Joven promesa - Campaña de concientización

La RED

EDI

CAMPAÑAS DE CONCIENTIZACIÓN

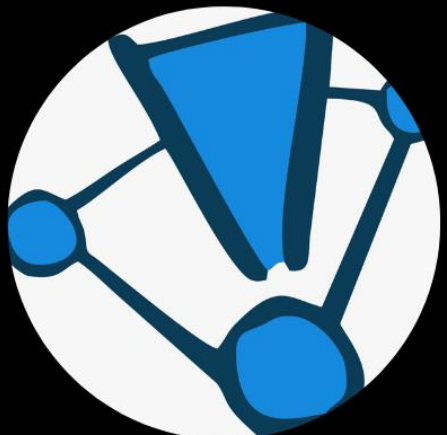
DESTACADAS EDI 2021

#MisDatosSoyYo

Mamá en Linea

16 días contra la violencia de genero digital

Grooming Argentina



Conciencia en Red

EDI

JOVEN PROMESA

DESTACADOS/AS EDI 2021

Mónica Velazco
El Salvador

José Vega Sacasa
Panamá

Ana Lambrecht
Argentina

Jorge Litvin
Argentina

David Oliva
Bolivia

Rodolfo Guerrero Martínez
México

EDI

Organismo/Institución

DESTACADOS EDI 2021

APPIF
Panamá

APANDETEC
Panamá

A.M.D.I
México

O.C.E.D.IC
Argentina

Defensoría del
Pueblo C.A.B.A
Argentina

EDI

Cuentas en redes sociales

DESTACADOS/AS EDI 2021

@Cibercrimen

COFFEE LAW
COMPARTIENDO IDEAS

Coffe Law

@oea_cyber

ORGANIZACION DE LOS ESTADOS AMERICANOS
Cyber
Más derechos para más gente

@identidadrobada

@infolabmdq

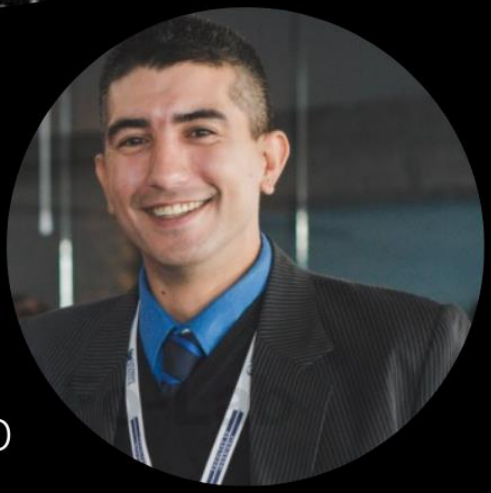
EDI

INFORMÁTICO/A

DESTACADOS/AS EDI 2021

Carlos Seisdedos
España

Romina Sejas
Argentina



Marcelo Romero
Argentina

Andrés Velazquez
México

Marcela Pallero
Argentina

Roberto Lemaitre
Picado
Costa Rica

EDI

Aporte académico

DESTACADOS/AS EDI 2021

Pablo Palazzi
Argentina

Sandy Palma
Martinez
Honduras

Ana D´iorio
Argentina

Karen Céspedes
Babilón
Perú

José Vega Sacasa
Panamá

EDI

Abogados/as

DESTACADOS/AS EDI 2021

Lorena Donoso
Chile

Rodrigo Iglesias
Argentina

Daniel López
Carballo
España

Daniela Dupuy
Argentina

Martín
Leguizamon
Argentina

José Vega Gallardo
Panamá

SOMOS LA RED

VAMOS DEJANDO HUELLA

ELDERECHOINFORMATICO.COM

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

LA RED

somos

ELDERECHOINFORMATICO.COM