EDI

Revista Digital -Diciembre 2021

Los Destacados EDI

Foto de tapa: Ivana Ramirez

-La espera-

2022

Edición n° 39 - Distribución gratuita

EDI

06.2022
CÓRDOBA –
ARGENTINA

Feria/Encuentro Internacional de derecho digital

TALLERES, NEGOCIACIÓN Y ANALISIS DEL DERECHO TECNOLOGICO

elderechoinformatico.com

EDICIÓN N° 39
DICIEMBRE 2022

ÍNDICE


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

EDITORIAL

Adiós 2021, siendo honesto no se si te vamos a extrañar, por mi lado, no mucho, bah, nada, no fuiste peor que el 2020, pero para eso no hace falta mucho mérito, así que tampoco es para que lo festejes tanto.

Se fue un año, donde perdimos amigos, tiempos, viajes, salidas, paciencia, ganas, momentos, oportunidades, esperanzas, y ganamos todo eso que perdimos (no voy a repetirlo),. Se fue el 2021, y preferiría recordarlo como el año antes de volver a lo que nos hacía bien. La Red EDI lo está pleneando empezando con un mega evento en el mes de Junio en la provincia de Córdoba / Argentina, una Feria y conferencias de los profesionales más reconocidos de Latinoamérica, Vamos a estar presentes con los Webinars y Conversatorios de siempre, la 2da edición de nuestra colección de Libros para Editorial Hammurabi, otro congreso presencial en el segundo semestre, convenios con Universidades para lanzar diplomados y cursos de actualización, van a conocer EDI Future....

Casi podría copiar y pegar editoriales de años anteriores, porque seguimos haciendo cosas después de 12 años, seguimos buscando marcar una diferencia, crecer, mejorar, compartir, llegar más lejos y más cerca,

Por último, nuevamente les acercamos este reconocimiento que denominamos **LOS DESTACADOS EDI**, su elección no es indiscutible, aunque si dundada, procuramos hacer un mimo a quienes consideramos han hecho méritos, ¿hay otros? Si los hay, pero en esta oportunidad no les tocó.

Se fue el 2021, cosas mejores vendrán, con seguridad, en ellas los esperamos.

Guillermo M Zamora
Director EDI

librería | hammurabi

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

en preparación

Colección «elderechoinformático.com»

11 volúmenes

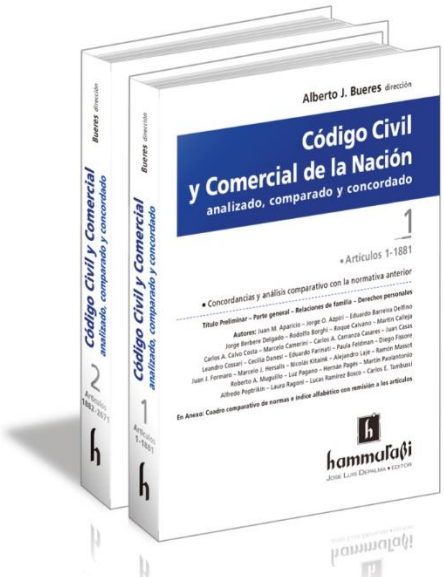
Guillermo M. Zamora dirección

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

Novedad

Código Civil y Comercial de la Nación

analizado, comparado y concordado



Alberto J. Bueres dirección

2 tomos | Artículos 1 - 2671

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

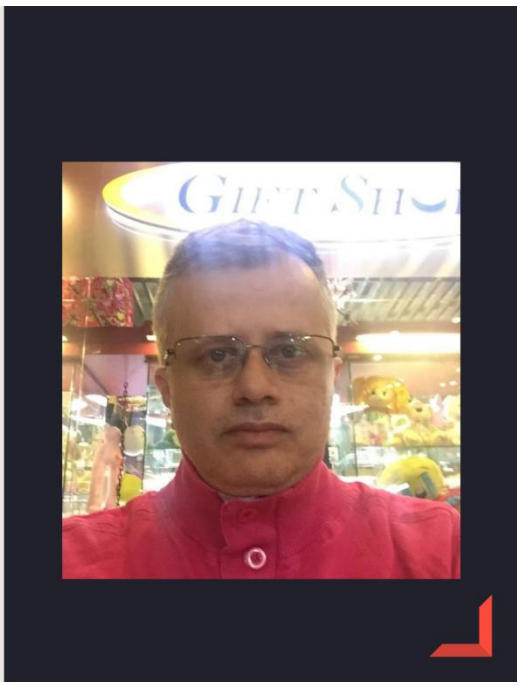
Contiene: Cuadro comparativo de normas. Indice alfabético de voces

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

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

Bienes intangibles y su protección

LUIS FERNANDO PÉREZ ANGARITA



Desde hace casi tres décadas empieza a cobrar relevancia el tema de activos intangibles, y así se evidencia en la normatividad que se empieza a generar tanto a nivel nacional como internacional.

A nivel nacional en el artículo 66 del Decreto 2649 de 1993 (Colombia) se introduce la definición de activo intangible. El código civil colombiano clasifica las cosas en cosas materiales e inmateriales. Incluso también se evidencia temas como el derecho a la propiedad intelectual, el cual solo recae sobre bienes intangibles e inmateriales (bienes intelectuales), sin embargo, este tipo de propiedad comparte cosas similares con la propiedad común en cuanto a su goce, uso y disposición por parte del propietario. Se evidencia que la normatividad es derivada casi siempre de normatividad anterior relacionada con activos materiales, pero ajustada a lo intangible e inmaterial. Así va a suceder con toda la normatividad vigente que rige este tipo de activos de los que este artículo aborda.

A nivel internacional, el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio[1], más conocido por sus siglas ADPIC o TRIP's, firmado en 1994 durante la Ronda de Uruguay del GATT, uniformó los estándares básicos de protección de estos bienes,

[1] Este acuerdo ha sido firmado por la mayoría de países del mundo.

reconociendo las cuatro categorías o formas fundamentales de protección: derechos de autor, patentes, secretos comerciales y marcas[2]. En septiembre de 1998 el Comité de Normas Internacionales de Contabilidad genera una norma (esta norma había sustituido a la NIC 9 Costos de Investigación y Desarrollo, que había sido emitida en 1993, la cual reemplazaba su versión anterior denominada Contabilidad de las Actividades de Investigación y Desarrollo que había sido emitida en julio de 1978.), la cual es adoptada en abril de 2001 por el Consejo de Normas Internacionales de Contabilidad con la NIC 38 - Activos Intangibles.

Definiciones de activo intangible:

El artículo 66 del Decreto 2649 de 1993, reglamentario del Código del comercio, definió el contenido y alcance de los bienes intangibles de la siguiente manera:

"*Art. 66. Activos intangibles. Son activos intangibles los recursos obtenidos por un ente económico que, careciendo de naturaleza material, implican un derecho o privilegio oponible a terceros, distinto de los derivados de otros activos, de cuyo ejercicio o explotación pueden obtenerse beneficios económicos en varios períodos determinables, tales como patentes, marcas, derechos de autor, crédito mercantil, franquicias, así como los derechos derivados de bienes entregados en fiducia mercantil*

Para reconocer la contribución de los activos intangibles a la generación del ingreso, se deben amortizar de manera sistemática durante su vida útil. (…)"

Ahora es pertinente reseñar también lo consignado en las Normas Internacionales de Contabilidad, relacionado con los bienes intangibles:

La NIC 38 – Activos Intangibles – define que un activo intangible es un activo identificable, de carácter no monetario y sin apariencia física. De acuerdo con esta misma norma, los atributos que debe cumplir un activo intangible son: ser identificable, el control de los beneficios económicos futuros por parte de la entidad y la generación de tales beneficios económicos incluye ingresos ordinarios por ventas de productos y servicios, ahorros de costos y otros rendimientos diferentes (párrafos 9 -17). Un activo intangible debería ser reconocido siempre que sea probable que los beneficios

[2] https://delitosinformaticos.com/07/2008/noticias/la-proteccion-juridica-de-los-activos-intangibles-en-las-empresas-de-ti

económicos futuros esperados que sean atribuibles al activo fluyan hacia la empresa, y el costo del activo puede ser medido confiablemente (párrafo 21).

Las NIIF (Normas Internacionales de la Información Financiera) definen al bien intangible como un recurso originado como resultado de eventos pasados, y del cual se espera fluyan beneficios económicos futuros. Los intangibles son activos no monetarios, y representan generalmente derechos abstractos, como puede ser una patente, una licencia de uso, una franquicia, una imagen de marca, la forma de hacer algo (know-how), entre otros[3].

Vida útil de los intangibles:

Dentro de las NIC se establecen parámetros sobre la vida útil de un activo intangible en los párrafos 88 y 89 donde se establece lo siguiente:

"*88. Una entidad evaluará si la vida útil de un activo intangible es finita o indefinida y, si es finita, evaluará la duración o el número de unidades productivas u otras similares que constituyan su vida útil. La entidad considerará que un activo intangible tiene una vida útil indefinida cuando, sobre la base de un análisis de todos los factores relevantes, no exista un límite previsible al periodo a lo largo del cual se espera que el activo genere entradas de flujos netos de efectivo para la entidad.*

89. La contabilización de un activo intangible se basa en su vida útil. Un activo intangible con una vida útil finita se amortiza (véanse los párrafos 97 a 106), mientras que un activo intangible con una vida útil indefinida no se amortiza (…)""

Las NIIF (Normas Internacionales de la Información Financiera) también hablan del tiempo de vida útil de los intangibles, y lo definen como el periodo de tiempo durante el cual se espera que contribuya a generar ingresos o beneficios para la persona y/o empresa. Cuando la vida útil no se puede determinar, se considera indefinida[4].

Medición y Evaluación de Intangibles:

La forma como se miden los activos intangibles depende del interés particular, y dependiendo de la forma existen diferentes modelos a emplear (Navegador skandia, valor agregado económico, monitor de activos intangibles, índice de capital

[3] https://www.gerencie.com/activos-intangibles.html

[4] https://www.gerencie.com/activos-intangibles.html

intelectual, metodología del valor concluyente), de los cuales no me adentraré en explicar cada uno ya que no es relevante para el propósito de este documento[5].

Los métodos de evaluación de los intangibles son: capital intelectual directo (Estima el valor financiero del activo intangible global a partir de cada uno de sus componentes), capitalización del mercado (Calculo de la diferencia entre la capitalización del mercado de una empresa y el valor de sus activos tangibles, siendo dicha diferencia el valor de los activos intangibles), y retorno sobre activos (el promedio de los beneficios antes de impuestos en un periodo es dividido por el promedio de activos tangibles, el resultado es el ROA el cual es comparado con el promedio de industria, la diferencia es el porcentaje generado por los intangibles)[6].

Luego de esta breve introducción y dejando en claro definiciones, conceptos, y mostrando como nace toda esta normatividad, revisemos ahora la normatividad actual en cuanto a la protección de los bienes intangibles.

Hay que tener en cuenta que toda creación intelectual original de naturaleza artística, científica o literaria, susceptible de ser divulgada o reproducida de cualquier forma tiene protección de derechos de autor, y sobre la misma recaen derechos morales y patrimoniales.

Donde ha cobrado alta relevancia la protección de activos intangibles es en empresas de TI, debido al crecimiento acelerado de emprendimientos (empresas de software y servicios informáticos), que ha hecho necesaria la protección de estos, y que se vea como una necesidad el desarrollo de legislación como estrategia de protección de los bienes intangibles o inmateriales.

Los activos intangibles más importantes en empresas de TI son el código fuente, el código objeto, las invenciones, las informaciones no divulgadas, el know-how, el conocimiento de los empleados, las bases de datos y los signos distintivos[7].

[5] https://www.gerencie.com/activos-intangibles.html
[6] https://www.gerencie.com/activos-intangibles.html
[7] https://delitosinformaticos.com/07/2008/noticias/la-proteccion-juridica-de-los-activos-intangibles-en-las-empresas-de-ti

Los intangibles de las empresas de TI actualmente cuentan con un régimen de protección especifico, con características propias, adecuado a las particularidades de cada intangible, y ha sido creada legislación propia en cada país que respalda esta protección.

Dentro de la legislación diseñada para tal fin, se protege el derecho de autor (o conocido también como copyright ©), los programas de computación y las bases de datos.

Derechos de autor, como se expresaba anteriormente en este mismo documento, se tiene sobre creaciones formales en el campo literario, artístico y científico; dicha protección abarca las expresiones mas no las ideas, y su protección empieza desde el mismo momento de la creación sin que haya necesidad de registro previo, y el tiempo mínimo de protección es de cincuenta (50) años. Bajo esta modalidad se está abarcando la protección de dos importante intangibles de las empresas de TI como son los programas de computación (programas fuente u objeto), y las bases de datos.

A pesar de que las ideas por si solas no se protegen, estas tienen un carácter de protección cuando originan una invención de un producto o de un procedimiento en cualquier campo de la tecnología y que cumplan con ciertas condiciones como son que sea algo novedoso, que constituya una actividad inventiva o que sea de utilidad o aplicación a nivel industrial. Cuando lo anterior ocurre se pueden proteger a través de legislación asociada a patentes. Su registro, si así se requiriera, tiene vigencia de veinte (20) años y no es prorrogable. Hay que resaltar que la mayoría de los países excluyen de este tipo de protección a los programas de computación.

Hay otros intangibles que no corresponden a formas de expresión ni invenciones pero que por su valor deben permanecer en secreto. Su protección no es abarcada como derechos de autor o patentes, y por tal razón requirieron un tipo de protección especial llamada secretos comerciales. Dicha protección dura mientras la información se mantenga en secreto. Dentro de esta categoría caben fórmulas, algoritmos, know how, métodos de organización interna, métodos de distribución, etc.

Dentro de los intangibles que tiene una persona o empresa, y que puede representar un elemento de gran valor es su reconocimiento a nivel comercial

mediante una marca, ya sea de su empresa, de sus productos o de sus servicios. Cualquiera de estas tres categorías puede tener asociada una marca, la cual hay que proteger legalmente ya que representa el reconocimiento de la empresa o bien, entre los diferentes clientes. El reconocimiento de una marca puede ser de un software, de un sistema operativo, de un producto, de un aplicativo entre otros, y está asociado a colores, tonalidades de estos, tipo de letra, entre otros símbolos. Por tal razón es importante tener en cuenta que las marcas deben registrarse ante los organismos creados para tal fin, con el objeto de protegerlas de un uso indebido, o uso sin autorización del dueño de esta.

Lo especificado anteriormente fue asociado a empresas de TI pero esto no quiere decir que solamente este sector cuente con activos o bienes intangibles. Hay muchos otros sectores de nuestra económica nacional y mundial que cuenta con este tipo de bienes, y para los cuales rige la misma reglamentación.

Muchas empresas fallan a la hora de valorar dichos bienes, y también de ejercer su protección apoyadas en mecanismos legales. Por ello es por lo que se ven temas como usurpación de marcas, robo de conocimiento, sin que ello represente muchas veces para los que usufructúan estos bienes un problema legal, precisamente por la falta de protección que ejerció el dueño o dueños originales del bien intangible.

Es evidente que la legislación actual, al ser elaborada, por personas con poco conocimiento del tema, ha sido realizada, y muchas veces adaptada de legislación internacional, sin tener en cuenta la realidad nacional. Por ello se encuentran vacíos, muchas veces, ocasionados por términos como el que se mencionó durante la clase cuando se habló de la palabra “normal” y de lo que ella podía significar.

Actualmente encontramos bienes intangibles que son gratuitos y los cuales no se les ha podido cuantificar su valor. Ejemplos de ello son Wikipedia, fotos personales almacenadas en Facebook, Google Maps, o videos que tenga una persona en YouTube. El problema de valorar estos activos es debido a que ninguno de estos sitios les cobra a los usuarios por su uso. Y así hay muchos otros ejemplos de bienes intangibles no valorados, no porque no se haya querido hacer sino porque no hay forma de hacerlo.

Otro campo donde los bienes intangibles son complejos de estimar su valor es el área de los seguros. Para el campo asegurador hay mucha discrepancia en que se puede asegurar y por qué valor, cuando de bienes intangibles se trata. Este es otro campo donde aún falta mucha claridad y normatividad al respecto.

Finalmente se evidencia que a pesar de los avances en materia legal, aún falta mucho camino por recorrer. El cambio ocasionado por la pandemia que viene afectando al mundo durante los dos últimos años ha hecho que mucha legislación sea revisada, y actualizada, y el tema de bienes intangibles es uno de los campos que se quedó rezagado. Hay una oportunidad única para que vean la importancia de poder valorar y proteger cosas inmateriales, pero también es evidente que para que esto suceda no solo se necesitan eventos como el vivido a causa de la pandemia, sino voluntad política de los gobiernos, y del organismo legislativo de cada país. Además, es necesario contar en el poder legislativo con personas idóneas para legislar al respecto.

No hay que perder la esperanza que se pueda avanzar en esta materia, y que se robustezca la legislación al respecto de los bienes inmateriales y su protección. Todo esto finalmente nos debe llevar a una legislación mundial unificada o si no es así por lo menos una legislación similar entre un país y otro que contribuya a la protección transnacional de este tipo de bienes.

SOMOS LA RED

VAMOS DEJANDO HUELLA

ELDERECHOINFORMATICO.COM

ANTECEDENTES

La raíz etimológica de la palabra arte, proviene del latín *ars – artis.* se refiere a la capacidad o habilidad para hacer algo, en concordancia a este concepto, la Real Academia de la Lengua Española lo define[8] como: *«Manifestación de la actividad humana mediante la cual se interpreta lo real o se plasma lo imaginado con recursos plásticos, lingüísticos o sonoros.»*

Exponer del arte, es hablar de la historia de la humanidad desde sus inicios teniendo una función ritual, mágica y religiosa; hasta la actualidad que tiene un fin comercial y de expresión hacia una determinada colectividad; esta forma de expresión se relaciona con el momento histórico vivido para cada civilización.

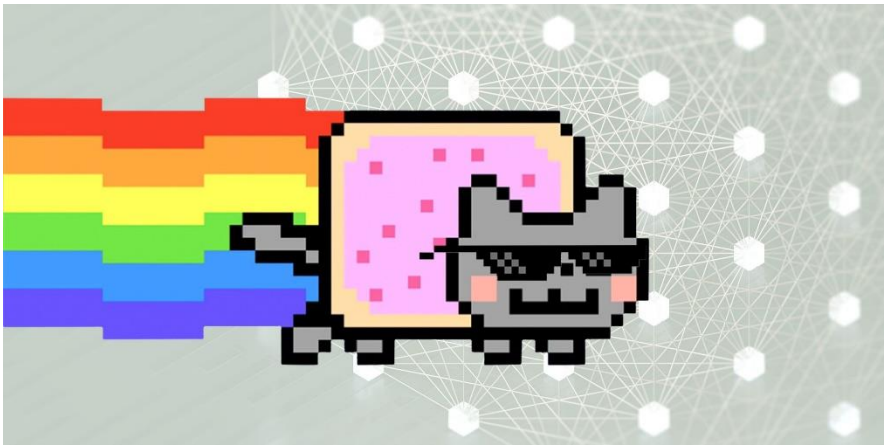
La clasificación del arte se remonta desde la Grecia antigua, distinguiéndolo en seis disciplinas: arquitectura (ej. *Parthenon* de Atenas), danza (ej. El cascanueces de Piotr Ilich Chaikovski), escultura (ej. David de Miguel Ángel), música (ej. Claro de Luna de Ludwig Van Beethoven), pintura (ej. La última cena de Leonardo da Vinci) y poesía (ej. Poema de Gilgamesh de los sumerios).

Con el desarrollo de nuevas técnicas y equipos de comunicación, surgieron otras disciplinas artísticas, entre ellas el llamado séptimo arte que se refiere al

[8] (Real Academia Española, 2021)

cine (ej. *Titanic* de James Cameron), el octavo arte en el que se cataloga a la fotografía, a pesar del debate que genera debido a que se lo considera como una extensión de la pintura, y en estas últimas décadas destacan también los videojuegos.

Sin embargo, los avances tecnológicos, permitieron nuevas formas de expresión y desarrollo para que la gente plasme sus ideas de formas que en años anteriores no hubiera sido posible concebir, y aquí es donde nace el **criptoarte.**



TOKENS FUNGIBLES Y NO FUNGIBLES

Para definir al criptoarte, es necesario citar el concepto de la tecnología que por detrás lo vuelve funcional, esto es la cadena de bloques (en adelante *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.

La información respaldada en la cadena de bloques se conoce como *token* y consiste en un bien intangible similar a una ficha, pero de tipo digital, emitido por una entidad privada descentralizada para un uso determinado.

Para fines de distinción, es necesario conceptualizar los *tokens* respecto de su transabilidad en el mercado:

- ***Tokens fungibles:*** es un activo digital intangible creado a partir de la tecnología *blockchain*, cuya característica consiste en ser sustituibles con el primer uso para ser intercambiables con otros de la misma calidad o naturaleza, tiene similitud con el concepto de bienes fungibles establecido en los códigos civiles de distintos países, el ejemplo característico para este tipo son las criptomonedas, específicamente *bitcoin*.

- ***Tokens no fungibles (NFTs):*** consisten en activos criptográficos creados mediante la tecnología *blockchain* que permiten representar objetos materiales o digitales, pero con la peculiaridad de que estos son de carácter único e irrepetible, lo cual hace que estos activos no sean intercambiables entre sí, dada su característica distintiva de los demás *tokens.*

CRIPTOARTE, CONCEPTO Y CARACTERÍSTICAS

Con los conceptos antes expuestos, se puede definir al critptoarte como una obra digital que puede o no ser materializada, la cual constituye un activo criptógrafico generado con la tecnología *blockchain* debidamente representado en un token no fungible (en adelante NFT).

La característica principal de este tipo de activos artísticos es que sus registros creados son únicos e inalterables, esto implica que su certificado de autenticidad tiene firma criptográfica, que lo vuelve original y le brinda al autor la seguridad de que no pueden reproducirse copias indiscriminadamente, porque su veracidad tiene un código único conocido como *hash.*

El *hash* es una función criptográfica que consiste en un algoritmo matemático que está programado para transformar la cadena de bloques, en una nueva serie de datos distinta a la de su origen, esto implica que cualquier cambio en el carácter por más mínimo que sea independientemente de su longitud, su valor resultante conlleva a una serie distinta al realizar la transacción, esto con la finalidad de evitar la falsificación o duplicidad de la información del bloque además de reforzar su seguridad, lo cual la hace irreversible.

Las ventajas que el criptoarte presenta son las siguientes:

- **Autenticidad:** los datos que se generan a través del criptoarte no pueden ser falsificados, ya que los mismos están en el registro descentralizado del *blockchain* por lo que puede ser verificada y comprobada su autoría, además que cada registro tiene el código *hash*, mismo que es único e irrepetible volviendo imposible su falsificación o duplicación.
- **Unicidad:** la pieza de criptoarte al ser un token no fungible, no existe otra de la misma calidad o naturaleza; a su

vez pueden crearse un número determinado de coleccionables que lo convierten en piezas digitales raras y únicas.

- **Seguridad:** a través de la criptografía se crea un sistema único programado para validar operaciones complejas y resolver conflictos propiciando que ningún tercero pueda modificarlas, y estas al ser transadas son irreversibles.
- **Transparencia:** mediante la tokenización de la obra, esta garantiza la propiedad y legitimidad a favor de su autor.

Sin embargo, a pesar de las bondades que el criptoarte presenta a favor de los artistas, no está exento de rechazo de algunos sectores y sus desventajas son:

- **Contaminación:** si bien existen beneficios económicos onerosos para quienes transan con criptoactivos, el proceso de minería conlleva a un exceso de electricidad que provoca daños colaterales en el ambiente, se estima que el proceso de minado por cada NFT, equivale a consumir la misma electricidad que usa una persona en Europa durante todo el mes[9], por lo que se analizan alternativas ecológicamente sustentables para evitar mayores perjuicios.
- **Especulación:** el mercado de criptoactivos se alimenta de las tendencias que rigen en ese momento, esto implica varios factores que coadyuvan a determinar el precio de una obra cripto como el nombre del artista, que tan conocido, el precio por centímetro cuadrado de la obra, su historial en ventas e influencia en el medio entre otros factores comparativos que determinan el precio a transarse.

El ejemplo más reciente de criptoarte, se dio el 11 de abril de 2021, en la casa de subastas *Christie´s* ubicada en Nueva York, el artista digital Mike Winklemann[10], conocido por el seudónimo *Beeple,* vendió su obra titulada *'Everydays: The First 5000 Days'*[11] bajo la suma de 69.3 millones de dólares, su obra consiste en el resultado de 5.000 imágenes que el creador ha elaborado diariamente a lo largo de los últimos 13 años, el tema de debate recae en como los NFTs

[9] https://www.eldiario.es/tecnologia/moda-nft-salirle-cara-planeta_1_7847137.html
[10] https://www.elpais.com.uy/vida-actual/nft-criptoarte-auge-mezcla-tecnologia-arte.html
[11] https://as.com/tikitakas/2021/04/07/portada/1617809057_730888.html

cambiarán drásticamente el mundo del arte y su formato autentificado mediante la tecnología *blockchain*.

MARCO JURÍDICO

El criptoarte como tal carece de regulación, en algunos países se ha logrado normar a las criptomonedas y al *blockchain* para desarrollar distintos proyectos por medio de su tokenización, lo que llevaría a que estas obras sean comercializadas libremente sin intermediarios.

Sin embargo, el criptoarte al ser una obra que tiene por detrás esfuerzo humano, se sujeta a la protección que la propiedad intelectual brinda a sus autores, para ello es necesario citar el Art. 2.1 del Convenio de Berna para la Protección de las Obras Literarias y Artísticas[12]:

> *«Los términos «obras literarias y artísticas» comprenden todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión, tales como los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con o sin letra; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía; las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresadas por procedimiento análogo a la fotografía; las obras de artes aplicadas; las ilustraciones, mapas, planos, croquis y obras plásticas relativos a la geografía, a la topografía, a la arquitectura o a las ciencias.»*

Mismo que fue ampliado en el Tratado de la OMPI sobre Derecho de Autor para los programas de ordenador, cuyo artículo 4 cita[13]:

> *«Los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2 del Convenio de Berna. Dicha protección se aplica a los*

[12] (Organización Mundial de Propiedad Intelectual - OMPI, 1979)

[13] (Organización Mundial de Propiedad Intelectual - OMPI, 1996)

programas de ordenador, cualquiera que sea su modo o forma de expresión.»

facilitaría su registro en las distintas organizaciones de protección de propiedad intelectual.

Mientras las ideas estén expresadas y

Al analizar la situación jurídica del criptoarte sobre la base de los artículos antes citados, existe una relación *sui generis* debido a que es un activo único que fusiona la expresión artística mediante el uso de la tecnología *blockchain*, porque al existir un respaldo único de una obra digital, nadie podría copiarla y alegar su autoría dadas las características que el NFT brinda para constatar la autoría y autenticidad.

Gracias a estos avances, la propiedad intelectual toma otro matiz de gran importancia ya que el derecho de autor de una obra determinada puede ser comprobado automáticamente y materializadas demostrándose esfuerzo humano, el derecho de autor del criptoarte está debidamente resguardado, con el elemento adicional del *blockchain* que brinda una característica criptográfica que lo vuelve una pieza única, rara y coleccionable que lo hace imposible de reproducirse ilícitamente.

Los NFTs son una revolución, la tecnología *blockchain* que los respalda ha cambiado las reglas en el mundo en distintos ámbitos creando matices interesantes, como en el arte, hoy en día que está no solo digitalizado, sino asegurado.

TRATAMIENTO DE DATOS PERSONALES EN LA NUBE CONFORME EL MARCO JURÍDICO MEXICANO

José Luis Chavez Sanchez

El cómputo en la nube es una tecnología que en los últimos años ha tenido una aceptación importante, sin embargo, tras la aparición del virus SARS-CoV2 y debido a las medidas que se adoptaron para contener la propagación, tales como el aislamiento, distanciamiento y confinamiento social, se incrementó de manera significativa el número de organizaciones del sector público y privado que como una respuesta para asegurar la continuidad de sus servicios orientaron sus esfuerzos para migrarlos hacia el cómputo en la nube y realizarlos de forma remota.

Para precisar la noción de cómputo en la nube, se adoptará la definición realizada por la National Institute of Standards and Technology (NIST), entendiéndose como "un modelo que permite el acceso a la red de forma adecuada, en cualquier lugar y bajo demanda, con el fin de compartir recursos de cómputo con un esfuerzo mínimo de administración o interacción del proveedor del servicio"[14].

El cómputo en la nube "es una herramienta importante de transparencia y optimización de recursos de gestión y es asimismo un

[14] Mell, P., & Timothy Grance. (2011). The NIST Definition of Cloud Computing. *NIST, Special Publication 800-145*, 1–7. https://csrc.nist.gov/publications/detail/sp/800-145/final

instrumento útil para cerrar la brecha digital y hacer accesibles los recursos de la tecnología y de la innovación a más personas, con el consecuente potencial de desarrollo económico, nuevas empresas y empleos, "[15] además permite agilizar y optimizar el tratamiento de la información para tener un mejor aprovechamiento de la misma.

Es fundamental atender de manera especial al tratamiento de la información que se realiza en la nube, sobre todo cuando esto es realizado por un tercero, sobre todo aquella que se refiere a las personas, debido a que "… está conformada principalmente por aspectos como nombre, domicilio, teléfono, edad, sexo, escolaridad, estado civil, religión, filiación política, ocupación, amigos, familia, cuentas bancarias, pasatiempos, estado de salud, etcétera"[16], debido a que la legislación mexicana obliga a las organizaciones (públicas y privadas) que poseen este tipo de información a garantizar que en todo momento se realizará un tratamiento lícito y legítimo de los mismos[17], por tal razón resulta vital el conocimiento y cumplimiento del marco normativo que regula su protección, con el propósito de evitar que se presenten usos inadecuados, lo cual repercutirá tanto en la imagen y reputación de la organización, como en la vida privada de las personas.

Para efectos de este análisis, se entenderá por dato personal, "cualquier información concerniente a una persona física identificada o identificable"[18]

En el caso de México, el derecho a la protección de los datos personales, se encuentra consagrado en la

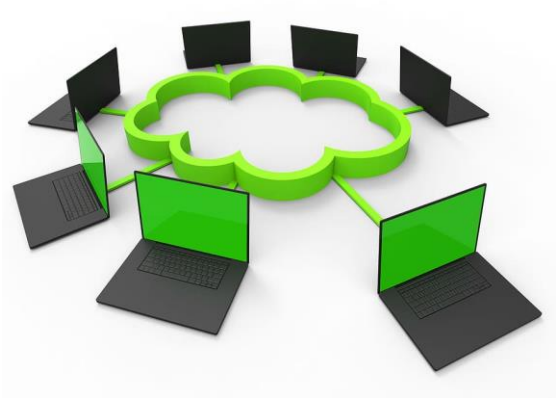
[15] Téllez Valdés, J. (2013). LEX CLOUD COMPUTING. Estudio jurídico del cómputo en la nube en México. En M. L. Ruiz (Ed.), *LEX CLOUD COMPUTING. Estudio jurídico del cómputo en la nube en México.* (1a ed., pág 139). http://ru.juridicas.unam.mx/xmlui/bitstream/handle/123456789/12154/consideraciones-finales.pdf?sequence=8&isAllowed=y

[16] Meraz Espinoza, A. I. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. Revista Ius, 12(41), página 301. https://doi.org/10.35487/rius.v12i41.2018.313

[17] El tratamiento de datos personales implica las operaciones o acciones, tales como la obtención, uso, divulgación y almacenamiento, sin importar el soporte físico, ni si son realizados de manera manual o automática, la definición normativa está contemplada tanto en Ley Federal de Protección de Datos Personales en Posesión de los Particulares en la fracción XVIII del artículo 3º como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en la fracción XXXIII de su artículo 3.

[18] Concepto establecido tanto la Ley General de Datos Personales en Posesión de Sujetos Obligados en su artículo 3, fracción IX, como en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en el Artículo 3, fracción V.

Constitución Política tanto en el artículo 6º, en la fracción II del apartado A), el cual indica: “la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes”, así como el artículo 16 párrafo segundo, el cual establece: “toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición[19], en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”.



Si bien anteriormente, se abordó la noción de cómputo en la nube por la NIST, es fundamental tratar la definición normativa establecida en el marco jurídico mexicano en la materia; es el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) en el año 2011, que por primera vez estableció una definición de cómputo en la nube, la cual está prevista en el artículo 52, el cual a la letra señala:

> *“…por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente”.*

Posteriormente en el 2017 la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), en la fracción VI de su artículo 3, estableció una definición similar:

> *Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante*

[19] Esta serie de acciones se conoce como derechos ARCO (Acceso, ratificación, cancelación y oposición) y son ejercidos por los titulares de los datos personales ante las respectivas autoridades y empresas.

> *procedimientos virtuales, en recursos compartidos dinámicamente;*

En septiembre del año 2021, en las "Políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal" (PDTICAPF), en la fracción XLIV del artículo segundo, define el cómputo en la nube de la siguiente forma:

> *Modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente,* ***que se encuentren localizados fuera o dentro del territorio nacional, en instalaciones del Estado o en instalaciones privadas****;*

Ésta definición, adicionó el supuesto de que los servicios de nube en cómputo no tienen ningún tipo de restricción en cuanto a la localización de sus recursos, pueden situarse en México o en el extranjero, y a su vez, estar ubicados en cualquier inmueble sin importar si pertenece a un ente público o a un particular.

Una figura que resulta vital sobre el tema analizado, es la referente al *Responsable* del tratamiento de datos personales, "tanto el artículo 3, fracción XIV, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), como el artículo 3, fracción XXVIII, de la LGPDPPSO, coinciden en definir a los Responsables… como aquellas personas físicas o morales que deciden sobre el tratamiento de los datos personales"[20], de tal forma que son estos quienes disponen cuáles y cómo serán ejecutadas las acciones encaminadas para la obtención, uso, divulgación y almacenamiento de los datos personales.

Es el Responsable del tratamiento de datos personales quien tiene a su cargo la facultad de realizar la contratación para que un proveedor (también denominado *Encargado*), de servicio, aplicaciones e infraestructura en la nube, sea el que realice el

[20] Davara Fernández de Marcos, I (coord.). (2019). *Diccionario de Protección de Datos Personales* (INAI (ed.); 1a ed.). INAI, pág. 782.

tratamiento de datos personales, de acuerdo con lo establecido en el artículo 63, 64 de la LFPDPPP y 111 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, y en el caso de las entidades del sector público, en el artículo 52 del RLGPDPPSO.

Las organizaciones del sector público que tengan el propósito de contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, deberán aportar datos que justifiquen dicha decisión, esto se presentará durante la realización del Estudio de Factibilidad, de acuerdo con lo señalado en el párrafo tercero del artículo 46 de las PDTICAPF.

Continuando con el análisis de los artículos 52 del RLGPDPPSO, 63 y 64 de la LFPDPPP, en ambas normas regula en términos idénticos las consideraciones que al menos deberá observar el Responsable cuando efectúe la contratación del proveedor de servicios de nube que realizará el tratamiento de datos personales:

1. Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley.
2. Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.
3. Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.
4. Guardar confidencialidad respecto a los datos personales sobre los que se preste el servicio.

De igual forma el Responsable también deberá verificar que dicho proveedor cuente con al menos los siguientes mecanismos:

1. Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
2. Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

3. Establecer y mantener medidas de seguridad[21] adecuadas para la protección de los datos personales sobre los que se preste el servicio;
4. Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, e
5. Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada por autoridad competente, informar de ese hecho al responsable.

Asimismo, la normatividad señala que en caso de que el proveedor no garantice la debida protección de los datos personales, conforme a la normatividad mexicana en la materia, el Responsable deberá abstenerse de adherirse o contratar dichos servicios.

Adicionalmente a los temas analizados, respecto a los puntos que se deben considerar para la selección y contratación de proveedores, para los servicios de infraestructura, plataforma y software de cómputo en la nube, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI),[22] ha expedido una serie de criterios y guías, para que las organizaciones en sus respectivos ámbitos, tengan documentos que las auxilien en el cumplimiento de los artículos 63, 64 de la LFPDPPP y 52 del RLGPDPPSO antes abordados. A continuación se mencionarán los documentos referidos:

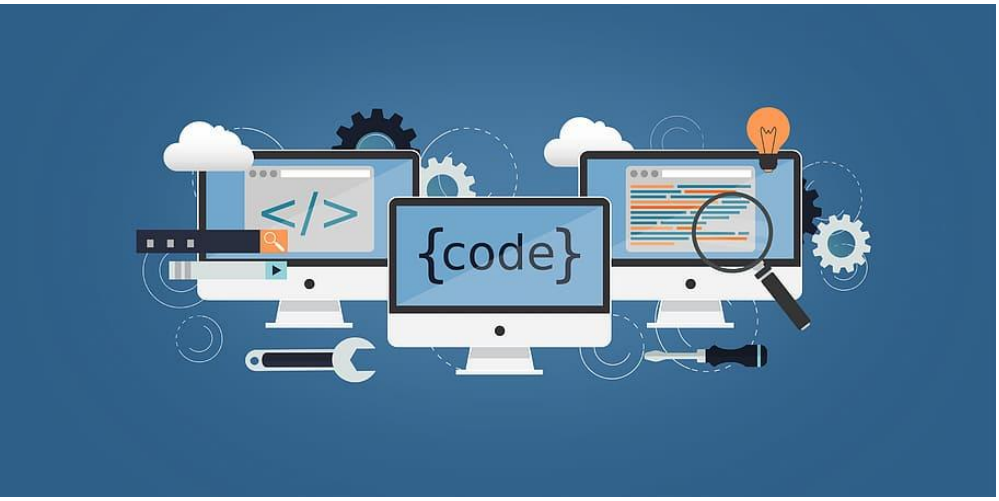
- Guía breve para Sujetos Obligados para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.[23]
- Criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.[24]
- Conformidad de contratos de adhesión de servicios de

[21] Las medidas de seguridad pueden ser físicas, técnicas y administrativas.
22 Es el organismo garante en el ámbito federal responsable de promover, vigilar y garantizar el cumplimiento del derecho de acceso a la información pública y la protección de datos personales en los términos que establezcan las leyes aplicables en la materia.
23 https://home.inai.org.mx/wp-content/uploads/Guia_SO_CC.pdf
24 https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/ComputoEnLaNube.pdf

cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales.[25]

Estos documentos contienen recomendaciones y buenas prácticas, que orientan a los Responsables del tratamiento de datos personales en la selección y contratación de proveedores. Las recomendaciones sugieren que los responsables deben:

a) Identificar los procesos y datos que se quieren migrar a la nube, el modelo de aprovisionamiento deseado y definir políticas internas y de seguridad para el servicio que se pretende contratar;



b) Seleccionar al proveedor con base en una evaluación de su reputación, considerando si está certificado o se somete constantemente a auditorías sobre gestión de seguridad de la información o de protección de datos personales, si ha sufrido incidentes o se han denunciado deficientes medidas de seguridad.

c) Considerar que los proveedores negocien los términos y condiciones del contrato de servicio.

d) Considerar si los contratos contienen cláusulas que indiquen: el apego al cumplimiento de la normatividad mexicana y que las controversias se resuelven en el territorio nacional; eviten que el proveedor reclame en cualquier momento la propiedad de la información proporcionada, y/o la que se genere directamente relacionada con el servicio.

e) Permitir que las organizaciones que realicen la

25 https://home.inai.org.mx/wp-content/uploads/ContratosASCN_CN.pdf

contratación, restrinjan o modifique el tipo de tratamiento en el servicio; además de que puedan acceder, modificar o borrar información en cualquier momento durante la vigencia del servicio, y en el caso de que la información la tenga que borrar el proveedor, se utilicen metodologías de borrado seguro.

f) Informar a las organizaciones contratantes de casos de vulnerabilidades, fallas en los servicios, así como de las acciones de remediación implementadas.
g) Optar por proveedores que garanticen transparencia en la cadena de personal o empresas contratadas o subcontratadas, mecanismos implementados para garantizar la confidencialidad de los datos personales, y la posibilidad de atender el ejercicio de los derechos ARCO de los mismos.

Las guías y recomendaciones también contienen listas de verificación que ayudan a los Responsables del tratamiento de datos personales para que paso a paso puedan verificar el cumplimiento de manera pormenorizada, así como revisar el contenido de los contratos que regulen la relación con los proveedores de servicio.

Sin duda, el conocimiento del marco jurídico analizado, permite a cualquier organización en México tener la certeza de que con la implementación de dichas medidas legales, la información referente a datos personales, será tratada y resguardada de manera lícita por los proveedores de servicios en la nube, lo cual repercutirá en el fortalecimiento tanto de su imagen como en la confianza con sus clientes y gobernados.

DIPLOMATURA GESTIÓN Y ESTRATEGIA EN CIBERSEGURIDAD

DIPLOMATURA EN DATA GOVERNANCE

PROGRAMA EJECUTIVO DIGITAL AWARENESS OFFICER

DIPLOMATURA EN ANÁLISIS DIGITAL FORENSE

cecib
centro de estudios en ciberseguridad

UNIVERSIDAD DEL CEMA
MCMLXXVIII
UCEMA

Una información está constituida por un dato o un conjunto de datos que al ser procesados y organizados, forman un significado en un determinado contexto, convirtiéndose en un conocimiento capaz de ser útil para diversos fines. En este sentido, se puede decir que el estado primitivo de la información son los datos que se procesarán y organizarán para la formación del conocimiento.

Los datos o el conjunto de datos pueden ser decisivos para la construcción de una estrategia y/o el mantenimiento de una actividad empresarial, por lo que la organización que los considera un activo y les atribuye un valor significativo, debe protegerlos.

En este sentido, la organización debe adoptar medidas contra los diversos acontecimientos que puedan poner en peligro su activo intangible necesario para la actividad empresarial (datos), como la adopción de políticas y la aplicación de procesos y procedimientos.

La eficacia de las medidas adoptadas por una organización pasa por la observancia de la tríada de a seguridad de la información compuesta por: personas, procesos y tecnología, y la observancia de estos elementos ayuda a la gestión eficaz de las vulnerabilidades.

La inversión en seguridad de la información ayuda a prevenir la pérdida de activos (datos), asegura la privacidad y garantiza la continuidad del negocio corporativo, entre otros beneficios. Además de la tríada mencionada, es necesario considerar tres aspectos esenciales: la confidencialidad, la integridad y la disponibilidad de la información.

Montanaro (2021, p.338-339) lo conceptualiza de la siguiente manera: "*Confidencialidad:* la que garantizará que sólo las personas que deben tener acceso a esos datos efectivamente lo tengan; *Integridad:* la que garantizará que ese conjunto de datos sea siempre el mismo que debe ser, independientemente del soporte en el que resida, del tiempo que pase o del medio por el que se haya transmitido; *Disponibilidad:* la que garantizará que ese conjunto de datos esté

siempre al alcance de quienes necesitan acceder a él."

Centrando este texto en los elementos "personas" y "confidencialidad", es necesario que la organización clasifique el tipo de datos que se tratan. En otras palabras, limitar el acceso de las personas (privacidad) y estar seguro de quien esta autorizado a acceder a determinados datos (exclusividad).

A partir de ahí, la organización adoptará medidas de seguridad de la información basadas en las personas, como la firma de acuerdos de confidencialidad, los registros de los empleados y la gestión del acceso a la base datos, la concienciación sobre la seguridad con un enfoque en la formación y las pruebas de eficacia, entre otras medidas

Al adoptar tales medidas y tratar datos personales, la organización estará en el camino de cumplir con el "principio de seguridad"[26] aliada con el "principio de prevención"[27] presente en el artículo 6, incisos VII y VIII de la Ley General de Protección de Datos Personales brasileña (LGPD – Ley Nº 13.709, del 14 de agosto de 2018), es decir, teniendo como objetivo "[…] prevenir la ocurrencia de daños derivados del tratamiento de datos, como el desarrollo de la formación y el *awarness* (práctica de estar vigilante, consciente)", la organización debe "[…] conocer dónde está el tratamiento de datos, las vulnerabilidades y las prioridades del tratamiento, haciendo una 'radiografía' de la empresa prevenirse de posibles incidentes" (TEIXEIRA; ARMELIN, 2019, p.49-50).

En este sentido, los miembros de la organización deben ser conscientes del valor existente en los datos tratados y de las consecuencias de su mal uso, estando debidamente formados, ya que cualquier desviación de la finalidad en su tratamiento puede traer consigo importantes reflejos en la relación interna y externa de la organización.

Una de estas consecuencias puede afectar a la relación empleado-empleador, es decir, a la relación laboral entre el empleado con acceso a determinados datos (exclusividad y privacidad) y la organización (datos como activo).

En este sentido, una reciente decisión brasileña del Tribunal Regional del Trabajo de la 2ª Región (TRT2) reconoció a aplicación de la sanción más severa aplicable a un empleado: la justa causa.

Según Garcia (2018, p.588; 590), "el despido con justa causa se produce cuando el empleador decide por la terminación del vínculo laboral, mediante el ejercicio de su potestad disciplinaria, ante la falta disciplinaria practicada por el trabajador", es decir, es "la terminación del contrato de trabajo por la práctica de un acto culposo, dotado de gravedad […]".

En Brasil, según Garcia (2018, p.591) "[…] sólo la ley se encarga de establecer las hipótesis de justa causa […] [pero] no impide que el juez interprete las normas legales, así como los hechos en discusión, para decidir si el empleado practico o no la justa causa".

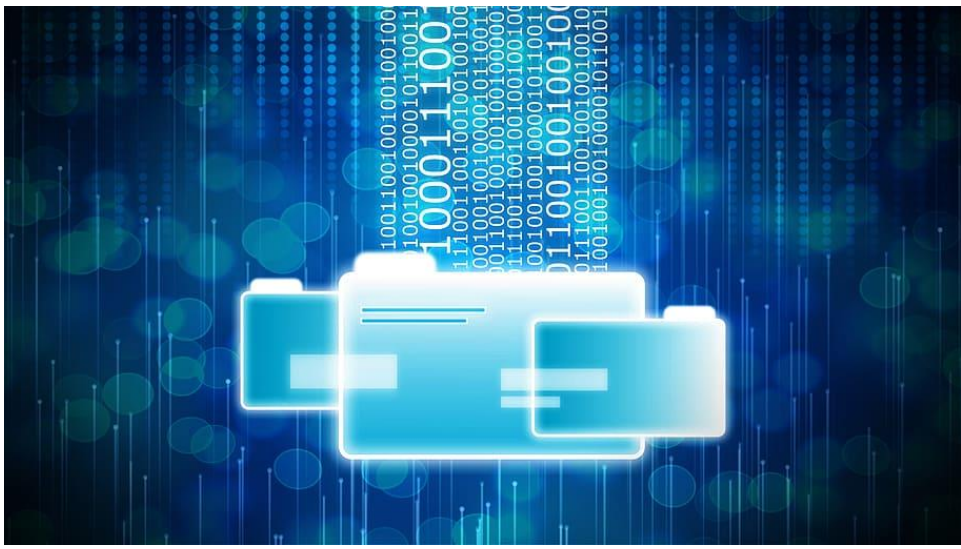
La legislación laboral brasileña se conoce como la CLT "Consolidación de las

[26] Principio de seguridad: "la utilización de medidas técnicas y administrativas apropiadas para proteger los datos personales contra el acceso no autorizado y la destrucción, pérdida, alteración, divulgación o difusión accidental o ilícita" (ley brasileña de protección de datos personales);

[27] Principio de prevención: "tomar medidas para evitar que se produzcan daños como consecuencia del tratamiento de datos personales" (ley brasileña de protección de datos personales).

Leyes del Trabajo" (Decreto-Ley nº 5.452, del 1 de mayo de 1943) y el artículo 482 establece la justa causa de rescisión del contrato de trabajo por parte del empleador.

Con base en artículo 482 de la CLT es posible citar motivos de justa causa, tales como: acto de improbidad; embriaguez habitual o en servicio; violación de secretos de la empresa; acto de indisciplina o insubordinación; abandono del empleo; acto que lesiono el honor o la buena reputación practicado en el trabajo contra cualquier persona, o lesión física, en las mismas condiciones, salvo en el caso de legítima defensa o defensa de terceros; entre otros motivos.



Así, para que exista justa causa, el motivo debe ser serio y estar sólidamente probado, para no perjudicar el principio de la continuidad de la relación laboral, que es la base del Derecho Laboral brasileño y está presente en la Constitución de la República de 1988.

Según Garcia (2018, p.79), "el principio de continuidad de la relación laboral pretende preservar el contrato de trabajo […] no solo dando seguridad al trabajador durante la vigencia de su contrato de trabajo, sino también en su integración a la empresa, favoreciendo la calidad del servicio prestado".

Así, no cualquier hecho puede dar lugar a la aplicación de la justa causa, sino que el hecho debe ser lo suficientemente grave y estar probado.

En este sentido, una reciente decisión brasileña del Tribunal Regional del Trabajo de la 2ª Región reconoció como válida la aplicación de la justa causa a un empleado. En el caso, el empleado presentó una demanda cuestionando la justa causa aplicada por el empleador contra él.

La demanda interpuesta por el trabajador (1000612-09.2020.5.02.0043) pretendía conseguir la revocación de la justa causa, ya que alegaba que la aplicación de la justa causa habría sido desproporcionada al hecho ocurrido.

En este caso, el empleador aplicó la sanción de justa causa al empleado porque había enviado datos personales confidenciales de la empresa a su correo electrónico personal. En otras palabras, el empleado había llevado los datos confidenciales de la empresa a su esfera personal, lo que caracterizó para el empleador el extravío de datos confidenciales y la violación de los procesos y procedimientos de seguridad de la información de la empresa.

En la resolución judicial, confirmado en segundo grado, los jueces entienden que el hecho de que el empleado de una empresa de *trade marketing* envíe datos confidenciales a su correo electrónico personal, sin que necesariamente los transmita a terceros, constituye un acto gravoso, ya que se acredita que el empleado era consciente de la necesidad de preservar la confidencialidad de los datos por él tratados dentro de la empresa.

Los jueces destacaron que el empleado firmó y conocía la clausula de confidencialidad del contrato de trabajo, el código ético y el acuerdo de confidencialidad y la adhesión a la política de seguridad de la información de la empresa.

Así, aunque el trabajador no haya compartido los datos confidenciales con terceros, sino que sólo los haya enviado a su proprio correo electrónico personal, se estableció en la resolución judicial que al despedir al trabajador, la empresa no violó el principio de continuidad de la relación laboral, por lo que es válida la justa causa de extravío de datos confidenciales, de acuerdo con el artículo 482 de la CLT.

La decisión del tribunal es un precedente muy importante para Brasil, que avanza hacia la implantación efectiva de un sistema de protección de datos, además de demostrar cómo la Ley General de Protección de Datos Personales (LGPD) puede relacionarse con las relaciones labores y repercutir en ellas.

REFERENCIAS

GARCIA, Gustavo Filipe Barbosa. **Manual de Direito do Trabalho**. 11 ed. Salvador: Editora JusPodivm, 2018.

MONTANARO, Domingo. Gestão de vulnerabilidades. In: MALDONADO, Viviane Nóbrega. LGPD Lei Geral de Proteção de Dados Pessoais: manual de implementação. 2 ed. São Paulo: Thomson Reuters Brasil, 2021. p. 327-352.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo. Salvador: Editora JusPodivm, 2019.

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO. **Recurso ordinário trabalhista**. 1000612-09.2020.5.02.0043. Rel. DANIEL DE PAULA GUIMARÃES; Julg. 20/10/2021.

#MIS DATOS SOY YO

Permitirle a una aplicación que acceda a tus datos, es permitirle que comparta tu vida para sus objetivos comerciales y la de sus socios tecnológicos.

EDI

#LES MEVES DADES SÓC JO

Puges moltes fotos a les teves xarxes socials?

Més possibilitats que pateixis de suplantació d'identitat.

EDI

Las ciudades han cambiando, se han perfeccionado y hoy buscan la categoría de Smart Cities, la nueva Metrópoli. Ante todo, podemos definir a las Smart Cities, o ciudades inteligentes como aquellas que cuentan con un sistema interconectado donde se aplican las nuevas tecnologías para que estas ciudades tengan un óptimo funcionamiento tanto del transporte público, pasando por el uso eficiente de los recursos, espacios

públicos, amigable con el medio ambiente, zona comercial, la comunicación entre sus habitantes entre otros.
Una ciudad inteligente es aquella que prioriza y pone a las personas en el centro del desarrollo, es decir una ciudad inteligente en post y para los ciudadanos y residentes que la habitan.

Las ciudades han avanzado y ya no son lo que eran hasta hace un par de años atrás. Imaginar la ciudad perfecta ya no es solo una ilusión o fantasía, es una realidad. Hoy no solo una ciudad buscar verse linda y limpia, sino lo que busca es una innovación tecnológica y urbana además de sumar una buena calidad de vida y cuidando el medio ambiente.

La base para hacer de una ciudad una Smart Cities son los datos. Cuando hablamos de datos debemos tener en cuenta que los datos solos, separados y fríos no nos sirven de mucho. Lo importante es analizarlos, como utilizar y transformar esos datos para que nos sean útiles, fáciles de implementar y eficientes.

¿Pero que hace que una ciudad se transforme en ciudad inteligente? La tecnología básicamente. El desarrollo de la tecnología (IoT internet en las cosas), las telecomunicaciones y la digitalización han generado la creación de las Smart Cities. La utilización de las nuevas tecnologías es fundamental para el avance y la conversión de ciudades en ciudades inteligentes. Para que esto resulte es necesario que las

ciudades reciban información, datos en forma instantánea, se almacenen y se analicen. Todo esto en un tiempo real, para que las acciones que se implementen sean eficientes y eficaces, para llevar a cabo esto es necesario contar con una infraestructura que así lo permita, todo esto a través de internet de las cosas.

¿Qué beneficios traen estas Smart Cities a sus habitantes? Vivir en una ciudad inteligente trae múltiples beneficios y herramientas para sus habitantes. Es decir, la utilización de las nuevas tecnologías será fundamental para hacer que en las ciudades contribuya al bienestar y seguridad de los residentes.

Con relación al uso de los datos es muy importante la utilización del big data, esto permitirá tomar y transformar los miles o millones de datos que se han producido tanto por los ciudadanos como por los objetos conectados a Internet (IoT). También otra forma de alimentar a las Smart Cities es a través del machine learning (sistema que permite aprender de los datos), la Inteligencia Artificial (IA) o la realidad aumentada, las mismas pueden ser utilizadas en múltiples áreas.

¿En qué gestiones ayudan las smart cities?

Agua: es un recurso escaso y sin embargo muchos creen que es inagotable. El agua vale más que el oro y no lo vemos. Utilizar el agua en forma inteligente, es decir, almacenarla, cuidarla, tratarla y mantener su calidad en todo momento. Podríamos predecir y saber cuándo deben las ciudades abastecerse de agua para evitar sequias, sobre todo en ciudades donde el agua no abunda o varía en época estacional. De esta forma no solo abastecemos a los ciudadanos de la ciudad, sino que mantenemos un equilibrio en el riego, evitando desperdicios innecesarios.

Recursos y servicios: A través de la optimización de los recursos se puede realizar un desarrollo sostenible gestionando de forma inteligente los recursos naturales y la energía para el sector público y privado, como por ejemplo controlando las temperaturas de edificios, empresas e industrias a través de edificios inteligentes.

Seguridad y control del tráfico: con la utilización del 5G (aumentará la velocidad de conexión y reducirá el tiempo de respuesta y a su vez multiplicará el numero de dispositivos conectados) permitirá que los vehículos se comuniquen entre si y también con otros dispositivos mejorando la seguridad vial (para automovilistas y peatones) permitiendo fluidez en el trafico gracias al manejo de semáforos, el estacionamiento y a la vez incentivar a la utilización de los transportes públicos. Todo esto reducirá demoras en autopistas, atascos y hasta accidentes. Además puede ser visto y supervisado por drones que tienen la capacidad de identificar y detectar todos estos problemas.
Inclusive existen carreteras y/o rutas que cuentan con tecnología que permite ante una determinada cantidad de acumulación de nieve poder derretirla para evitar o reducir accidentes.

Ciudad segura: sin duda una ciudad más inteligente es una ciudad más segura. Ya que se aprovechan los avances de las tecnologías permitiendo que circuitos tomen las patentes de los vehículos y los vinculen con sistemas como fuerzas de seguridad para saber en instantes si un dominio tiene algún pedido de secuestro; cámaras de seguridad vinculadas también con las fuerzas policiales reduciendo de esta manera los delitos.

Cuidado ambiental: uno de los mayores consumidores de recursos como electricidad, agua entre otros son los edificios corporativos. Muchos de ellos los desperdician. En una ciudad inteligente podemos tener sensores en edificios que detecten la cantidad de gente que se encuentra en el edificio para cuidar el agua, el aire y la electricidad reduciendo el impacto ambiental.

Ciudad = Salud: el avance de las tecnologías fue fundamental para el avance de la salud. La conectividad garantiza una rápida y efectiva atención médica tanto en forma personal como en forma remota.

Gobierno Abierto: con las ciudades inteligentes los gobiernos también se ven incluidos en esta transformación. Si los gobiernos obtienen los datos en forma online pueden realizar las gestiones públicas necesarias para sus habitantes, contar con una administración más transparente y utilizar bien los datos.

Educación: sobre todo en épocas como las que nos tocan vivir, la tecnología fue de gran ayuda a la hora de estudiar. La tecnología acerco la escuela a la casa de mil de millones de niños, niñas y adolescentes, que con lo que podían estudiaban. Una ciudad inteligente es una ciudad que apuesta al cambio y a la innovación digital renovando las estructuras viejas y obsoletas por modernas y eficientes.

Constante crecimiento: hay un crecimiento sostenido de la ciudad no solo proporcionando un buen lugar para trabajar y vivir, sino que también crece la administración pública y crece su transparencia ante la mirada del ciudadano, las políticas se hacen visibles y mejora la gestión. Una ciudad que crece y muestra su crecimiento y políticas es una buena ciudad para vivir.

Autos autónomos: una nueva tecnología que viene a cambiar el paradigma de lo que es manejar un automóvil. Hoy aún nos cuesta imaginar un automóvil que se conduzca solo, que se de sus propias ordenes. Imaginemos como serán las ciudades del futuro cuando todos los automóviles se manejen a sí mismos y se den prioridad en la calle, frenando con anticipación a un semáforo en rojo o detectando cuando un peatón ponga un pie sobre la senda

peatonal. Ni hablar de dar el paso a otro vehículo o respetar las velocidades máximas y mínimas para circular y reducir su velocidad si el clima no acompaña.

Y obviamente reducir el estrés del conductor cuando maneja o el nerviosismo que puede sentir cuando siente que un auto “se le abalanza” o un conductor que tiene poca experiencia en el manejo… eso ya no sucedería con los autos inteligentes. Veremos igualmente con el tiempo como se terminan adaptando ya que constantemente los están actualizando y transformando. ¿Disminuirá la tasa de accidentes y muertes en una ciudad inteligente?

Hasta ahora todo parece positivo…¿quien no quiere vivir en una ciudad con esas características?… lo único que tal vez podría hacernos pensar es que sucede con nuestra privacidad y seguridad en los datos, cosas tan simples como ir a cualquier lugar y que solo sepan quienes se nos cruzan en el camino o con quien nos vamos a encontrar, ahora resulta que la ciudad inteligente va a saber todo sobre nosotros, que hago, que no hago, que hice y que voy hacer… lo preocupante sería quien ve esos datos que acumula la ciudad, si le va a dar un uso confidencial y seguro obteniendo solo lo que necesita de una forma anónima o sabrá mas de nosotros que nosotros mismos…

Para que las ciudades se conviertan en inteligentes más allá de la importancia de la tecnología, se requiere el desarrollo de las comunicaciones y la importancia de la conectividad. A través de la implementación del 5G cambiará la manera de comunicarnos porque la

velocidad que trae va a permitir ver casi todo en tiempo real.

¿Qué ejemplos encontramos de ciudades inteligentes?

Como hemos visto, ser una ciudad inteligente trae muchas ventajas, como ser una mayor transparencia en la administración pública, gobiernos más eficientes y transparentes, mejor atención al ciudadano y permite implementar y mejorar las policitas públicas. Como ejemplos tenemos a:

New York: sin duda una de las ciudades más cosmopolita del mundo. Cuenta con un sistema de alumbrado público inteligente, medición del agua en los edificios públicos, un sistema inteligente en el tráfico que se regula minuto a minuto con el fin de despejar el tráfico en general, control de los semáforos, una variedad de IoT (internet en las cosas), una red grande y veloz de Wi-Fi entre otras.

Además esta ciudad piensa también en las personas mayores, de esta manera ha instalado más bancos en los espacios verdes, han aumentado el tamaño de la fuente (letra) en los letreros informativos entre otras cosas.

Barcelona: está conectada por cientos de kilómetros de cable de FO (fibra óptica) y hoy prácticamente el Wi-Fi libre y gratuito cubre toda la ciudad. Es una de las ciudades donde más Smartphone hay por cantidad de habitantes de esta manera sus residentes están más conectados. Cuenta con una inclusión digital súper amplia en cuanto a formación. Con relación al transporte ha introducido autobuses híbridos, ha colocado placas solares y con relación al tráfico. Además cuenta con una eficiente gestión con relación a los residuos por tener contenedores inteligentes que reducen los malos olores.

Hong Kong: Cuenta con una gran tecnología y una economía inteligente, la gran mayoría de las transacciones se realizan con Tarjeta.
Cuenta con un transporte público óptimo y con aeropuertos inteligentes donde hay un contador que verifica el equipaje.
Además tiene miles de puntos de acceso a Wi-Fi gratuito.

Oslo: se enfoca en una atmosfera sostenible y amigable con el medioambiente, cuenta con luces inteligentes y brindan mayor o menor intensidad de luz según la necesidad de ese momento.
Además un control de tráfico para evitar demoras y accidentes tiene una gran cantidad de vehículos eléctricos. Apunta a la reducción de tráfico y ha implementado gran cantidad de ciclovias.

Dubai: Plantea digitalizar todos los servicios del gobierno y de esta forma eliminar el papel.
Apunta además a que en el 2030 un 25% de los viajes de transporte que se realizan en la ciudad sean con vehículos autónomos.
La policía cuenta con robots policías que se desplazan por las calles y pueden reconocer movimientos de personas tienen una tablet en el frente donde los residentes pueden denunciar hechos delictivos. También cuentan con vehículos policiales autónomos que cuentan con sensores, cámaras HD que reconocen objetos a una distancia de 100 metros.

Santiago de Chile: es la ciudad más inteligente dentro de Latinoamérica, tiene una gran inversión en la tecnología 5G y ha puesto a los ciudadanos en el centro del desarrollo.
Cuenta con un enfoque en la gobernabilidad, planificación, gestión pública, medio ambiente, transporte entre otros.

Las ciudades inteligentes o ciudades del futuro ya son un hecho y están hoy presentes entre nosotros. La cuestión ahora es mejorarlas e incentivar a que todas las ciudades sigan este camino no solo por un tema tecnológico sino por el tema del impacto ambiental que generamos todos los días. Una ciudad inteligente es una ciudad más sana y que colabora con el medio ambiente disminuyendo el impacto climático.

ElDerechoInformatico.com

EDI

LA RED QUE VA MÁS ALLÁ DE
LO QUE PODÉS VER

La educación argentina fue siempre una temática de debate en el campo social y político. Desde la ley 1.420, que data de 1884 como piedra angular del sistema educativo argentino, hasta la Ley de educación Nacional 26.206 en 2006, la ampliación de derechos y la integración al sistema educativo de niños, niñas y adolescentes fue notorio, sin embargo, falta un largo camino por recorrer en dicha temática y más en tanto inclusión digital y la educación de nativos digitales.

El contexto de pandemia de 2020-21 ha dejado expuesto las fragilidades del sistema educativo y de las falsas creencias populares del “acceso universal a la red", esto no se vio reflejado en la educación, tanto desde el punto de vista de los educadores, estudiantes y sus familias. La creencia de estar conectados por un celular constantemente en un contexto de “normalidad” no obtuvo su correlato en tanto “el saber utilizar la tecnología” y eso se visibilizó en el estrés del sistema educativo durante el primer periodo del 2020.

Cultural y socialmente las redes han cambiado y estar fuera de ellas es literalmente no existir, la falta de existencia conlleva diversos inconvenientes, es estar fuera del sistema, de los cambios, novedades, oportunidades laborales, del conocimiento, “vida social” y negocios. Hoy, la vida es casi impensable sin la “conexión a la red”, prendemos la tv y ya estamos conectados. Lo cual nos

obliga a reflexionar, practicar una verdadera deontología desde todas las ciencias es imperioso de cara al futuro. Como se pudo observar en las estadísticas realizadas por AALCC[28] , se concluye que la falta de educación digital conlleva múltiples peligros para los usuarios, que con un click o al registrarse en una aplicación se encuentran "navegando" para no decir "naufragando" en la red. Los usuarios son cada día más jóvenes, son nativos tecnológicos, pero este ingreso al mar que llamamos red no se acompaña con educación, creyéndose que se está totalmente seguro por el solo hecho de estar en una ubicación conocida (casa, habitación, oficina, etc) no se toma real conciencia sobre los peligros que pueden causar y como señalan diversos casos hasta físicos.

Como se mencionó anteriormente, la creencia en el anonimato que otorga la red, la seguridad de estar en un lugar conocido y sobre todo la creencia que el acceso y la búsqueda de información por parte de los educandos, es la exacta que se busca, también es parte de la educación de los nativos digitales. Seguramente muchos docentes de todos los niveles, pueden dar fe de esto, la falsa creencia que "googlear" es la solución al problema que se busca sin distinguir fuentes o veracidad de lo encontrado es un problemática a tener presente, porque así también se viralizan las famosas "fake news", experimentos peligrosos, datos falsos, en fin información falsa y/o peligrosa.

Hasta el momento tenemos algunos puntos de interés, la creencia del anonimato dentro de la red, la seguridad que nos confieren por estar seguros en entornos conocidos y la veracidad de todo lo encontrado en ella.

En tanto el primer punto, la creencia del anonimato de una parte y que con quien se interactúa es esa persona, nos deja vulnerables y es así como un alto porcentaje de seres humanos en el

[28]Recuperado de : https://www.cibercrimen.org.ar/2021/06/07/crecimiento-exponencial-del-fraude-en-2021-estadisticas-aalcc/ https://www.cibercrimen.org.ar/2020/05/03/importante-incremento-de-delitos-informaticos-en-cuarentena/

mundo son víctimas de todo tipo de delitos, como aquellos contra la integridad sexual, porque creemos que no podrían realizarse por falta del o los sujetos en el hecho[29] .
Para comprender esto, pongamos un ejemplo simple:

> *"Imaginemos que nos encontramos en una red social por ejemplo Facebook, nos llega una notificación de amistad de una persona que no conocemos, pero que tenemos amigos en común. Por esas cuestiones de la vida, en algún momento comenzamos a charlar sobre nosotros, la charla es muy interesante. Nos cuenta algo de su vida, nos manda fotos etc. Con el correr del tiempo se comienza a dar el "sexteo" (charlas eróticas, envío de fotos etc.), se intercambian fotos de desnudez y de pronto todo cambia y se nos pide un dinero a cambio de no divulgar esas imágenes íntimas"*

Claramente, aquí nos encontramos frente a un delito de extorsión que se encuentra contemplado en el art 169 del Código Penal Argentino y que debe ser denunciado.
Desde el punto de vista moral, si uno es mayor de edad, el ejemplo planteado puede ser catastrófico, denigrante, pero, si se trata de un niño/a u adolescente trae acompañado una complejidad mucho mayor con consecuencias y daños mayores que incluso en algunos casos llevan al suicidio.

Esto nos lleva al segundo punto, ya que insólitamente, muchas veces se cree que la inseguridad se da en el "afuera", pero con la tecnología, el "afuera" ingresó por la puerta de los hogares para quedarse. ¿Se puso a pensar la cantidad de fotos que tiene en sus redes sociales sobre espacios de su casa, lugares que visita, etc.? La idea

[29] "Carignano, Franco Daniel p.s.a. producción de imágenes pornográficas de menores de 18 años, etc. - Recurso de Casación". https://justiciacordoba.gob.ar/justiciacordoba/Inicio/indexDetalle.aspx?codNovedad=22212

no es volvernos paranoicos, es educarnos, tomar los recaudos necesarios. Para quienes ejercen el cuidado de niños/as y adolescentes, muchas veces este mundo es incomprensible y no pueden o no saben cómo resguardarlos de los peligros que allí se encuentran. Las modalidades cambiaron y con un simple “no aceptes nada de extraños en la calle” bastaba, ahora, el mundo es más grande porque estamos interconectados. Existen infinidad de aplicaciones y programas que pueden monitorear la actividad de los niños/as y adolescentes pero esto no es suficiente, para ello, es necesario educarlos y educarnos digitalmente, comprendiendo que los peligros pueden suceder por la conexión y que en el caso de que sucedan situaciones peligrosas o dudosa se encuentren atentos y puedan denunciar ante las autoridades pertinentes

La marginalidad digital, algunas reflexiones.

Una problemática compleja, en un mundo que día a día hace que la vida de algunos sea más simple, para otros se vuelve cada día más lejana. El impedimento de acceder por cuestiones económicas y sociales a las nuevas tecnologías y a la conectividad, generan exclusión. La tríada educación, tecnología y derecho se vuelve más fuerte y es menester tomarlas en consideración en un mundo digital.

En la actualidad, el contexto mundial de pandemia visibilizó lo antes mencionado, aquellos que se encontraban en situaciones de fragilidad educativa, sufrieron la desconexión casi total con el ámbito educativo, imponiendo a los educadores de todos los niveles un esfuerzo por buscar la forma de reconectar con el educando. Fue en 2020, donde se manifestó la brecha digital y por consiguiente el no cumplimiento del derecho a la educación de un sector que se encuentra excluido y expulsado socialmente, que como señalan Corea y Duschatzky sobre expulsión social, “*La expulsión social produce un desexistente, un "desaparecido" de los escenarios públicos y de intercambio. El joven expulsado perdió visibilidad, nombre, palabra, es una "nn- ' nuda vida", porque se trata de sujetos que han perdido su visibilidad en la vida pública, porque han entrado en el universo de la indiferencia, porque*

transitan por una sociedad que parece no esperar nada de ellos[30]*.*

Por lo brevemente expuesto, es sencillo unir este concepto de expulsión social, con el ejercicio de un derecho básico como la educación, no solo en lo formal como fueren las asignaturas básicas como Matemática, Literatura, Ciencias Sociales o Ciencias Naturales, es coartar del derecho a todo tipo de aprendizaje y dentro de esto a otro tipo de conocimientos como los delitos informáticos a los que los niños, niñas y adolescentes son más vulnerables.[31]

Tal vez, el error más común en nuestro sistema educativo es la falta de equipos técnicos dirigidos directamente a las escuelas con campañas reales de concientización, llevada a cabo como parte de una política de Estado, de hecho, el desconocimiento tanto de los educandos en temas concernientes a obligaciones y derechos es una gran deuda que se debe saldar.

Por otra parte, en Argentina la legislación sobre delitos informáticos data de 2018, sin embargo su difusión es escasa en ámbitos no especializados, generando una nueva brecha entre quienes pueden acceder a esos conocimientos y quienes no, ingresando en una incertidumbre de saberes y consiguientemente de acceso a la justicia, por falta de conocimiento. La falta de educación en nuevas tecnologías, conlleva a que los delitos cibernéticos no se denuncien, aun cuando es visible su aumento, la premisa es simplemente verificable acorde al tercer muestreo de denuncias judiciales de la república argentina (2015)[32].

En conclusión, ante lo expuesto sucintamente, es necesario que la triada Educación, Tecnología y Derecho se fortalezcan creando ciudadanos digitales y se promueva el acceso a la red, no como meros decisores de qué ver o qué elegir, o entregando computadoras a todos los

[30] Corea, C., & Duschatzky, S. (2002). *Chicos en banda: los caminos de la subjetividad en el declive de las instituciones*. Paidós.

[31] AALCC, E. (2020, 24 diciembre). *Estadísticas año 2020 completo*. AALCC. https://www.cibercrimen.org.ar/2020/12/24/estadisticas-ano-2020-completo/

[32] Sain, G. (2018, 1 abril). *Tercer muestreo de denuncias judiciales en la República Argentina*. http://www.bibliotecadigital.gob.ar/items/show/1755.

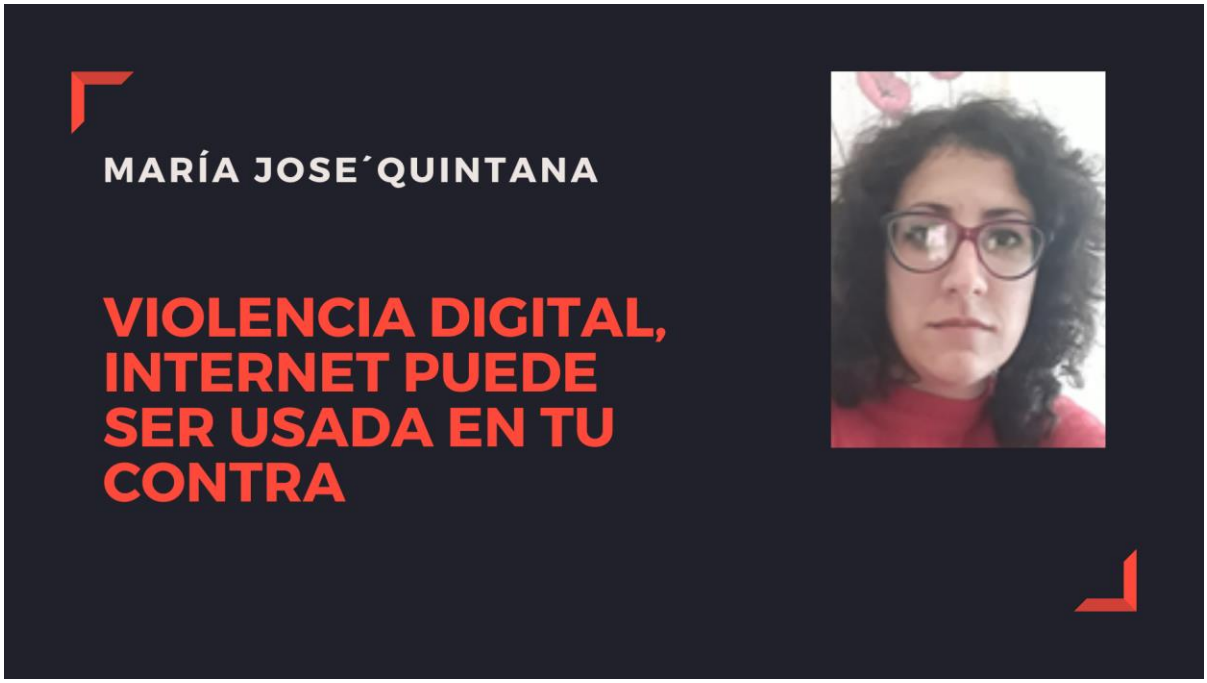
que tener la herramienta no es saber utilizarla. Dista mucho el ciudadano digital, del simple usuario que selecciona una película en una plataforma virtual o realiza compras de electrodomésticos en plataformas muy específicas, adquisición de videojuegos, entre otras cosas. Un ciudadano digital, tiene una identidad propia aún cuando parezca que se encuentra de incógnito en una red, es un ser que opina, que busca, se encuentra con otros y al mismo tiempo tiene la obligación de respetar y hacer respetar los derechos más básicos, y también denunciarlos cuando son violados. Por ello, debemos, “Educar al ciudadano digital”, es una cuestión que no puede esperar, es imperioso que las nuevas generaciones puedan ejercer sus derechos en este nuevo mundo cada día más digitalizado, en un marco donde muchos acceden pero pocos conocen.

Prof. Galderisi, Maximiliano

Future

EDI

El espacio de La Red donde



Internet es un medio magnifico que nos permite romper las barreras del tiempo y del espacio y hacer cosas increíbles, tales como trabajar remotamente; conectarnos con seres queridos que viven lejos; en tiempo real; vincularnos con personas de otras naciones, lo que implica crecer cultural y profesionalmente; capacitarnos, etc.

Como herramienta que es, puede ser bien o mal utilizada, para construir o para destruir, como un martillo, con el que se puede hacer una casa o matar a alguien.

Key Words: violencia digital; acoso; grooming; sextorsión, porno venganza; lesiones.

I. Para empezar a poner la lupa.

La intimidad de todos está expuesta, mal utilizados, los medios digitales son peligrosos aunque no se los perciba así de manera inminente.

Desde hace algunos años, se generó en la sociedad la sensación de que la vida de las personas sólo cobra importancia, en la medida que era expuesta en una vidriera pública adonde contar maravillosas historias de éxito y felicidad. El uso masivo de dispositivos y de las redes de conexión, sumado al encierro que vivimos a nivel mundial como producto de la pandemia, aceleraron nuestros procesos de vinculación con el mundo digital.

De ahí un *exceso de confianza* al compartir contenido en redes sociales, con el fin de pertenecer. Actualmente las consecuencias negativas de estas malas prácticas se han visto exponencialmente incrementadas. Es que con toda nuestra vida privada servida en bandeja, es fácil

quedar expuesto, y luego que ese material sea usado en tu contra.

Los colectivos más vulnerables siguen siendo las mujeres y los niños, niñas y adolescentes, sin embargo las prácticas de hostigamiento digital, revange porn, sextorsión y acoso también alcanzan a los hombres.

II. Violencia digital.

La violencia digital ocurre cuando se usa internet y los medios digitales para dañar a alguien, para perseguir, hipervigilar, hostigar, acosar. Hay diferentes modalidades, entre las cuales está el ***bullying o ciberbullying***, que consiste en acosar a otro, con el objeto de intimidarlo, menoscabarlo o amedrentarlo, generalmente se da en ámbitos laborales o escolares entre personas de la misma edad, al que las redes sociales le facilitaron el terreno para su desarrollo y expansión como a muchos otros delitos.

El ***acoso* o seguimiento**, hipervigilancia y asedio de hombres y mujeres con el objeto de exhibir su intimidad públicamente, exponerlos a la humillación pública, siendo una gran mayoría de casos producto de una relación sentimental consentida, en los que *el atacante se vale de imágenes intimas que obtuvo dentro de la intimidad de la relación de pareja, para luego exponer a la víctima*. Pero también, estos actos pueden llegar a darse sin que haya mediado ningún tipo de relación sentimental anterior. Como en el caso de aquel que usa material que una persona publicó en las redes y lo desnaturaliza o tergiversa con el fin de dañarla.

Cómo se manifiesta?

Puede tener distintos tipos de lesividad e incidencia en la vida de las víctimas, ir desde la mera sensación de molestia, incluir afectación en la vida laboral, o pasar a ser una sombra que invade todas las esferas de la vida de quien la padece. Afectando su psiquis, sus relaciones interpersonales, su imagen social y profesional. Los casos más graves se dan, cuando el acoso es antesala de delitos graves en el mundo físico, como el abuso sexual.

También puede configurar otros delitos, como la **extorsión**: coaccionando a alguien a que haga o tolere algo contra su voluntad, bajo amenaza de que si no lo hace se publique material intimo que la deje expuesta públicamente.

Cuando esto se concreta, muchas veces dicho material privado, que

generalmente es de contenido sexual, es enviado por el atacante al círculo íntimo de la persona, quien queda en una situación de vulnerabilidad pública, afectando su vida laboral social y salud, acción vulgarmente se conoce como **porno venganza**. Hasta llegar incluso a lesionar gravemente su psiquis, caso en el cual se configuro otro delito más: **las lesiones**. La salud según el concepto de la OMS incluye el tanto el ámbito físico, como el psicológico, es un todo que engloba el bienestar humano, cuando el ataque altera el equilibro en la psiquis de la víctima, su salud e incolumidad como individuo se ve vulnerada, lo cual configura el delito de lesiones leves.

III. Uno de los delitos más graves que nos convoca, *el grooming*.

Se trata de otra forma de acoso, pero esta vez es el practicado por un adulto hacia niñas, niños y adolescentes, el que haciéndose pasar alguien de su edad engaña a su víctima, siendo su principal objetivo de carácter sexual, el de establecer una relación de intimidad ya sea para hablar de sexo o sexualidad, obtener fotografías de sus víctimas e incluso pactar encuentros personales, dejando la puerta abierta para la comisión de delitos más graves, todo ello, mediante el uso de dispositivos electrónicos y redes de conexión de internet.

Entre las consecuencias más graves del grooming conforme la casuística nacional e internacional, está el delito de abuso sexual infantil, la trata de personas, el abuso con intención de obtener material fílmico y de imágenes que exhiban las situaciones de abuso hacia los niños, niñas ya adolescentes y por su puesto muchas veces, el acoso y el abuso terminan en un homicidio o femicidio.

Según los expertos, es un tipo de ataque masivo de **ingeniería social**. Ataque de ingeniería social quiere decir, que el atacante o victimario se vale de la información que nosotros volcamos en las redes sociales, la que nosotros mismos le proporcionamos a la comunidad digital.

Este tipo de delincuentes, saben dónde desarrollan las actividades las víctimas de la edad que ellos buscan encontrar. Por ejemplo, que tipo de redes sociales usan, que paginas visitan, que intereses tienen, que series o películas miran, quienes son sus ídolos, que juegos usan, tienen la posibilidad de acceder a toda esa información que usan para mezclarse entre sus víctimas y acecharlas con la excusa de tener los mismos

intereses y los mismos problemas que ellos.

De ese modo despliegan una red alrededor de su víctima, como si se tratase de una telaraña en la cual se van haciendo amigos de sus amigos, simulando la falsa identidad de un menor, hasta ganarse la confianza y así obtener material como fotos o videos con contenido sexual de los niños que luego puede ser intercambiado en redes de pedofilia, y a la vez es usado para extorsionar al menor y seguir obteniendo más material.

IV. Consejos para prevenir:

- **Manejar la privacidad propia y de sus hijos en los dispositivos**, como leer las políticas de privacidad a la hora de crear una cuenta en una red social o al descargar aplicaciones.
- **Elegir con cuidado qué información publicar en redes**; qué imágenes, ser selectivo. No exponer datos de la intimidad.
- **Dialogar con los chicos** sobre los riesgos del uso de las redes sociales generando un marco de comportamiento seguro sin temor, ya que internet también es un sitio para obtener información.
- **Explicara los hijos las reglas básicas** como que las personas pueden mentir en su identidad del otro lado de la pantalla, que no deben aceptar ni hablar con desconocidos, si están jugando online conversar únicamente sobre el juego y no intercambiar datos de contacto como dirección, teléfonos, nombres de la escuela a la que asisten y mucho menos acceder a pedidos tales como sacarse la ropa o mostrar una foto
- No compartir las claves; cerrar sesiones de navegación; borrar historiales, usar doble factor de autenticación.
- **Denunciar usando las líneas oficiales que los Estados proveen o en la comisaría más cercana.**

V. Conclusiones

Es necesario ser conscientes y poner en valor nuestra intimidad como un activo crucial en la sociedad de las comunicaciones en la que vivimos. El flujo de información personal que todo el tiempo le regalamos a la red de redes tiene mucho más valor del que nosotros pensamos. NO hay que exponerse gratuitamente, sino ser proactivos en la autodefensa de nuestros datos cada vez que interactuamos. Sin importar cuanta confianza se tenga en el interlocutor que está del otro lado, recordemos que el canal es público, y no hay nada 100% seguro en la red.

Así que, la mejor forma de defendernos es aprendiendo a tomar conciencia y valorar que nuestra intimidad es la última frontera, para defender.

"LOS DESTACADOS"

EDI

2021

CUENTA EN RED SOCIAL

DALAT

Comunidad-
Instagram: @dalatcomunidad
Linkedin: linkedin.com/company/dalatcomunidad/

LAS DE SISTEMAS

Comunidad-
Instagram: @lasdesistemas
Linkedin: linkedin.com/company/lasdesistemas/

DERECHO INFORMÁTICO

Sitio web
Twitter: @derechotecno
Instagram: @derechoinformatico

Jorge Litvin

Abogado
Twitter: @cokilitvin
Instagram: @cokilitvin

JOVEN ABOGADO/A - REVELACIÓN

Mónica Velazco - El Salvador

Dario Echeverría Muñoz - Ecuador

Camilo Dalmao - Uruguay

María Pia Aquino - Argentina

EVENTO / INSTITUCIÓN

EDI

ACADEMIA MEXICANA DE DERECHO INFORMÁTICO

Primera asociación mexicana dedicada al Derecho de las Tecnologías de Información, y la segunda más antigua en Iberoamérica.

COLADCA

Comunidad-
Comunidad Internacional en Gestión de Riesgos y Seguridad /InSecurity www.coladca.com

IGF HONDURAS

Evento del Foro para la Governanza de Internet
Plataforma global de múltiples partes interesadas que facilita la discusión de cuestiones de política pública relacionada con internet

OCEDIC

Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales de la Facultad de Derecho, Universidad Austral

ATLANTICs

Asociación que busca fomentar la educación digital, evento: LA LOCURA SUPREMA"

INFORMÁTICAS/ OS

MARÍA ANGÉLICA CASTILLO DE RIOS - PERÚ

Gerente Público de La Autoridad Nacional del Servicio Civil - SERVIR.

CARLOS SEISDEDOS - ESPAÑA

Docente universitario - Expositor internacional
Autor del libro Open Source INTelligence (OSINT): Investigar personas e Identidades en Internet- -

SANDY PALMA - HONDURAS

Coordinadora Honduras Cibersegura
Chair IFG Honduras 2021
Top 50 Women in Cybersecurity Latin America 2021

ABOGADA/O

EDI

Rodolfo Guerrero Martinez - México

Carmen Velarde Koechlin - Perú

Carlos Richeri - Argentina

Claudia Avalos México

Karina Medinaceli - Bolivia

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

LA RED

somos

ELDERECHOINFORMATICO.COM