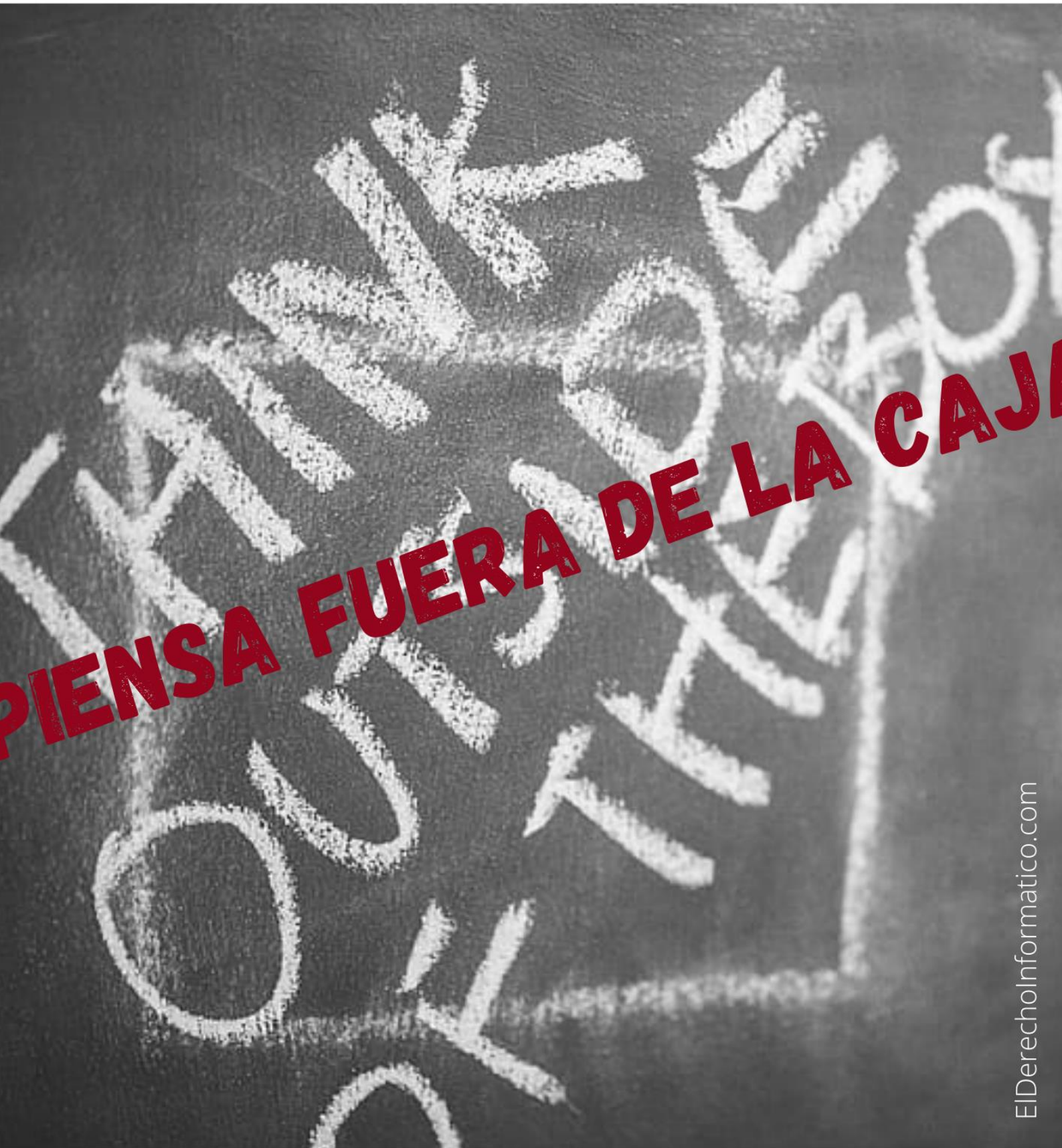
EDI

Revista Digital Distribución gratuita

OCTUBRE 2020 | EDICIÓN N° 36



EDI

Vamos...

ELDERECHOINFORMATICO.COM

INDICE

#MIS DATOS SOY YO

Primer Encuentro
#MIS DATOS SOY YO
"Tecnologías emergentes y Protección de Datos Personales"

Fecha: jueves, 29 de octubre de 2020
Hora: 17:00 a 19:45 Uruguay
15:00 a 17:45 Ecuador- Perú

EDI

#MEUS DADOS SOU EU

Se você receber uma mensagem pedindo "dados comerciais"

Entre em contato diretamente com a página que supostamente está solicitando os seus dados. Estes minutos extras podem lhe poupar muitos problemas.

EDI

EDITORIAL

Se nos escurre lento, contante y persistente este 2020, lleno de “nuevas normalidades”, normalidades que nos resistimos (en muchos casos) a aceptar, reuniones de medio vestir (camisa arriba, pantalón corto abajo), reuniones de fondos falsos para no mostrar nuest os caos privados, feliz cumpleaños cantados a una pantalla, charlas de café atadas a la saturación del ancho de banda de nuestro internet o el ajeno, aprendemos y aprehendemos todo lo que se nos cruce en webinars, conferencias, conversatorios, charlas, jornadas, congresos, todo ello a la distancia, sin escuchar la risa de la anécdota contada en un break, el abrazo del reencuentro, el viaje tan esperado, los nervios de contarle a una audiencia nuestro trabajo concienzudamente preparado durante meses... nuevas normalidades que le dicen, que se yo, déjenme pensar con mis años a cuestas que eso debe ser más bien una nueva realidad, que es muy distinto, la realidad es lo que nos toca vivir a cada momento, la normalidad es lo que vivimos a lo largo del tiempo, o por lo menos es lo que me gusta pensar a mi. Dejo el último párrafo para contarles que La Red lanzó junto a Hammurabi una colección de obras multiautor hace unos 15 días, 1 año de trabajo y esfuerzo, que creamos EDI Joven, que hicimos 2 congresos, que lanzamos 3 revistas, 1 edición especial y armamos programación estable de nuestro canal en Youtube, cumplimos 1 año de #MisDatosSoyYo (la campaña de concientización), reimos, festejamos, soñamos, sufrimos, nos permitimos tener fe y con ella, esperar con paciencia a la próxima realidad, la que nos haga más felices, que seguro será pronto...

EL DERECHO INFORMATICO
CAPÍTULO COLOMBIA

EDI

LA RED
ESTAMOS DONDE
ESTÁS VOS

La era de los algoritmos ¿enemigos o aliados?

Por
Ariadna Luján Martínez y
Francisca Ojeda Campos

INTRODUCCIÓN:

Mucho se ha hablado en los últimos años acerca de los algoritmos como herramientas de Inteligencia artificial (IA), y más aún se ha hablado sobre el riesgo inherente que conlleva su utilización: el hecho de que pueden reproducir o profundizar sesgos[1], y en consecuencia cómo en muchos casos han afectado los derechos de los ciudadanos, a tal punto de negar el acceso a algunos o privar de ciertos beneficios a otros.

Recientemente se realizó la Locademia de Derecho y tecnología organizada por la Red de Derecho Informático, donde pudimos exponer acerca del tema que hoy traemos a este paper. En esa oportunidad mencionamos los distintos tipos de sesgos, una característica propia de los seres humanos y que hoy se ha trasladado a los sistemas de inteligencia artificial, resultando en lo que se conoce como sesgos algorítmicos.

Pero el fin de este trabajo no es profundizar sobre los sesgos en sí, sino, como quedará demostrado, ofrecer una mirada más optimista

[1] *"La acción de apoyar u oponerse a una persona o cosa en particular de manera injusta, debido a que permite que las opiniones personales influyan en su juicio"* (Cambridge English Dictionary).

respecto de los algoritmos, e intentar hacernos cargo de sus riesgos, a través de ciertas consideraciones que estimamos se deberían tener en cuenta al momento de implementarlos como herramienta, de manera de enfocarnos en posibles soluciones. ¿Son los algoritmos nuestros enemigos?. La respuesta dependerá de nosotros, los humanos.

DESARROLLO:

"*La dificultad radica, no en las nuevas ideas, sino en escapar de las viejas*"[2].

Previo a desarrollar lo que podemos llamar nuestra propuesta de protocolo, creemos necesario precisar algunos conceptos.

¿Qué son los algoritmos?

Son un conjunto de instrucciones o reglas definidas, ordenadas que permite solucionar un problema, realizar un cómputo, procesar datos y llevar a cabo tareas o actividades, siguiendo pasos sucesivos, llegando a un resultado final (obtener patrones). Estos algoritmos , son entrenados con datos, lo que nos lleva a relacionarlo con **Machine learning[3]:** El término *aprendizaje automático* se refiere a la detección automatizada de patrones significativos en los datos. En las últimas dos décadas se ha convertido en una herramienta común en casi cualquier tarea que requiera la extracción de información de grandes conjuntos de datos. Existen diversas técnicas de machine learning, como aprendizaje supervisado, no supervisado, aprendizaje por refuerzo, y también las redes neuronales profundas o deep learning.

Entonces, ¿Cómo relacionamos estos conceptos?

Tenemos → Grandes cantidades de datos → estos son procesados con ALGORITMOS de Machine learning → como resultado se establecen **patrones.**

Por todo lo expresado es que cuando hablamos de **sesgos algorítmicos** debemos saber que los mismos reflejan los valores de los humanos que están implicados en la codificación, recolección de datos para entrenar al algoritmo.

Creemos que cualquier sistema de protección que busque velar por la no vulneración de derechos y un ejercicio y desarrollo responsable de

[2] Keynes, John Maynard.

[3] Corvalán, J. (2020). *Perfiles digitales humanos*. La Ley.

la inteligencia artificial, debe contemplar, un ámbito humano y un ámbito técnico.

Siguiendo los lineamientos del Libro Blanco del 2020 de la Comisión Europea[4], y las Recomendaciones Generales de la Red iberoamericana de protección de datos personales[5] es que llegamos a las **siguientes proposiciones:**

ÁMBITO HUMANO O ÉTICO : Los sistemas son realizados por humanos, por tanto, el avance y desarrollo de la IA debe ir necesariamente acompañado de una formación tanto de quienes crean los sistemas, como de quienes toman las decisiones de implementación, y de los destinatarios o usuarios.

Es importante entender a la IA como la herramienta compleja que es, y que al ser diseñada por y para las personas, requiere que reforcemos aspectos humanos que hoy son sumamente relevantes. En este sentido, formar equipos con un alto grado de conciencia en materia de ética es fundamental, de manera de fomentar el pensamiento crítico y cuestionador, y así poder crear sistemas que sean coherentes con los valores e ideas de la sociedad actual.

Por otro lado, los seres humanos naturalmente tenemos sesgos, para disminuir esto y poder avanzar en la educación y formación digital debemos formar un ecosistema de IA que acerque las ventajas de la tecnología a la sociedad, lo que debe hacerse desde distintos ámbitos y considerando los diversos actores que pueden estar involucrados.

Desde el **sector público**: Asegurar el acceso de datos y a la infraestructura informática. Además es necesario un marco político que promueva la investigación y la innovación. Promover la educación digital desde los primeros niveles de educación hasta los universitarios, y esto debe ir acompañada de regulación o protocolos que sean flexibles, ya que la necesidad de adaptación y re adecuación será constante con los avances que existen día a día.

Desde el **sector privado**, es necesario que el mismo pueda participar en la agenda de innovación e investigación (según

[4] Comisión Europea (2020). Libro Blanco sobre Inteligencia Artificial.

[5]Red Iberoamericana de Protección de Datos (2020). Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial.

sugiere el Libro Blanco) lo cual creemos que es efectivamente necesario. Pero además contar con **participación ciudadana**, facilitando el acceso a la información y que la misma sea clara, promoviendo la transparencia de los algoritmos, la consulta pública a la hora de hacer regulaciones y la promoción de softwares de código abierto.

Interdisciplinariedad: En palabras simples, significa que en el proceso de desarrollo de sistemas algorítmicos exista una *combinación de actores, elementos y valores de distintas áreas del conocimiento*[6]. Este es el factor estrella de nuestra propuesta, sin colaboración, sin aportes de distintas áreas todo lo demás no será exitoso. ¿Cómo lo implementamos? Un simple y claro ejemplo, si debo crear un algoritmo que me ayude a seleccionar beneficiarios o no de tarjetas de crédito, esto se verá reflejado agregando personas al equipo de trabajo que no sean afines a la empresa, invitando a expertos externos en materias que podrían considerarse obvias como economía, pero también expertos de otras áreas como podría serlo sociólogos u otras, que integren una mirada más amplia y que traspasen lo técnico.

ÁMBITO TÉCNICO[7]:

El ámbito humano debe necesariamente complementarse con protocolos de funcionamiento y revisión de los sistemas mismos, lo que hemos denominado área técnica, es decir, a realizarse en el proceso de desarrollo del algoritmo o en el post procesamiento del mismo.

Elegimos dos sistemas de auditoría de modelos de machine learning, enfocados en reconocer y mitigar los sesgos que pueden introducirse en los sistemas de diversas formas y en distintas etapas del desarrollo del modelo. Si bien existen otros sistemas de auditoría, lamentablemente aún no es una práctica estandarizada. Es imprescindible una revisión constante, ya que solo así se podrá

[6] Cevasco, L., Corvalán, J., Le Fevre, E. (2019). Inteligencia Artificial y Trabajo. Construyendo un nuevo paradigma de empleo.

La Real Academia Española lo define como Dicho de un estudio o de otra actividad: Que se realiza con la cooperación de varias disciplinas.

[7] Como mencionamos anteriormente, el objetivo de este paper es hacer una breve reseña de nuestra disertación en el Congreso, por lo cual para ampliar conocimientos humildemente los dirigimos al canal de youtube de EDI donde podrán profundizar lo que aquí tratamos

disminuir al máximo y a tiempo los posibles impactos negativos que pudieran existir al implementar modelos basados en algoritmos.

Modelo Fair ML[8]

Es un paquete de python desarrollado por Microsoft, que implementa algoritmos para detectar problemas de equidad de grupos de modelo de aprendizaje automático y a su vez mitigar injusticia.

¿Cómo funciona?

Hay algoritmos para mejorar el modelo durante el entrenamiento, pero también se puede utilizar un algoritmo de postprocesamiento para mejorar modelos ya existentes. Funciona a través de un panel de evaluación para evaluar cómo las predicciones de un modelo afectan a distintos grupos y a su vez, utiliza algoritmos de mitigación para disminuir la injusticia en la clasificación.

Utiliza un enfoque de equidad grupal que responde a la pregunta ¿Qué grupos de personas tienen riesgo de sufrir daños? Tanto daños de asignación[9] como daños en la calidad[10].

¿Cuál es el truco? Mide la dependencia de un modelo de sus entradas cambiandolas, si un cambio provoca drásticamente una modificación en la salida entonces el modelo es sensible a la característica.

Modelo aequitas[11]

Es una herramienta desarrollada por el Center for Data Science and Public Policy for Social Good Foundation, originalmente en la Universidad de Chicago, y actualmente en la Universidad de Carneige Mellon en EE.UU. Es una herramienta de código abierto[12] que permite auditar modelos de machine learning para detectar y mitigar sesgos, respecto de múltiples atributos (etnicidad, sexo, edad, etc.).

Se basa en una definición de sesgo entendida como medida de

[8] https://fairlearn.github.io/

[9] Este daño se produciría negando acceso a productos, servicios, o información a un grupo de personas.

[10] Este daño se produciría disminuyendo la calidad del servicio.

[11] Pedro Saleiro, Benedict Kuester, Abby Stevens, Ari Anisfeld, Loren Hinkson, Jesse London, Rayid Ghani, Aequitas: A Bias and Fairness Audit Toolkit, (2018).

[12] https://github.com/dssg/aequitas

disparidad entre grupos, en comparación con un grupo de referencia. A su vez, el grupo de referencia, se puede seleccionar utilizando varios criterios (los mencionados más arriba).

Lo distintivo de Aequitas es que tiene presente que sesgo y *"fairness"* no son conceptos absolutos y que están necesariamente vinculados al escenario al que se aplican, como asimismo al análisis y a la interpretación dentro de ese contexto. Por otro lado, pretende ser útil también a autoridades en general y no limitarse a ser entendido únicamente por personas con conocimiento técnico.

Una explicación más detallada del funcionamiento tanto del modelo Fair ML como de aquietas excede el objetivo de este documento, por lo cual, para aquellos que deseen profundizar en la materia, se recomienda acceder directamente a las fuentes. Lo importante es difundir su existencia y dar cuenta de que existe un interés y preocupación por desarrollar inteligencia artificial responsable con sello ético y en beneficio de las personas.

Conclusión:

Es ilusorio pretender que los modelos basados en algoritmos solucionarán automáticamente estructuras sociales complejas y que requieren ser reparadas desde diversos ámbitos. El desarrollo de la IA debe ir de la mano con el factor humano. De ahí entonces es que cobra vital importancia dicho factor, junto con la ética y los valores que defendemos y queremos, por un lado, y la necesidad de monitorear constantemente los sistemas de inteligencia artificial por otro.

En este sentido, es imperativo que la implementación de sistemas de IA vaya acompañada de discusiones y capacitaciones en el ámbito humano y de auditorías a los modelos, como alguno de los que mencionamos previamente, de forma de lograr una IA que sea a la vez útil, responsable y con enfoque social.

En este sentido, resulta acertado lo que expresa Kate Crawford, de Microsoft Research, "*es hora de reconocer que los algoritmos son una creación humana que hereda nuestros prejuicios [...]:* ***nuestra IA será tan buena como lo seamos nosotros"***[13]**.**

Creemos firmemente que esta afirmación va de la mano de educación ética y digital de los ciudadanos, y distintos actores sociales, como mencionamos, de estados PROACTIVOS, que no se resistan a lo que ya está sucediendo

[13] MERINO, Marcos. *Los algoritmos con sesgo racial son algo que venimos arrastrando desde los años 80.* *h*ttps://www.xataka.com/inteligencia-artificial/algoritmos-sesgo-racial-genero-problema-que-venimos-arrastrando-anos-80

sino que desde la interdisciplinariedad y la escucha de todos los sectores busquen soluciones de las que TODOS participemos. Que la IA sea potencialmente destructiva o potencialmente beneficiosa, hoy por hoy creemos que está en manos de nosotros, los humanos.

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

APLICACIÓN DE BLOCKCHAIN EN EL SECTOR PÚBLICO[1]

Por Ángela Maritza Pereyra

[1] Versión escrita de la charla dada en el Congreso Internacional Locademia Joven de Derecho y Tecnología, llevado a cabo los días 22/23/24 de septiembre de 2020.

Todos conocemos o alguna vez tuvimos un juego Lego y es difícil que no se nos venga a la mente sus piezas de colores, y más aún cuando veíamos las cosas que era posible armar con ellas. Algo similar ocurre con la Blockchain (o cadena de bloques): podemos conocer en líneas generales de qué se trata, pero las posibilidades de aplicación todavía siguen en fase inicial y aún no sabemos dónde se encuentra el límite, y más aún si consideramos que, junto con otras herramientas, constituye un integrante importante de lo que podría titularse como los "Jinetes de la Cuarta Revolución Industrial".[14] La intención de este breve artículo es llamar la atención sobre el tema y comenzar a reflexionar sobre algo que hoy ya está en marcha y promete seguir dando mucho de qué hablar.

Por motivos de extensión no me explayare respecto a las características de esta tecnología, bastando con señalar la relevancia que cobra el hecho de que sea un registro descentralizado, la inmutabilidad de la información allí contenida, el uso de métodos criptográficos para garantizar su seguridad, la necesidad de un protocolo de consenso respecto a los agregados que se vayan realizando, así como la trazabilidad y transparencia que le son inherentes

[14] Heredia Querro, S., 2020. *Smart Contracts: Qué Son, Para Qué Sirven Y Para Qué No Servirán*. 1st ed. Ciudad Autónoma de Buenos Aires: IJ Editores, p.38.

gracias a los Smart Contracts.[15] ¿Cómo se vincula esto con el sector público?[16] Desde hace mucho tiempo asistimos al espectáculo de una sociedad que se familiariza cada vez más con estas tecnologías, lo cual se ve reflejado en su estilo de vida; el problema es que la administración pública por lo general no acompaña este proceso. Todos en algún punto hemos tenido que realizar trámites engorrosos, colas interminables, ver cómo papeles que habíamos presentado se perdían, se traspapelaban o demoraban siglos en obtener un sellado, y ni hablar cuando vemos por las noticias la opacidad de la información pública en general, que resulta de difícil acceso o directamente esto no es posible (usted juzgue la cantidad de casos y recuérdelos, no pasaré lista aquí). Tal vez sea hora de que los servidores públicos puedan echar mano a herramientas que permitan sanear esta relación con los ciudadanos, que hoy se caracteriza por un gran nivel de desconfianza, y ver si de esta forma contribuimos a generar una ciudadanía más participativa e involucrada con la *res publica*. Es una deuda importante que tenemos con ellos.

En este punto es importante recordar que en esta relación intervienen 2 sujetos: el ciudadano y el Estado. Éste último no es cualquier sujeto, sino que posee características que lo van a distinguir, es decir prerrogativas estatales, y gracias a las cuales siempre ocupará un lugar especial; todo lo cual permite que afirmemos que los procesos que decida adoptar el Estado van a tener necesariamente un impacto considerable en todos. Estas prerrogativas no fueron meros caprichos del legislador, sino que obedecen a la necesidad de que el Estado pueda desenvolverse adecuadamente en el cumplimiento de sus funciones, pero el problema se presenta cuando la otra parte de la relación (el ciudadano) siente que la misma se ha desequilibrado, por lo que se comienza a tornar difícil de llevar y las reglas del juego ya no están tan claras (recordemos que la confianza es importante para

[15] Valentini, D. (2019). *Adopción De Tecnologías Disruptivas En La Contratación Pública: Blockchain Como Herramienta De Eficiencia, Transparencia Y Aliado Contra La Corrupción*. Recuperado el 16 septiembre de 2020 en https://www.austral.edu.ar/derecho/2019/04/01/adopcion-de-tecnologias-disruptivas-en-la-contratacion-publica-blockchain-como-herramienta-de-eficiencia-transparencia-y-aliado-contra-la-corrupcion/

[16] Al hablar de "sector público" me refiero tanto al Poder Ejecutivo como al Legislativo y Judicial, siendo comprensivo también de los niveles nacional, provincial y municipal.

cualquier construcción sólida que queramos encarar).

No es dato menor que gran parte de las iniciativas de Blockchain estén orientadas al sector público,[17] lo cual nos muestra que, si es posible tener más transparencia, rapidez, seguridad en los datos, dinamismo en las relaciones estatales y participación ciudadana, así como menos burocracia, discrecionalidad en las decisiones y opacidad en el manejo de la información. Estas iniciativas todavía se encuentran en fase experimental, razón por la cual desde ya debo adelantar que en esta materia no está todo dicho y sin posibilidad de discusión; por el contrario, nos encontramos en un momento trascendental, donde es bueno observar y aprender de lo que ocurre, y por qué no, considerar aplicarlo si el caso lo permite. A vuelo de pájaro puedo mencionar algunos casos que en próximas ediciones profundizaremos:

- Licitación Pública: podemos tomar como ejemplo patente de esto a Aragón,[18] entre otros. Si analizamos las diversas etapas que la conforman, observamos que hay posibilidad de aplicarles Smart Contracts a muchas de ellas,[19] contribuyendo de esta manera a que se respeten los plazos de entrega, la privacidad de las ofertas, la inalterabilidad de cualquier dato o fecha y poder realizar una adecuada trazabilidad durante este proceso, así como en la posterior ejecución en cuestión.[20]
- Títulos de Estudio: ya sean de nivel secundario, universitario, etc. Es posible acortar el tiempo de espera

[17] Initiative map | EUBlockchain. (2020). Recuperado el 20 de septiembre del 2020 en https://www.eublockchainforum.eu/initiative-map

[18] El Gobierno autónomo de Aragón adjudica un contrato público mediante tecnología Blockchain. (2020). Recuperado el 17 de septiembre de 2020 en https://es.cointelegraph.com/news/the-autonomous-government-of-aragon-awards-a-public-contract-using-blockchain-technology

[19] Licitaciones. (2020). Recuperado el 17 de septiembre de 2020, de https://bfa.ar/blockchain/casos-de-uso/licitaciones

[20] Un debate que deberíamos tener es respecto a la posibilidad de parametrizar y reglar criterios, y más aún en sistemas como el de la República Argentina donde, por ejemplo, la adjudicación se hace en favor de la oferta más conveniente para el organismo contratante (art. 15 del Decreto 1023/21 sobre Régimen de Contrataciones de la Administración Pública).

para su entrega final nuevamente por medio de Smart Contracts que permiten una interacción más ágil entre los organismos involucrados, así como una mayor confianza en la autenticidad del título puesto que la información se mantiene íntegra y podemos seguir el estado del proceso paso a paso.[21] [22]

- Registros Públicos: un ejemplo muy acabado de esto lo encontramos en el registro de la propiedad inmueble en Georgia.[23]
- Gestión de Documentos: pensemos en documentos de identidad, pasaportes, expedientes, etc.[24]

[21] Títulos Académicos. (2020). Recuperado el 17 de septiembre de 2020 en https://bfa.ar/blockchain/casos-de-uso/titulos-academicos

[22] Para que no haya más títulos apócrifos, cobra fuerza blockchain y una universidad argentina ya lo aplica. (2020). Recuperado el 17 de septiembre de 2020 en https://www.infobae.com/educacion/2019/01/05/para-que-no-haya-mas-titulos-truchos-cobra-fuerza-blockchain-y-una-universidad-argentina-ya-lo-aplica/

[23] Georgia utiliza Blockchain en el registro de propiedad de inmuebles - The Crypto Legal. (2020). Recuperado el 17 de septiembre de 2020 en https://thecryptolegal.com/georgia-utiliza-blockchain-en-el-registro-de-propiedad-de-inmuebles/

[24] Controlar y gestionar la identidad digital a través de Blockchain. (2020). Recuperado el 17 de septiembre de 2020 en https://www.4tic.com/software-gestion-documental-archivo/gestionar-identidad-digital-blockchain

- Prestación de Servicios: como salud, electricidad, agua, logística, etc.[25]
- Declaraciones Juradas: de funcionarios y personas públicas.
- Ejecución Presupuestaria.
- Etc.

A modo de conclusión, considero que la Blockchain es más que una moda y un mero expediente digital: más que una moda porque es integrante de una familia de nuevas tecnologías que llegaron para quedarse, y más que un expediente digital porque nos permite automatizar una serie de procesos como consecuencia del cumplimiento de una serie de condiciones,[26] lo cual representa todo un universo de oportunidades que no se agota en la simple desaparición del formato papel y su posterior evolución a un documento PDF, como podría pensarse. Se suele caracterizar a la Blockchain como disruptiva,[27] más considero que esto no es así debido a que su origen se remonta al 2009, siendo para algunos más antigua en el tiempo;[28] es decir que hace más de 10 años que apareció, y en cuestiones de tecnología sabemos que los tiempos son muy cortos debido a los constantes avances que se presentan, por lo que una década de por sí ya es una franja de tiempo bastante grande. Insisto: el avance es lento pero seguro, y su carácter de herramienta al servicio de la humanidad no debe despreciarse.

Y aquí es fundamental el aporte que puedan hacer los abogados y personas del ámbito legal, puesto que es necesario conocer los beneficios y desventajas de esta tecnología, así como velar por el cumplimiento de las garantías legales (y más en asuntos públicos), pero también tener la capacidad de hacer un juicio crítico respecto al caso en cuestión que se nos presenta. Una cosa es ser valiente, y animarse a considerar nuevas

[25] Jaimovich, D. (2020). Cómo Estonia se convirtió en el país más digital del mundo. Recuperado el 17 de septiembre de 2020 en https://www.infobae.com/tecno/2019/11/20/como-estonia-se-convirtio-en-el-pais-mas-digital-del-mundo/

[26] Smart Contracts. (2020). Recuperado el 18 de septiembre de 2020 en https://bfa.ar/blockchain/smart-contracts

[27] Entendiendo al término como indicativo de una rotura brusca. ASALE, R. (2020). disrupción | Diccionario de la lengua española. Recuperado el 19 de septiembre de 2020 en https://dle.rae.es/disrupci%C3%B3n

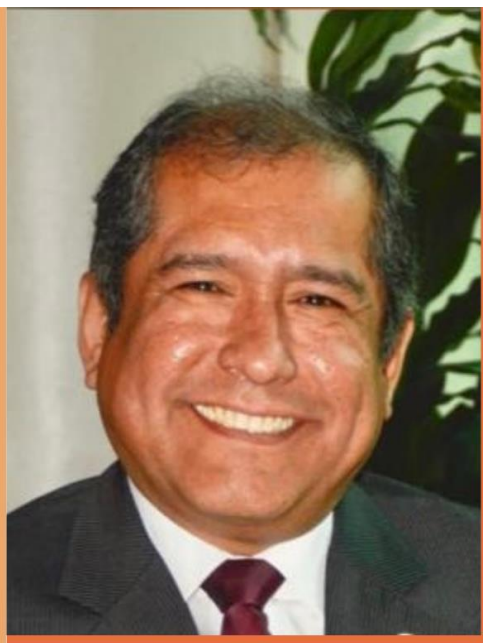
[28] Haber, S., & Stornetta, W. (1991). How to time-stamp a digital document | Journal of Cryptology. Recuperado el 19 de septiembre de 2020 en https://dl.acm.org/doi/10.1007/BF00196791

experiencias, y otra es ser temerario y pretender blockchenizar cualquier cosa que se nos cruce. Tarea fundamental y para nada fácil será que nos detengamos a analizar cada caso puntual, ver si hay algo que mejorar (tal vez no sea así) y qué alternativas tenemos, cuidando de nunca olvidar que el principal destinatario de lo que hagamos será el ciudadano.

Ante todo, transparencia.

¿ES NECESARIA UNA REGULACION ESPECIAL DE FIRMA ELECTRONICA EN EL PERU?

CARLOS
PEDROZA BARRIOS*



RESUMEN

Con el avance de las nuevas tecnologías, los distintos campos del derecho se han visto trastocados en cuanto a su uso o aplicación en diversos temas jurídicos entre los cuales se encuentra la firma manuscrita respecto de la firma electrónica como sustituto de aquella en ambientes puramente electrónicos como la manifestación de voluntad. Si bien es cierto que la firma digital está siendo utilizada mayormente como una solución práctica en estos momentos, no podemos dejar de lado a la firma electrónica como genero para lo cual el autor plantea que se dé una regulación especial al respecto.

PALABRAS CLAVE

Firma electrónica / Firma Digital / Firma manuscrita

MARCO NORMATIVO

Ley 27269: Ley de firmas y certificados digitales
Decreto Supremo N° 052-2008-PCM: Reglamento de la ley de firmas y certificados digitales

---

La ley de firmas y certificados digitales[29] regula la utilización de la firma electrónica otorgándole la

[29] Ley N° 27269: Ley de firmas y certificados digitales

misma validez y eficacia jurídica que el uso de la firma manuscrita u otra análoga que conlleve manifestación de voluntad[30].

Como podemos apreciar dicha norma lo que busca es regular la firma electrónica en todas sus modalidades como un género. Luego en el artículo 3ro y demás de la ley, esta se dedica a desarrollar la firma digital, que viene a ser una especie del género firma electrónica[31]. Podemos pues decir en un primer momento que lo que la norma nos indica es que si bien regula la firma electrónica, en el fondo lo que busca es regular al detalle la firma digital desviándose del objeto de la ley indicada.

La ley modelo de la CNUDMI[32] regula la firma electrónica y no la digital por el principio de neutralidad tecnológica en su artículo 2 inciso a), indicando que por "***firma electrónica*** *se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos*".

Así también la Ley Modelo de la CNUDMI sobre Comercio Electrónico[33] en su artículo 7 – Firma en el párrafo 1) nos indica:

> 1) *Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:*
>
> *a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y*
> *b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del*

[30] Primer párrafo del artículo 1° de la Ley N° 27269

[31] "… la doctrina tratan a la firma electrónica como el género y a la digital como una especie de la primera. (…)". Citado en el libro "El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas" página 19

[32] Ley modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al Derecho Interno – Año 1996

[33] Ley modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al Derecho Interno – Año 1996

caso, incluido cualquier acuerdo pertinente.

Regresando a lo indicado por nuestra ley n° 27269 de firmas y certificados digitales en su artículo 1[34], podemos precisar que lo que se solicita respecto de la firma en los documentos electrónicos es:

a. Identificar al firmante (la persona)
b. Asociar a esa persona con el contenido del documento, y
c. Seguridad de la participación de esa persona en el acto de firmar propiamente

Entonces podemos tener una primera conclusión, en el sentido, que nuestra norma busca concentrarse en dos funciones básicas de la firma:

a. La identificación del generador o autor del documento, y
b. Certeza que este generador o autor del documento manifiesta su intención de vincularse con dicho documento

Lo importante del presente tema, radica que podemos afirmar que "la firma electrónica es un método de seguridad informática y documental asociado a la incorporación de datos en forma digital que permitan las funciones de autenticidad, integridad y no repudio respecto del contenido de un mensaje de datos"[35]. Por lo tanto, este mecanismo debe ser fiable y apropiado. Para la ley modelo de la CNUDMI[36], una firma electrónica es fiable si:

a) los datos de creación de la firma, en el contexto en que

[34] **Artículo 1.- Objeto de la ley**

La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

[35] Peña Valenzuela, Daniel. "De la firma manuscrita a las firmas electrónica y digital". Página 124

[36] Párrafo 3° del artículo 6° de la Ley modelo de la CNUDMI

son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Este método para ser apropiado, debe tomar en cuenta, entre otros, los siguientes factores jurídicos, técnicos y comerciales[37]:

a) la perfección técnica del equipo utilizado por cada una de las partes;

b) la naturaleza de su actividad comercial;

c) la frecuencia de sus relaciones comerciales;

d) el tipo y la magnitud de la operación;

e) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable;

f) la capacidad de los sistemas de comunicación;

g) la observancia de los procedimientos de autenticación establecidos por intermediarios;

h) la gama de procedimientos de autenticación que ofrecen los intermediarios;

i) la observancia de los usos y prácticas comerciales;

j) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados;

k) la importancia y el valor de la información contenida en el mensaje de datos;

l) la disponibilidad de otros métodos de identificación y el costo de su aplicación;

m) el grado de aceptación o no aceptación del método de identificación en el sector o la esfera pertinente, tanto en el momento en el que se acordó el método como en el que se comunicó el mensaje de datos; y

n) cualquier otro factor pertinente (Guía para la incorporación al derecho interno de la Ley Modelo de

[37] Párrafo 75 de la Segunda Parte – Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001, página 40

la CNUDMI sobre Comercio Electrónico, párrs. 53 y 56 a 58).

Es importante recordar que las firmas electrónicas se vienen usando hace muchas décadas – principalmente en el sector privado – con el fin de poder identificarse y generar documentos electrónicos, mensajes de datos fiables, entre otros. Esto es lo que se conoce como el Intercambio electrónico de documentos o Electronic Document Interchange (EDI). Si bien es cierto con el devenir del tiempo, la firma digital ha surgido como una alternativa, ambas (la electrónica y digital) son perfectamente válidas y aceptadas por la normativa y no podemos afirmar que una sea más segura y confiable que otra. Para determinar el uso de alguna de ellas, deberá entonces asegurarse lo señalado líneas arriba:

a. La identificación del generador o autor del documento, y
b. Certeza que este generador o autor del documento manifiesta su intención de vincularse con dicho documento

Quisiera a continuación mencionar algunos aspectos señalados en un estudio de la CNUDMI titulado "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas"[38]:

a. La definición de "firma electrónica" en los textos de la CNUDMI es deliberadamente amplia, para que abarque todos los métodos de "firma electrónica" existentes o futuros. Siempre que el método utilizado "es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos," a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente, se deberá considerar que cumplen las prescripciones legales en materia de firma. Los textos de la CNUDMI relativos al comercio electrónico, así como un gran número de otros textos legislativos, se basan en el principio de la neutralidad tecnológica y por lo tanto pretenden dar cabida a todas las formas de firma electrónica. Así pues, la definición de firma electrónica dada por la CNUDMI abarcaría todo el abanico de técnicas de "firma electrónica", desde los altos niveles

[38] CNUDMI "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas", Viena, 2009

de seguridad, como los sistemas de garantía de la firma basados en criptografía asociados a un sistema de ICP (una forma habitual de "firma digital" (…), hasta los niveles de seguridad más bajos, como códigos o contraseñas no cifrados. La mera inclusión del nombre mecanografiado del autor al final de un mensaje de correo electrónico, que es la forma más habitual de "firma" electrónica, por ejemplo, cumpliría la función de identificar correctamente al autor del mensaje siempre que no sea infundado utilizar un nivel tan bajo de seguridad[39].

b. En el curso de los años se ha creado una serie de distintas técnicas de firma electrónica. Cada una de ellas tiene por objetivo atender a distintas necesidades y proporcionar distintos niveles de seguridad y también entraña diferentes requisitos técnicos. Los métodos de autenticación y firma electrónicas pueden clasificarse en tres categorías, a saber: los que se basan en lo que el usuario o el receptor sabe (por ejemplo, contraseñas, números de identificación personal (NIP)), los basados en las características físicas del usuario (por ejemplo, biométrica) y los que se fundamentan en la posesión de un objeto por el usuario (por ejemplo, códigos u otra información almacenados en una tarjeta magnética. En una cuarta categoría se podría incluir a diversos tipos de métodos de autenticación y firma que, sin pertenecer a ninguna de las categorías arriba citadas, podrían también utilizarse para indicar el iniciador de una comunicación electrónica (por ejemplo, un facsímil de una firma manuscrita, o un nombre mecanografiado en la parte inferior de un mensaje electrónico). Entre las tecnologías que se utilizan en la actualidad figuran las firmas digitales en el marco de una infraestructura de clave pública (ICP), dispositivos biométricos, NIP, contraseñas elegidas por el usuario o asignadas, firmas manuscritas escaneadas, firmas realizadas por medio de un lápiz digital, y botones de pulsación del tipo de "sí" o "aceptar" o "acepto". Las soluciones híbridas basadas en la combinación de distintas tecnologías están adquiriendo una aceptación creciente,

[39] Ibídem, párrafo 21, página 15

como por ejemplo en el caso del uso combinado de contraseñas y sistemas TLS/SSL (seguridad del estrato de transporte/estrato de zócalos seguro), que es una tecnología en la que se utiliza una combinación de cifrados de clave pública y simétrica. Las características de las principales técnicas de uso actual se describen infra (…)[40].

c. La firma digital funciona bien como un medio para verificar las firmas que se crean durante el período de validez de un certificado. Sin embargo, cuando el certificado caduca o se revoca la clave pública correspondiente pierde validez, aunque no esté en entredicho el par de claves. Por ello, todo mecanismo de ICP requeriría un sistema de gestión de la firma digital para asegurar que la firma siga disponible a lo largo del tiempo. La dificultad principal proviene del riesgo de que los registros electrónicos "originales" (esto es, los dígitos binarios o "bitios" que conforman el fichero informático en que se registra la información), incluida la firma digital, pueden resultar ilegibles o poco fiables con el tiempo, principalmente por la obsolescencia del programa, del equipo físico o de ambos. De hecho, la firma digital podría resultar insegura por los avances científicos en materia de criptoanálisis; el programa de verificación de las firmas podría faltar durante períodos prolongados, o el documento podría perder su integridad. Por ello, la conservación a largo plazo de la firma electrónica es en general problemática. Aunque por un tiempo se consideró que la firma digital era indispensable a efectos de archivo, la experiencia ha demostrado que no está exenta de riesgos a largo plazo. Como toda modificación del registro posterior al momento de creación de la firma dará lugar a que la verificación no funcione, las operaciones de reformateado destinadas a mantener la legibilidad futura del registro (como la "migración" o la "conversión") pueden afectar a la durabilidad de la firma. En realidad, la firma digital se concibió más para dar seguridad a la comunicación de información que para conservarla. Las iniciativas para superar este problema

[40] Ibídem párrafo 16, página 13

todavía no han dado con una solución duradera[41].

d. Un volumen importante de operaciones comerciales electrónicas se lleva a cabo en redes cerradas, es decir, en grupos con un número limitado de participantes a los que pueden acceder únicamente personas o empresas previamente autorizadas. Las redes cerradas apoyan el funcionamiento de una sola entidad o de un grupo de usuarios cerrado ya existente, como las instituciones financieras participantes en el sistema de pagos interbancarios, las bolsas de valores y productos básicos, o una asociación de líneas aéreas y agencias de viajes. En tales casos, la participación en la red se suele restringir a instituciones y empresas admitidas previamente en el grupo. La mayoría de dichas redes han existido desde hace varios decenios, emplean tecnología muy avanzada y han adquirido un alto nivel de pericia en el funcionamiento del sistema. El rápido crecimiento del comercio electrónico en el último decenio ha dado lugar a la aparición de otros modelos de redes, como las cadenas de suministro o las plataformas comerciales[42].

Por lo citado líneas arriba, podemos afirmar y sustentar que existen diferentes métodos de firma electrónica, donde se encuentra la firma digital como una especie de aquella. La firma electrónica como genero puede servir para determinados procesos, trámites, etc.; así como la firma digital en algunos casos será la más pertinente.

Por lo que podemos precisar que en nuestro país:

a. Es perfectamente válido el uso de firmas electrónicas como género, dentro de la cual se encuentra la firma digital como especie (cuyo uso también es válida)
b. Las firmas electrónicas deben ser admitidas como medio de prueba toda vez que estas deben garantizar:
   b.1 La identificación del generador o autor del documento, y
   b.2 Certeza que este generador o autor del documento manifiesta su intención de vincularse con dicho documento
c. El Decreto Supremo N° 052-2008-PCM Reglamento de la ley de firmas y certificados

[41] Ibídem párrafo 51, página 26

[42] Ibídem párrafo 79, página 37

digitales en su artículo 1° segundo párrafo[43] - como se encuentra redactada en estos momentos - no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas, siempre que cumplan los requisitos establecidos en el artículo 2° de la ley 27269[44], pero no regula el uso de la firma electrónica.

d. Sin embargo, solo tenemos algunas referencias o menciones sobre la firma electrónica en el artículo 2° de la ley y en las definiciones del Decreto Supremo N° 052-2008-PCM Reglamento de la ley de firmas y certificados digitales:

d.1 Sobre la Neutralidad Tecnológica, entendida como la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que puedan utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información[45].

[43] **Artículo 1°.- Del objeto**
(…).
Reconociendo la variedad de modalidades de firmas electrónicas, la diversidad de garantías que ofrecen, los diversos niveles de seguridad y la heterogeneidad de las necesidades de sus potenciales usuarios, la Infraestructura Oficial de Firma Electrónica no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas, siempre que cumplan los requisitos establecidos en el artículo 2° de la Ley.

[44] **Artículo 2.- Ámbito de aplicación**
La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

[45] **Neutralidad tecnológica.-** Es el principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente; asimismo, implica la no discriminación, preferencia o restricción de ninguna de las

d.2 Respecto del No Repudio en su relación con lo mencionado en el Artículo 2° de la Ley 27269[46].

d.3 Se menciona un Sistema de Intermediación Electrónico, indicando el uso de componentes de firma electrónica[47].

d.4 Por ultimo, se define la Infraestructura Oficial de Firma Electrónica, mencionando únicamente la generación de firmas digitales, dejando de lado las firmas electrónicas, no obstante lo señalado en el artículo 2° de la Ley 27269[48].

diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.

[46] **No repudio.-**
(…).
En el ámbito del artículo 2° de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

[47] **Sistema de Intermediación Electrónico.-** Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros.

[48] **Infraestructura Oficial de Firma Electrónica.-** Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de:

Por lo mismo que la Ley 27269 establece el concepto de firma electrónica y su reconocimiento mediante su uso, resaltamos que el reglamento actual de la Ley mencionada[49], se dedica exclusivamente a reglamentar la firma digital y desarrollar todo lo referente al Infraestructura oficial de firma electrónica (OIFE) que se dedica exclusivamente a tomar en cuenta la firma digital como instrumento de uso en el país.

Pero no debemos olvidar que la ley 27269 regula la firma electrónica dándole el mismo valor que la firma manuscrita y por lo tanto estimamos que debe reglamentarse su uso, disponibilidad y consecuencia de su utilización.

A nuestro entender, debería darse un reglamento o una norma especial que desarrolle la firma electrónica como parte del sistema nacional, por cuanto es importante su desarrollo tomando en cuenta que su uso viene dándose décadas atrás en nuestro país y puede perjudicar actualmente si todo se direcciona – como aparentemente – se deduce de la normativa como esta legislada actualmente a la firma digital.

Por último, a modo de conclusión final, esta normativa debería basarse o construirse en base a lo siguiente:

a. Acuerdo EDI.- mediante el acuerdo de voluntades donde se estipularan las condiciones legales a que se ajustaran las partes para realizar comunicaciones, transacciones o cualquier otra actividad mediante el uso del intercambio electrónico de datos (EDI).
b. Respecto de la firma electrónica; verificar los datos (que serían únicos y personales) como códigos, contraseñas, biometría o claves criptográficas que se

1) La integridad de los documentos electrónicos;
2) La identidad de su autor, lo que es regulado conforme a Ley.

El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

[49] Decreto Supremo N° 052-2008-PCM Reglamento de la ley de firmas y certificados digitales

usaran para crear la firma electrónica.

c. Rescatar el concepto de firma electrónica de la ley 27269.
d. Reiterar el principio de neutralidad tecnológica.
e. Establecer la confiabilidad de la firma electrónica, estableciendo sus requisitos.
f. Verificar el valor jurídico de la firma electrónica indicando que esta tendrá la misma fuerza que la firma manuscrita u otros tipos diferentes a la firma digital.
g. Indicar la admisión y valor probatorio de la firma electrónica.
h. Deberá también establecer los criterios de seguridad de las firmas electrónicas de acuerdo a la normativa técnica que emitiría el INACAL.

Grooming - Ponencia del Congreso Locademia Joven

Juan David: Ingeniero de Sistemas y Especialista en Seguridad Informática
Christopher: Técnico Universitario en Redes de Computadoras
Emilse Maria del Milagro: Abogada, profe adscripta UNC

¿Qué es el grooming?

- “Grooming” es el acoso sexual de una persona adulta a un niño, niña o adolescente por medio de Internet.
- Las personas que realizan grooming se llaman groomers o acosadores.

<u>Elementos característicos</u>

- Medio: tics.
- Componente sexual
- Sujeto activo: GROOMER
- Sujeto pasivo: NNYA

¿Qué ley protege a los niños, niñas y adolescentes del grooming?

Desde diciembre del 2013 se incorporó el grooming como delito al Código Penal. El artículo 131 establece una pena de prisión de 6 meses a 4 años.

¿Cómo actúa la persona acosadora?

El acosador suele crear un perfil falso en redes sociales, aplicaciones, videojuegos multijugador u otro medio social. Se hace pasar por una persona menor de edad para generar confianza y tener una relación de amistad con niños, niñas o adolescentes.

Luego, el acosador le pide a la víctima fotos o videos con contenido sexual.

Cuando lo consigue, chantajea y amenaza al niño, niña o adolescente con hacer público ese material si no envía nuevas fotos o

videos o si no acepta un encuentro personal. Otras veces, si existe una relación de confianza, puede que la víctima acceda a un encuentro personal con el acosador.

En otras ocasiones, el acosador obtiene fotos o videos sexuales de la víctima sin necesidad de contacto previo, mediante el robo de contraseñas, hackeo de dispositivos o de cuentas. Posteriormente inicia el período de chantaje.

El grooming puede derivar en otros graves delitos:

- Pornografía infantil
- Trata de personas
- Abuso sexual
- Homicidio

El acosador usa distintas estrategias:

- Se hace pasar por una persona menor de edad de edad con fotos o videos falsificados o alterados.
- Se crea más de un perfil falso y genera muchas identidades.
- Adapta su lenguaje para generar confianza (usa la misma “jerga”).
- Aprovecha la información que los niños, niñas o adolescentes comparten en las redes sociales o servicios de mensajería instantánea sobre sus gustos y preferencias.
- Entabla amistad en juegos en línea de moda para conseguir información personal.
- Usa el tiempo para fortalecer el vínculo.

¿Cómo detectar el grooming?

Se debe prestar atención a los cambios de conducta o humor del niño, niña o adolescente: si presenta repentina tristeza, baja su rendimiento escolar o quiere estar solo, si se observa nerviosismo, o ansiedad respecto del uso de los dispositivos (por ejemplo en el caso de estar siendo amenazado/a y debe responder a los mensajes).

¿Qué hacer ante un caso de grooming?

Con el niño, niña o adolescente:

- Dialogar.
- Evitar avergonzarlo o culparlo para que pueda contar con sinceridad lo que le pasó.
- Evitar interrogarlo.
- Acompañarlo con afecto con el objetivo de protegerlo.

Con los datos intercambiados entre el acosador y el niño, niña o adolescente:

- Reunir toda la información y hacer la denuncia en la fiscalía más cercana.
- No borrar contenido de la computadora o teléfono celular.
- Guardar las conversaciones, las imágenes y los videos que el acosador y la víctima

se enviaron porque sirven de prueba.
- Descargar las fotos o cualquier otro material enviado por el acosador.
- Revisar la computadora o teléfono celular usada por la víctima, cambiar las claves de acceso y controlar que no tenga un software malicioso (malware).
- Cambiar las claves de acceso a las redes sociales.
- Limitar la lista de contactos y configurar la privacidad en las redes sociales. Hablar con el niño, niña o adolescente sobre la importancia de incluir en la lista de contactos solo personas conocidas.

Con el acosador:

- No denunciarlo en la red social o plataforma web. Si lo denuncias el administrador del sitio web puede bloquear como usuario al acosador. Al ser bloqueado se pierde la información para hacer la investigación y el acosador puede crear un nuevo perfil y seguir acosando a otros niños, niñas y adolescentes.
- No amenazarlo ni enfrentarlo.
- Denunciarlo en la fiscalía o comisaría más cercana.

Consejos para prevenir el grooming:

Entender que los niños, niñas y adolescentes de esta generación viven en un contexto digital y no distinguen entre el “mundo offline” (“físico”) y el “mundo online” (Internet). Su universo está poblado de amigos/as virtuales. Los nombres de los amigos suelen cambiar de una red a otra y por eso no siempre pueden identificarlos en las redes

No prohibir que los niños, niñas o adolescentes tengan amigos virtuales. Darles herramientas para que conozcan y comprendan los riesgos que tiene compartir datos personales en la web, redes sociales y servicios de mensajería instantánea.

Reforzar que más allá de la confianza y la amistad que se haya generado, las personas desconocidas con las que se relacionan por medio de Internet siguen siendo desconocidas. Explicar que es muy fácil abrir un perfil con datos falsos.

Buenas prácticas para prevenir el grooming:

- Los adultos deben usar con responsabilidad sus propias redes sociales. Configurar la privacidad y evitar compartir fotos de sus hijos e hijas con el uniforme del colegio o con información que permita conocer el barrio o domicilio en forma pública.
- No facilitar información o imágenes comprometedoras

por medios electrónicos porque es difícil borrar el material que circula en Internet.

- No hacer videoconferencias con desconocidos. Al mostrarse por medio de una cámara se exponen frente a un desconocido que puede filmarlos o fotografiarlos y luego hacer circular esa imagen por la web o usarla para futuras extorsiones.
- Configurar los controles parentales en televisores, cables y plataformas de contenidos.
- Configurar la privacidad en las redes sociales y aplicaciones. Dentro de las herramientas de privacidad que tienen las redes sociales existen opciones más avanzadas: armar subgrupos entre los contactos y elegir qué información ve cada grupo, controlar las etiquetas antes de publicar contenido en el muro, bloquear un perfil, entre otros

¿Cómo evitar el robo de imágenes?

- Poner contraseñas en todos los dispositivos utilizados (teléfono celular, tableta, netbook, notebook o computadora de escritorio).
- Usar contraseñas seguras, fáciles de recordar pero difíciles de adivinar. Lo recomendable es mezclar números y letras, signos de puntuación y caracteres de otro tipo. Evitar datos predecibles.
- No compartir las contraseñas. En el caso de niños y niñas se recomienda que los padres conozcan las contraseñas que usan.
- Evitar usar la misma contraseña para todas las cuentas y dispositivos.
- Evitar usar nombres completos y datos personales en las direcciones de mail. Pueden usarse frases, seudónimos, alias, entre otros.
- Evitar descargar e instalar software y aplicaciones de tiendas no oficiales.
- No usar el nombre completo como nick o usuario en las redes sociales. Es preferible colocar sobrenombres y evitar el apellido.
- Es importante que los padres tengan una actitud presente y activa mientras los niños, niñas y adolescentes navegan por internet.
- Tener presencia en la “vida online” de sus hijos significa conocer las páginas web que visitan, las redes sociales que usan y las personas con las que se relacionan.
- Conocer las páginas que sus hijos visitan con frecuencia. Es necesario que conozcan las políticas de privacidad,

reglas y características de cada sitio.
- Acompañar a sus hijos aunque sientan que saben menos que ellos sobre las Tecnologías de la Información y la Comunicación (TIC).
- Dar a los niños, niñas y adolescentes herramientas para distinguir entre el “mundo offline” y el “mundo online” y entre aquellos amigos que conocen personalmente y aquellos que conocen por medio de la web.
- Dialogar con los hijos para que puedan compartir sus preocupaciones e inquietudes.
- Respetar la privacidad de los niños, niñas y adolescentes (por ejemplo, no ingresar a escondidas a sus cuentas o casillas de email).
- Trabajar en forma proactiva con los educadores y las instituciones educativas

Derecho y Tecnología

EL SUPLEMENTO LEGAL DE NEURONA BA

CON EL OBJETIVO DE ACOMPAÑAR EL DEBATE ACERCA DE LA EXPANSIÓN EN EL USO DE LAS TIC Y SU IMPACTO EN EL DERECHO, DESDE NEURONA BA LANZAMOS ESTE SUPLEMENTO SOBRE "DERECHO Y TECNOLOGÍA". TIENE LA COORDINACIÓN DE NUESTRO COLUMNISTA HABITUAL, EL ABOGADO, DOCENTE E INVESTIGADOR, ERNESTO LICEDA, CON UNA AMPLIA TRAYECTORIA EN ESTAS TEMÁTICAS.

AUTORES

ERNESTO LICEDA // Coordinador del suplemento legal Tecnología y Derecho de Neurona BA.

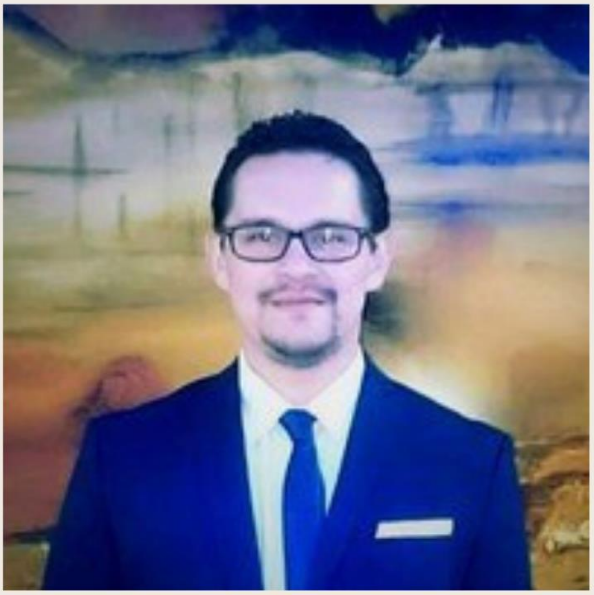
ERNESTO ÁNGELES GUERRERO // Maestro por la Universidad Nacional Autónoma de México. Presentador e investigador en InfodemiaMX.

JOSÉ M. LEZCANO // Docente Investigador en el GECSI, Facultad de Ciencias Jurídicas y Sociales, UNLP.

LUCÍA VAZQUEZ // Directora Provincial de la Dirección de Mediación de la provincia de Buenos Aires, y Yael Falótico, Directora en la Dirección provincial de Mediación.

ARIEL H. SIMONE // Relator en la Fiscalía de Casación Penal, Ministerio Público de la Provincia de Buenos Aires.

HERNÁN A. GHIRARDI // Perito Informático en Poder Judicial, Provincia de Buenos Aires, Ministerio Público.



BLOCKCHAIN Y CRIPTOMONEDAS: MECANISMOS DE NEGOCIACIÓN, VENTAJAS Y RIESGOS[1]

AUTOR: AB. DARÍO ECHEVERRÍA MUÑOZ. MSC, LL.M

(23 DE SEPTIEMBRE DE 2020). LOCADEMIA JOVEN DE DERECHO Y TECNOLOGÍA -

1. GENERALIDADES

La criptomoneda consiste en una moneda virtual utilizada como medio de intercambio sin la presencia de un regulador central, el *bitcoin* fue creado en 2008 por alias "Satoshi Nakamoto"[50]. Entre sus características principales destaca que no es una moneda vinculada a una determinada economía, pero como sucede en todo mercado financiero, su fuente principal de inversión es la especulación, con el cual su valor puede subir o bajar dependiendo de la volatilidad del mercado en el que se negocia.

El mercado de criptomonedas al ser descentralizado no es afectado por sucesos económicos, políticos y sociales a diferencia del mercado financiero que, si sufre la influencia de las divisas tradicionales, sin embargo, a pesar de la incertidumbre que genera el mercado de criptomonedas, estos son los factores que lo influyen:

- **Oferta:** el ofrecimiento de la criptomoneda en el mercado.
- **Demanda:** la intención de los inversionistas por adquirir criptomonedas.
- **Capitalización:** el valor que las criptomonedas adquieren en el mercado y cómo los usuarios perciben su fluctuación y volatilidad.

[50] (Nakamoto, 2008)

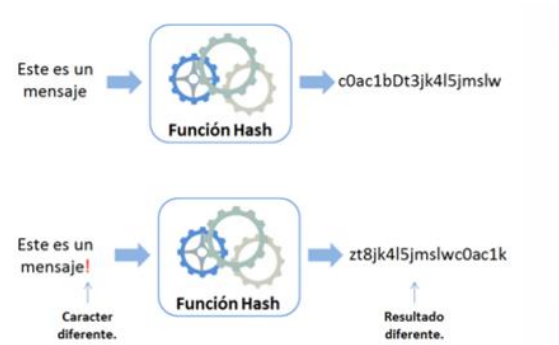
- **Prensa:** todo medio escrito o digital en el que se informa al público
- **Integración:** el grado de infraestructura existente y su vinculación en los sistemas de pagos para su adquisición.
- **Hechos relevantes:** aquellos sucesos o circunstancias que afectan al mercado de criptomonedas como cambios regulatorios, fallos de seguridad o acontecimientos económicos.

2. PROCESO DE LAS TRANSACCIONES DE LAS CRIPTOMONEDAS

El procedimiento de negociación de las criptomonedas para vincular la oferta y demanda entre sus participes, conlleva a un proceso conocido como minería de datos que, a través de la cadena de bloques (blockchain) se validan las transacciones mediante los procedimientos de *hash* y criptografía asimétrica, el cual perfecciona la transacción con el monto negociado en el mercado de criptomonedas.

a) ***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.

Ejemplo:



Input	Hashing algorithm: SHA-1
Fox	dfcd3454bbea788a751a696c24d97009ca992d17
fox	ff0f0a8b656f0b44c26933acd2e367b6c1211290
fox1	fcb9f413aa14b3fbec3c29d53dcf880994282874

b) **Criptografía asimétrica:** Es un método a nivel de tecnologías de la información, el cual utiliza un par de claves para el envío de mensajes de datos, ambas son de propiedad de la persona que realiza la transacción de criptomonedas.

b.1) Clave pública: es una llave que tiene acceso público el cual el emisor utiliza al realizar la transacción para cifrar el mensaje y a su vez el receptor lo valida una vez que esta fue perfeccionada.

b.2) Clave privada: es una llave de acceso restringido que solamente está en poder de su propietario, el emisor valida la transacción para enviar el mensaje y el receptor lo descifra

una vez perfeccionada la negociación de criptomonedas.

3. ELEMENTOS DE LAS TRANSACCIONES DE LAS CRIPTOMONEDAS

El proceso de transacción de las criptomonedas también se compone de elementos necesarios para su perfeccionamiento y estos son los siguientes:

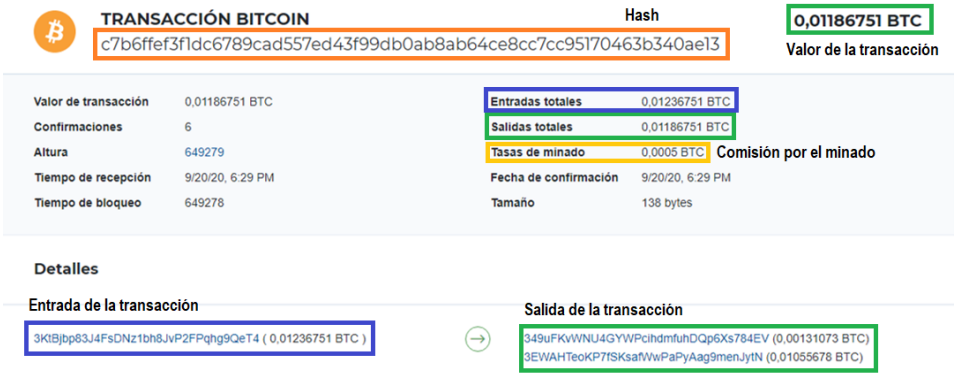
3.1. Entradas (*inputs*): Consisten en las referencias de origen de la transacción, esto es, donde proceden las transferencias y contienen la dirección donde originalmente se transarán las criptomonedas.

3.2. Salidas (*outputs*): Estas contienen la dirección de destino para perfeccionar la transferencia y la cantidad negociada en criptomonedas, estas pueden ser una o varias.

3.3. *Hash:* Cada transacción realizada tendrá siempre esta característica y esto consiste en ser un identificador único generado a partir de las entradas y salidas generadas en la negociación de criptomonedas volviéndolo un valor único e irrepetible dentro de la cadena de bloques.

3.4. Tasa de comisión: Es el pago que reciben los mineros por procesar una transacción de criptomonedas, siempre tendrán reconocimiento económico cada vez que se genere un nuevo bloque.

En la siguiente imagen están resaltados todos los elementos explicados anteriormente dentro de una transacción de bitcoin realizada el 20 de septiembre del 2020 en el explorador de bloques Bit2Me:[51]



4. VENTAJAS Y RIESGOS DE LAS CRIPTOMONEDAS

El desarrollo de este tipo de moneda ha generado expectativas y varios beneficios para sus usuarios

[51] https://explorer.bit2me.com/btc/block/0000000000000000ca6013b6579e88049320a156efb34888fd0a982d07c3a

en relación con la moneda tradicional, y resulta interesante saber qué beneficios trae consigo.

4.1. Anonimato: Los usuarios realizan las transacciones a través de seudónimos, en este sentido cada persona es identificada a través de una clave alfanumérica pública con la finalidad de resguardar su identidad.

4.2. Seguridad: Tiene como base la criptografía y firmas digitales, el cual crea un sistema único programado para validar operaciones complejas y resolver conflictos propiciando que ningún tercero pueda modificar las transacciones realizadas volviéndolas irreversibles, además que vuelve imposible la falsificación o duplicación de las criptomonedas.

4.3. Código abierto: Al estar en una red descentralizada, cada transacción de criptomonedas consta en un registro único irrevocable que constituye un libro abierto público,[52] lo cual hace que sea transparente.

4.4. Confianza: Al ser un sistema autónomo, las transacciones entre usuarios se realizan sin la intervención de intermediarios y su control lo llevan quienes transan las criptomonedas, además que este mercado no tiene influencia externa que influya en la fluctuación de precios.

4.5. Inmediatez: Los procesos de transacción de criptomonedas son ágiles, lo que otorga celeridad en su negociación evitando cualquier retraso innecesario.

5. RIESGOS DE LAS CRIPTOMONEDAS

Al mismo tiempo, las criptomonedas están sujetas a diversos riesgos y desventajas que aún evitan el asentamiento de este mercado en la sociedad y su desconfianza en gran parte de los usuarios.

5.1. Riesgos regulatorios: Al no existir todavía una regulación en criptomonedas, no hay supervisión a este mercado, lo que genera una falta de control en determinar el origen de los activos, conllevando a ser un medio de pagos ilícitos o transacciones favorables para el mercado negro, terrorismo, entro otros.

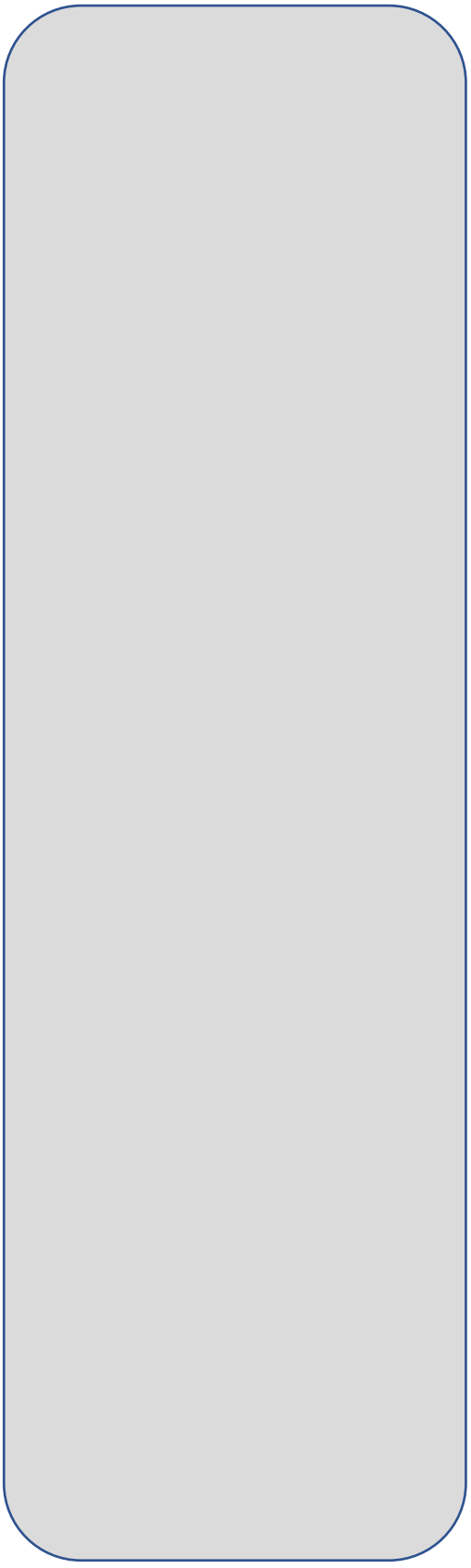
5.2. Riesgos en ciberseguridad: Al no existir políticas claras de protección de datos y faltas en los sistemas de seguridad en las plataformas a favor de los usuarios, explota la

[52] https://explorer.bit2me.com / https://www.blockchain.com

vulnerabilidad (hacking) para la filtración de información causando perjuicios a sus participes en el robo de datos personales y montos en criptomonedas.

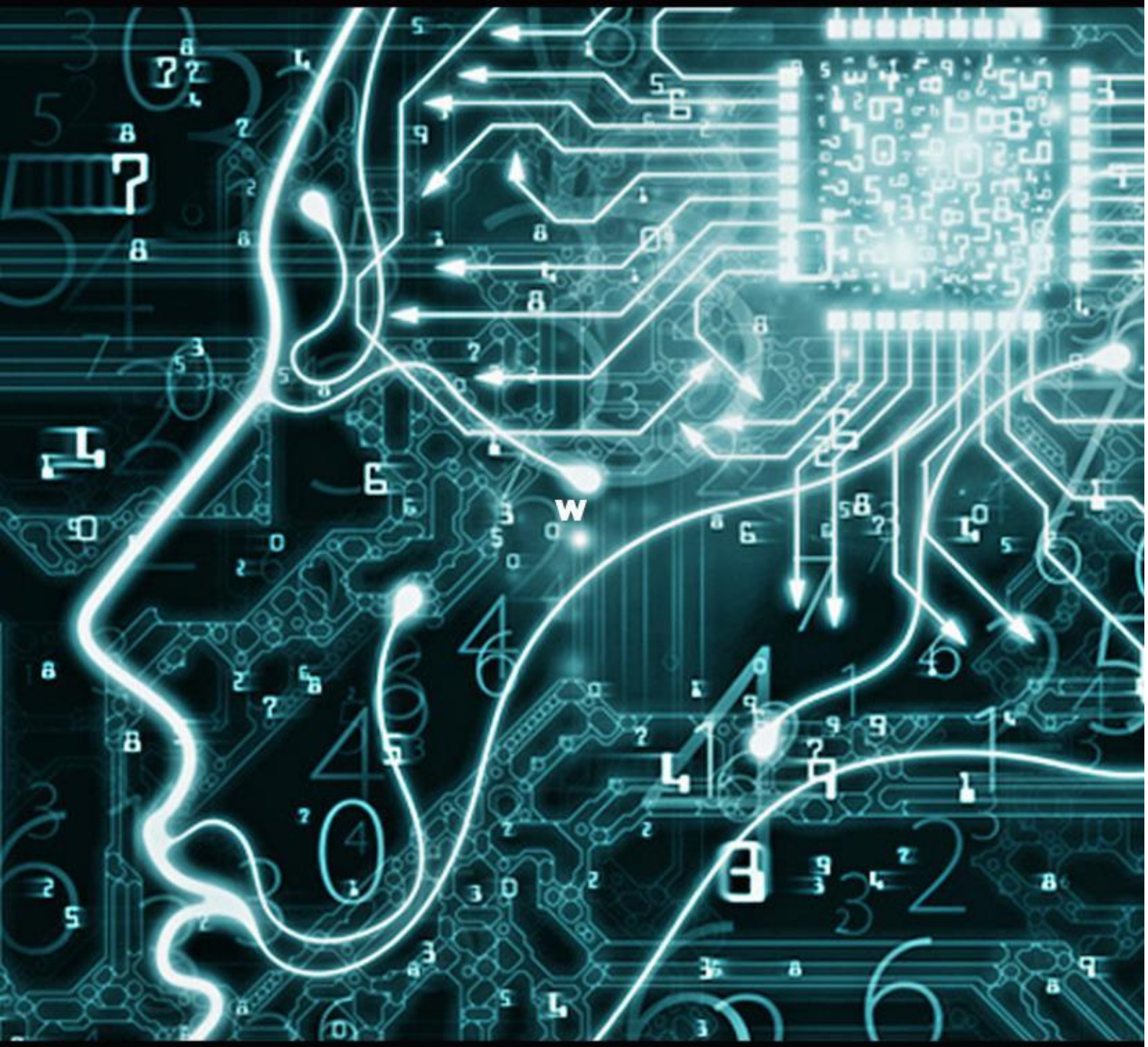
5.3. Riesgos especulativos: Como todo mercado, este se alimenta de la especulación, cuya volatilidad provoca la alteración de precios y su fluctuación repentina e imprevista, puede provocar pérdidas financieras a los usuarios.

5.4. Riesgos de estafa y fraude: Al ser un medio de captación de recursos, es llamativo para fines criminales y publicidad que promete a potenciales usuarios obtener rendimientos elevados en el corto plazo, siendo tácticas utilizadas por las pirámides financieras o estafadores, conllevando a la desconfianza de este mercado.



OCEDIC

OBSERVATORIO DE CIBERCRIMEN Y EDIVENCIA DIGITAL
EN INVESTIGACIONES CRIMINALES



OCEDIC@AUSTRAL.EDU.AR

/OCEDIC

OCEDIC.COM

/OCEDIC.UA

UNIVERSIDAD AUSTRAL | DERECHO
Departamento de Derecho Penal y Procesal Penal

¿Los Smart Contracts son realmente una novedad para el legislador venezolano?

María Alejandra Ruiz[1]

[1] Abogada Magna Cum Laude de la Universidad Central de Venezuela, cursante de la Maestría de Derecho Internacional Privado y Comparado de la Universidad Central de Venezuela. Asociada del departamento de litigios del escritorio jurídico Baker Mckenzie. Profesora de Derecho Procesal en la Universidad Monteávila..

Hemos estado expuestos a un sinfín de noticias sobre la novedad de lo que actualmente se denomina "Smart Contracts" o "Contratos Inteligentes", entendiéndose por éstos aquellos "*contratos en formato electrónico y de carácter autoejecutable*"[53] que i) se encuentran redactados en un lenguaje informático, ii) normalmente utilizan la tecnología de la cadena de bloques o "blockchain", principalmente pero no exclusivamente, por su característica de inmutabilidad, y iii) deben ejecutar primordialmente obligaciones y controlar activos, según declaraciones de Nick

[53] Marina Echebarría Saenz. "Contratos Electrónicos Autoejecutables (Smart Contract) y Pagos con Tecnología Blockchain". Revista de Estudios Europeos Nº 70 julio-diciembre. 2017. pp. 69-97. Consultado en: http://uvadoc.uva.es/bitstream/10324/28434/1/Estudios-Europeos-2017-70-Contratos-electr%C3%B3nicos-autoejecutables...%2869-97%29.pdf

Szabo[54]. Es común leer artículos que señalan la necesidad de un nuevo marco legal que regule y atienda las características propias de este tipo de contratos, haciendo hincapié en la incertidumbre legal que pueden generar su utilización, principalmente, por encontrarnos frente a una figura en formato electrónico que no requiere de la intervención de las partes para su ejecución, sino que una vez determinadas las condiciones del acuerdo y establecidos los eventos desencadenantes, se ejecutará automáticamente."[55]

Ha sido tanto el impacto de esta tecnología, que su utilización ha causado una transformación en el sector bancario, asegurador, minero, inmobiliario, agrícola, entre otros; sin dejar de mencionar, el reconocimiento que se le ha dado en los estados de Arizona y Nevada, así como en países, como Bielorrusia.[56]

Sin embargo, actualmente no existe una definición reconocida de forma unánime por los distintos países, e incluso, es común observar algunos artículos que afirman que el contrato inteligente no puede ser considerado ni siquiera un contrato sino simples *"códigos informáticos que reemplazan la letra de un contrato*"[57], pero si al ejemplo nos remitimos, la escritura también es un código que representa el consentimiento de las partes en un documento. En consecuencia, se está dejando a un lado que, sin importar el formato en el que se encuentre, escrito u oral, en lenguaje tradicional o en lenguaje informático, la naturaleza jurídica del contrato en realidad no varía, s*iempre que en el fondo se busque representar el consentimiento de dos*

[54] Información obtenida del twitter @NickSzabo4, 31 Julio 2018

[55] Marina Echebarría Saenz. "Contratos Electrónicos Autoejecutables (Smart Contract) y Pagos con Tecnología Blockchain" p. 70

56 Artículo de Javier Ruiz "Bielorrusia legaliza las criptomonedas, las ICO y los contratos inteligentes" publicado el 27 de diciembre de 2017. Consultado en: https://www.fin-tech.es/2017/12/bielorrusia-legaliza-las-criptomonedas-ico-contratos-inteligentes.html

[57] Artículo de Francisco Aravena Riveros "La regulación de los contratos inteligentes" publicado el 07 de noviembre de 2017. Consultado en: https://lexlatin.com/opinion/la-regulacion-contratos-inteligentes

partes. En este sentido, los abogados Stephan Meyer y Martin Eckert señalan que un contrato inteligente puede ser legalmente exigible siempre que los términos del acuerdo entre dos o más personas se encuentren reflejados en el código informático del cual se trate.[58]

De este modo, nuestro Código Civil establece que "*el contrato es una convención entre dos o más personas para constituir, reglar, transmitir, modificar o extinguir entre ellas un vínculo jurídico*"[59], por lo que, siguiendo esta definición sólo se necesita el simple consentimiento entre las partes para que se perfeccione un contrato. En consecuencia, no se exigen formalidades adicionales[60], ni un idioma en específico, ni que se encuentre redactado en un determinado documento. Es perfectamente posible que un contrato se encuentre encriptado, redactado en un idioma desconocido por el común de las personas o que ni siquiera se encuentre escrito; ya que la autonomía de la voluntad de las partes es el principio general en esta materia.

En este sentido, si se está en presencia de un Smart Contract, o se tiene planeado utilizar esta figura, se deberá revisar, en primer lugar, los artículos de nuestro Código Civil para conocer si es posible subsumirlo en las normas generales sobre la materia. No obstante, ¿sería correcto decir que nuestro legislador no previó lo que actualmente sucede con las novedades tecnológicas?, ¿no hay ninguna norma que pueda regular específicamente a los contratos que se encuentren en formato electrónico y que además sean autoejecutables?

Se puede decir que el legislador venezolano lo previó de manera astuta a través de la inclusión , en la Ley sobre Mensajes de Datos y Firmas Electrónicas, de los principios de i) *neutralidad tecnológica,* el cual consiste en no favorecer o reconocer a un tipo

[58] Artículo de Simón Chandler "Los contratos inteligentes no son un problema para los sistemas legales del mundo, siempre y cuando se comporten como los contratos legales" publicado el 8 de febrero 2019. Consultado en: https://es.cointelegraph.com/news/smart-contracts-are-no-problem-for-the-worlds-legal-systems-so-long-as-they-behave-like-legal-contracts

[59] Código Civil Venezolano. Gaceta Oficial Nº 2.990 Extraordinario del 26 de Julio de 1982. (Artículo 1.133)

60 Con excepción de algunos contratos.

determinado de tecnología sino incluir "las tecnologías existentes y las que están por existir", y ii) *equivalencia funcional*, el cual consiste en otorgarle eficacia jurídica a toda la información que se encuentre contenida en un mensaje de datos, tal y como se le otorga a un documento escrito en papel. Principios que se reflejaron por primera vez[61] en la Ley Modelo de la CNUDMI sobre Comercio Electrónico del año 1996.[62]

En este sentido, entre los principales objetivos de la Ley sobre Mensajes de Datos y Firmas Electrónicas se pueden destacar: i) asegurar el otorgamiento y reconocimiento jurídico de los mensajes de datos, entendiéndose por éstos "*toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio*" y ii) otorgarle al mensaje de datos la misma eficacia probatoria que la ley otorga a los documentos escritos. Ahora bien, en aquellos casos que la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos siempre que:

a) La información que contengan pueda ser consultada posteriormente.
b) Conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduzca con exactitud la información generada o recibida.
c) Se conserve todo dato que permita determinar el origen y el destino del mensaje de datos, la fecha y la hora en que fue enviado o recibido.[63]

De esta forma, si la información puede ser consultada y permanecer

[61] Claudia Madrid Martínez. "Medios electrónicos de pago en comercio internacional". Revista Venezolana de Legislación y Jurisprudencia. Caracas, 2018. p. 137

[62] Consultado en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

[63] Ley sobre Mensajes de Datos y Firmas Electrónicas. Decreto con Fuerza de Ley Nº 1.204 del 10 de Febrero de 2001, publicada en Gaceta Oficial Nº 37.148 del 28 de febrero de 2001. (Artículos 2, 7 y 8)

inmutable, de manera tal que se pueda determinar el origen y el destino del mensaje de datos, esta ley puede ser idónea para su regulación. Así pues, pareciera que los Smart Contracts pueden cumplir los requisitos anteriormente descritos con el único obstáculo de la inteligibilidad, ya que la propia Ley señala en su artículo 1 que la misma "*tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda* ***información inteligible en formato electrónico****, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas".* No obstante, dicho obstáculo puede superarse con la colaboración de un experto que ayude a traducir la voluntad de las partes; y es que la propia ley deja abierta dicha posibilidad al señalar que *"toda persona podrá recurrir a los servicios de un tercero"* para dar cumplimiento a los requisitos señalados en el párrafo anterior.

Sin embargo, todo dependerá de cada caso en concreto, puesto que en aquellos acuerdos en los cuales ambas partes del contrato no se encuentren determinadas, se deberán sortear temas como la capacidad de los contratantes, la amplitud y validez del consentimiento, el momento de perfeccionamiento del contrato, así como, tomarse en cuenta posibles dificultades para determinar la identidad de los contratantes. Por este tipo de inconvenientes, se está planteando una redefinición de esta figura para denominarla "*contrato legalmente inteligente*", a fin de lograr una combinación entre códigos informáticos y lenguaje legal tradicional[64], y utilizar los Smarts Contracts, desde un sentido estricto, sólo como códigos informáticos para la autoejecución de un acuerdo previamente establecido fuera de la blockchain.[65]

Lo cierto es que, esta novedosa figura, independientemente de la denominación que se le otorgue de manera definitiva, y que probablemente no se establezca de forma inmediata sino con el avance de las discusiones sobre el tema, se podría subsumir en las normas previamente establecidas y el ordenamiento jurídico venezolano puede brindar, de cierta forma, una protección a la hora de optar por su utilización. Tal y como se expresó, su

64 Artículo de Josh Stark "Making Sense of Blockchain Smart Contracts" publicado el 4 de junio de 2016. Consultado en: https://www.coindesk.com/making-sense-smart-contracts

[65] Carlos Tur Faúndez. "Smart Contracts. Análisis Jurídico". Editorial Reus, Madrid, 2018. Pp. 59 y ss.

utilización se está propiciando en sectores comerciales inimaginables, por lo que no se puede dejar de un lado su importancia y la que tendrá en un futuro inmediato.

LA PERSONA ELECTRÓNICA Y LA PERSONALIDAD ELECTRÓNICA
Breves notas sobre posibles definiciones

POR GABRIELA D'ARGENTO GODOY

I. INTRODUCCIÓN

La Unión Europea ha destinado especial atención a la robótica al no poder ignorar la evolución creciente y sostenida de tal fenómeno y sus posibles consecuencias jurídicas.

Es así como nace el Proyecto de Informe de la Comisión de Asuntos Jurídicos del Parlamento Europeo, de fecha 31 de mayo de 2016, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica. Posteriormente, de aquel documento, surgió la Resolución del Parlamento Europeo, de fecha 16 de febrero de 2017, con recomendaciones destinadas a la Comisión. En este último documento, el Parlamento Pide a la Comisión que, *cuando realice una evaluación de impacto de su futuro instrumento legislativo, explore, analice y considere las implicaciones de todas las posibles soluciones jurídicas*. Entre éstas, el Parlamento Europeo señala:

> *"…crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos*

supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente."

Ahora bien, ante la posibilidad de que cada vez se diseñen robots más autónomos, es decir, que puedan tomar sus propias decisiones, y que puedan aprender más y mejor de su entorno, siendo pertinente otorgar personalidad jurídica a éstos, cuestión ésta última muy discutida entre la doctrina internacional, ¿qué podría entenderse por persona electrónica y personalidad electrónica?

II. PERSONA Y PERSONALIDAD JURÍDICA

La existencia del Derecho se encuentra atada a la existencia de la persona. Refiere María Candelaria Domínguez que la persona constituye el centro de gravedad de todo sistema democrático de derecho, por lo que cualquier interpretación jurídica siempre debe ser en favor de ella. [66]

La persona, protagonista del ordenamiento jurídico, es todo ente susceptible de ser titular de deberes y derechos jurídicos. Es todo ente capaz de figurar como sujeto pasivo o activo en una relación jurídica.[67]

Existe la persona natural, que es aquel individuo de la especie humana, y la persona jurídica en estricto sentido, que hace referencia a los entes distintos al ser humano a los que el ordenamiento jurídico les atribuye personalidad jurídica. De tal suerte que ésta última, la persona jurídica en estricto sentido, constituye una invención del Derecho. [68]

Por otro lado, si bien la persona y la personalidad jurídica están íntimamente relacionadas, son cuestiones distintas. Pues, la personalidad es la aptitud, cualidad o idoneidad para ser

[66] Domínguez Guillén, María C. Derecho Civil I, Personas. Venezuela, Ediciones Paredes, 2013, p.39

[67] Aguilar Gorrondona, José L. Personas, Derecho Civil I, Venezuela, Editorial Universidad Católica Andrés Bello, 2013, p. 39. El autor cita tres definiciones de persona en Derecho, considerándolas equivalentes.

[68] Domínguez Guillén, María C. Derecho Civil I, Personas. Venezuela, Ediciones Paredes, 2013, p.51.

titular de deberes y derechos o, lo que es igual, la personalidad es la aptitud, cualidad o idoneidad para ser persona. [69]

Entonces, ¿qué podría entenderse por persona robótica responsable y personalidad robótica?

III. PERSONA ROBÓTICA RESPONSABLE Y PERSONALIDAD ROBÓTICA

Un robot es máquina o ingenio electrónico programable que es capaz de manipular objetos y realizar diversas operaciones que, generalmente, imita la figura y los movimientos de un ser animado.[70] Es una entidad virtual o mecánica artificial que parece tener un propósito propio.

Cuando se habla de robot autónomo, debe pensarse en una entidad virtual o mecánica artificial que, en mayor o menor medida, toma sus propias decisiones. Un robot que ha sido programado para aprender de su entorno y, en función de ese aprendizaje, decidir.

En contrapartida, mientras más autónomo sea un robot, menor control podría tener el ser humano sobre tal creación. Pues, si dicha máquina es capaz de aprender más y mejor, tomando decisiones con independencia, se asemeja al desarrollo del ser humano que, una vez pasada la niñez y la adolescencia, llega a ser un adulto independiente, que decide por sí mismo y es responsable de sus actos. De aquí que surjan algunas inquietudes desde la perspectiva jurídica.

¿Qué podría entenderse por persona robótica responsable? Para comenzar, vale decir que, de la lectura de la Resolución del Parlamento Europeo, de fecha 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, se desprende que tal categoría se circunscribe, al menos principalmente, a los robots autónomos. Si hay control humano sobre la máquina y ésta no puede decidir por sí sola, no debe

[69] Domínguez Guillén, María C. Derecho Civil I, Personas. Venezuela, Ediciones Paredes, 2013, p.47.

[70] Real Academia Española, Diccionario de la Lengua Española.

pensarse en ella como autónoma.

Dicho lo cual, nos aventuraremos a ofrecer una breve y sencilla definición de la persona robótica. En este sentido, consideramos que ésta es aquella entidad virtual o mecánica artificial, que goza de un gran grado de independencia en la toma de decisiones, pudiéndola hacer impredecible, susceptible de ser titular de deberes y derechos jurídicos. Desglosando dicha definición, podemos señalar lo siguiente:

a) *Aquella entidad virtual o mecánica artificial:* es una creación del ser humano, que puede ser corpórea (por ejemplo, un brazo mecánico) o incorpórea (por ejemplo, un bot).
b) *que goza de un gran grado de independencia en la toma de decisiones, pudiéndola hacer impredecible*: sistemas que operan en entornos complejos, que no requieren de la intervención humana, ya que aprenden, "piensan" y actúan por sí mismos, aún cuando algunos de ellos necesiten de un mantenimiento regular.
c) *susceptible de ser titular de deberes y derechos jurídicos*: capaz de figurar como término subjetivo en una relación jurídica.

La Resolución del Parlamento Europeo, de fecha 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, además, agrega el vocablo "responsable". En este sentido, el Parlamento Europeo ha establecido en la Resolución mencionada:

> *"…AG. Considerando que también son manifiestas las deficiencias del marco jurídico vigente en el ámbito de la responsabilidad contractual, ya que la existencia de máquinas concebidas para elegir a sus contrapartes, negociar cláusulas contractuales, celebrar contratos y decidir sobre su aplicación hace inaplicables las normas tradicionales;*
> *considerando que esto pone de relieve la necesidad de adoptar nuevas normas eficientes y actualizadas, acordes con los avances tecnológicos y las innovaciones recientemente*

aparecidas y utilizadas en el mercado;

…AI. Considerando que, pese al ámbito de aplicación de la Directiva 85/374/CEE, el marco jurídico vigente no bastaría para cubrir los daños causados por la nueva generación de robots, en la medida en que se les puede dotar de capacidades de adaptación y aprendizaje que entrañan cierto grado de imprevisibilidad en su comportamiento, ya que un robot podría aprender de forma autónoma de sus experiencias concretas e interactuar con su entorno de un modo imprevisible y propio únicamente a ese robot;…"

Por no dejarlo pasar por desapercibido, parece pertinente apuntar que, al hablar de una persona robótica *responsable*, ello denota que tal entidad virtual o mecánica artificial, que goza de un gran grado de independencia en la toma de decisiones, susceptible de ser titular de deberes y derechos jurídicos, podrá tener responsabilidad contractual y extracontractual, es decir, que deberá responder en razón de haberle causado un daño a otro. Así, por ejemplo, en el futuro, si se ha celebrado un contrato con un robot autónomo y éste cae en incumplimiento, se encontraría ante una obligación de responder patrimonialmente.

¿Qué podría entenderse por personalidad robótica? Nos atrevemos a definirla como la aptitud, cualidad o idoneidad para ser una persona robótica. Nuevamente, al desglosar dicha definición, apuntamos que:

a) *La aptitud, cualidad o idoneidad:* significa que se reúne las condiciones necesarias u óptimas para algo determinado.
b) *para ser una persona robótica*: debe entenderse como la posibilidad de ser una entidad virtual o mecánica artificial, que goza de un gran grado de independencia en la toma de decisiones, pudiéndola hacer impredecible, susceptible de ser titular de deberes y derechos jurídicos.

"Tener personalidad robótica" será reunir, en palabras muy sencillas, las condiciones necesarias u óptimas para ser una persona robótica. ¿Cuáles serán dichas condiciones?

Pues, las que se establezcan en el ordenamiento jurídico.

Finalmente, nos gustaría afirmar que no pretendemos que estas definiciones ofrecidas sean inequívocas y completas. Por el contrario, creemos que para su construcción se requiere de gran debate y que, en virtud de su novedad, queda mucho por asimilar y escribir. Es por ello que nos permitimos aportar las mismas en contribución de fomentar la investigación y discusión en el área.

LIBERTAD Y OLVIDO Reto de la Sociedad de la Información

Por: Rodolfo Guerrero Martínez

La sociedad vive confundida ante la abominable actualización producto de la innovación tecnológica que se utiliza en todo momento y prácticamente en cualquier parte en donde estemos. En el contexto de la nueva realidad no se prevén los derechos constitucionales- digitales de los cuales somos acreedores como el acceso a internet, a la privacidad, integridad y accesibilidad de información.

La existencia de una diversidad de temas desconocidos por el ciudadano del siglo XXI crea vulnerabilidad, a su vez cierto rechazo y apatía en participar para su entendimiento e integración rumbo la construcción de la sociedad de la información y del conocimiento requerida en la nueva realidad. *¿Cuáles son los tópicos a entender en este tiempo digital?*

1. **Inteligencia artificial:** Es la expresión del intelecto humano automatizado el cual ha sido posible con el paso del tiempo y a través del avance de las tecnologías electromagnéticas. (La cultura es la transformación de la naturaleza para la sobrevivencia)[71].

[71] Guerrero Martínez Rodolfo. Videoconferencia "Abogado Disruptivo: La Nueva era del Derecho". 1er Simposio Internacional "Enseñanza del derecho en Ambientes Virtuales" en el marco de actividades académicas de la

2. **Internet de la Cosas:** Sistema en el cual los objetos del mundo físico se podían conectar a Internet por medio de sensores[72].
3. **Big Data:** Comprensión y análisis de gran cantidad de información proveniente de una red social, plataformas o sistemas de datos. Entre las sus características podemos encontrar la integración, la administración y el análisis en el uso de datos.
4. **Datos personales:** Son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Se clasifican en: datos de identificación (CURP, Credencial de elector, número de seguridad social, domicilio) y sensibles (salud, origen étnico o racial, preferencias sexuales, ADN)[73].
5. **Algoritmo:** Es una secuencia lógica y finita de pasos que permite solucionar un problema o cumplir con un objetivo por medio de la captación de datos[74].
6. **Cibernética:** Pretende ser el puente entre las ciencias, el punto de conexión entre los mundos tecnológico y humano, a la vez reflejo y motor de la necesidad de integración y el trabajo interdisciplinario entre las ciencias[75].

Del Analfabetismo funcional a la alfabetización digital

Justamente el hecho de usar tecnología no te vuelve tecnólogo, así como el tener libros no te convierte en intelectual. La etapa que se vive es compleja debido al negligente uso de acceso a internet para ingresar a plataformas web y redes sociales, lo cual convierte a

Universidad Nacional Autónoma de México. 8 de octubre de 2020.

[72] El concepto de internet de las cosas lo propuso Kevin Ashton en el Auto-ID Center del MIT en1999, donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores.

[73] Véase la clasificación realizada por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. *http://www.infodf.org.mx/index.php/protege-tus-datos-personales/%C2%BFqu%C3%A9-son-los-datos-personales.html*

[74] Un algoritmo es una serie de pasos organizados, que describe el proceso que se debe seguir, para dar solución a un problema específico. (Fadul, 2004).

[75] Pérez Luño, Cibernética, informática y derecho [53], p. 20. *https://archivos.juridicas.unam.mx/www/bjv/libros/8/3937/6.pdf*

toda la población en víctimas, sin importar su edad, raza o estatus económico.

El analfabeta funcional podemos entenderlo como "cuando una persona ha desarrollado los conocimientos y las técnicas de lectura y escritura suficientes para realizar de manera efectiva todas las actividades de orden verbal propias de su cultura o grupo social" (Hamadache y Martin, 1986).

Sin embargo esto es insuficiente, ya que se carece una capacidad de abstracción –ver las cosas de distintos puntos de vista- y una habilidad de interpretación –el poder integrar varios conceptos y fundamentos al caso particular-.

Es aterrador el transitar de una sociedad cuando es sometida de forma silenciosa por su ignorancia en el uso de las TIC (Tecnologías de la Información y Comunicación), lo cual no solo deriva en la pérdida de acceso a ciertas funciones de una aplicación o sobre las bondades que la innovación nos ofrece, sino en la libertad de decidir, de saber y conocer dónde estamos y hacia dónde nos dirigimos.

La alfabetización digital es importante porque es la clave de la inclusión. La brecha digital es también brecha social. Ambas se alimentan mutuamente. Dado a este razonamiento la alfabetización digital es también la clave del desarrollo de la Sociedad de la Información y el conocimiento. Únicamente la sociedad que entienda a precisión su importancia y, en consecuencia, despliegue una estrategia formativa adecuada y sea capaz de gestionar el cambio adecuadamente, estará en condiciones de desenvolverse con flexibilidad y capacidad de liderazgo en la sociedad informacional de este siglo que cada vez se torna más disruptivo y de tecnologías emergentes.

El problema de la libertad de expresión

"Si se quita la libertad de expresión,
Entonces mudos y silenciosos podemos
Ser guiados, como ovejas al matadero".
GEORGE WASHINGTON

La libertad siempre ha sido un término complejo no sólo por la definición de la palabra, la cual está constituida por un haz, variable en el contexto histórico, de libertades concretas y reales, sino por el entendimiento que cada persona le otorga[76]. En este contexto tecnológico, la libertad de expresión se ha visto en dificultades, ya que en varios casos se prohíbe hablar de

[76] Véase el libro Constitucionalismo mestizo Sáchica, Luis Carlos publicado por la Universidad Nacional Autónoma de México UNAM. *https://biblio.juridicas.unam.mx/bjv/detalle-libro/323-constitucionalismo-mestizo*

ciertos temas de interés por sus características políticas, religiosas, en otras situaciones es desvirtuada dado a que esto perjudica a derechos de terceros, respecto al hecho de emitir opinión sin argumento, y por la manifestación de ello en un canal inadecuado de comunicación.

En el punto anterior, las redes sociales ha sido un instrumento muy fuerte para democratizar el derecho a conocer y saber, donde la comunidad digital (ciudadanos) no solo es pasiva sino también activa al crear y producir conocimiento. Sin embargo también se han utilizado para construir de "tribunales virtuales" que carecen de toda institucionalidad constitucional, y perjudican a una persona por medio de un meme, un video, un *screenshot* que luego se publican en diferentes canales digitales en dañan la buena honra, fama e intimidad de una persona.

Recordemos que la libertad de expresión es definida como toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección (Artículo 13 de la Convención Americana sobre Derechos Humanos).

Sin embargo, la decisión jurídica no es sencilla, y menos cuando se trata de un tema jurídico-tecnológico; es indispensable entender que la aplicación de todo derecho fundamental como el de libertad de expresión no aplica en caso general sino a cada caso en concreto mediante determinación del juez.

En este razonamiento es loable hacernos la pregunta si *¿un súper juez puede alcanzar la respuesta única?* El súper juez de Dworkin Hércules J. parece haber resuelto todos los problemas de incertidumbre, ya que no solo posee información ilimitada acerca del asunto a decidir, sino que también dispone de todo el tiempo y la capacidad necesarios para tomar la decisión. Dadas las condiciones podría esperarse que Hércules J. logre una respuesta legal única, y que además pueda exhibir muy buenas y coherentes razones para justificar tal respuesta. Pero el problema es el de producir una decisión legal con un algoritmo, ya que Hércules no puede comportarse como un operador de algoritmos sino como un decisor racional cuya meta es la maximización de la certeza legal[77].

[77] Barragán Julia. Informática y Decisión Judicial. Ed. Fontamarra. Año 2008. P.60

El olvido a favor del interés legítimo

Ante el panorama inexacto y difuso de un marco jurídico, ético y de convivencia del mundo digital, las personas se ven en riesgos sobre la protección de su imagen, fama, intimidad, privacidad y el punto más alarmante y número uno, su dignidad humana.

En la actualidad los distintos marcos jurídicos han buscado proteger la integridad digital del ciudadano que sustente que un interés es legítimo, ya que de lo contario podrá peligrar el acceso de información de terceros y la disponibilidad libre de información. Un poderoso ejemplo es la ambicioso Reglamento General de Protección de Datos de la Unión Europea (RGPD).

Recordemos los antecedentes del interés legítimo en el tratamiento de datos donde la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecto al tratamiento de datos personales y a la libre circulación de estos datos, norma que actualmente está derogada por el RGPD, recogía en su artículo 7 la posibilidad de que el tratamiento de datos se pueda realizar si *"es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva"*[78].

En el contexto actual apreciamos en el artículo 6° del Reglamento General de Protección de Datos de la Unión Europea sobre la licitud del tratamiento, y comprobamos como no es necesario cuando el mismo es requerido para:

1. **La ejecución de un contrato**, o lo que antes se denominaba el mantenimiento de una relación negocial, laboral o administrativa.
2. **El cumplimiento de una obligación legal.** La cual no necesariamente debe ser un acto legislativo adoptado por un parlamento, pero sí debe ser clara precisa y su aplicación previsible para los destinatarios de conformidad con la Jurisprudencia del Tribunal de Justicia de la Unión Europea (en adelante TJUE) y del Tribual Europeo

[78] Consulte Diario Oficial de las Comunidades Europeas N° L 281/31. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES*

de Derechos Humanos. (Considerando 41 y 45).

3. **El cumplimiento intereses públicos**, debiendo garantizarse que el tratamiento debe tener su base y finalidad en derecho de la UE o en el de los Estados Miembro (6.3 y considerando 45). A este respecto, el RGPD establece en el apartado 2 del art. 6, que, tanto para el cumplimiento de intereses públicos como obligaciones legales, los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del RGPD.

Apreciar que entre las situaciones que permiten el tratamiento lícito de datos sin consentimiento, la satisfacción del interés legítimo es la excepción que mayor indeterminación podrá producir en la aplicación práctica del RGPD, ya que podría recurrirse a la misma como cajón de sastre para la no obtención del consentimiento del interesado en determinadas situaciones en las que el mismo resulta de difícil o imposible obtención.

Por esta razón, el RGPD en sus considerandos 47[79] a 49[80] establece ejemplos de cuando podríamos encontramos ante un interés legítimo por parte del responsable, aclarando que siempre habrá que realizar una evaluación meticulosa y aplicar la regla de la expectativa legítima o razonable para la consideración de dicho interés legítimo (dicha regla es

[79] Véase UE RGPD. Razón 47 que inicia señalando: *"El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable".*

[80] Véase UE RGPD. Razón 47 que comienza señalando: "*Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos…".*

establecida por el Grupo de trabajo 29 en Opinión nº 6 de 2014)[81].

Rumbo a la consolidación de la sociedad de la información

La ruta a seguir no es sencilla, la sociedad de la información y conocimiento debe ser considerada una sociedad de personas, no de tecnologías, ya que eso es clave para que la ciudadanía avance en la lucha contra la brecha digital que reside en la educación. También que la prioridad social sea la inversión en conocimiento y eso significa que es aprender a aprender. Eso no es un juego de palabras, más bien un cambio cultural muy importante que afecta de forma total a cualquier proyecto de alfabetización digital, porque, estar alfabetizado digitalmente es poseer la capacitación tecnológica imprescindible para sobrevivir en esta era digital y poder actuar críticamente sobre en ella.

El reto primordial depende de la educación digital, que lleva consigo un gran proyecto transformador que tiene consecuencias políticas, económicas y sociales.

Sin duda existen varios objetivos que priorizar como:

- Proporcionar el conocimiento de los lenguajes que conforman los documentos multimedia interactivos y el modo en que se integran;
- Brindar conocimiento y uso de los dispositivos y técnicas más frecuentes de procesamiento de la información.
- Favorecer la actitud de receptores críticos y emisores responsables en contextos de comunicación democrática.

Además de tener presente tres elementos para medir el mayor o menor grado de conocimiento del alfabeto digital: 1. El manejo de un computador y sus periféricos. 2. Manejo de softwares esenciales. 3. Conocimiento informático[82].

En la nueva realidad donde se ha obligado al aislamiento social y al desempeño de actividades de manera remota, incluyendo las actividades de formación educativas, deben de actualizar las políticas de educación adoptadas por los gobiernos así como la educación recibida el interior de los hogares en relación con las TIC y su incorporación a la vida cotidiana solo de esa manera podremos obtener

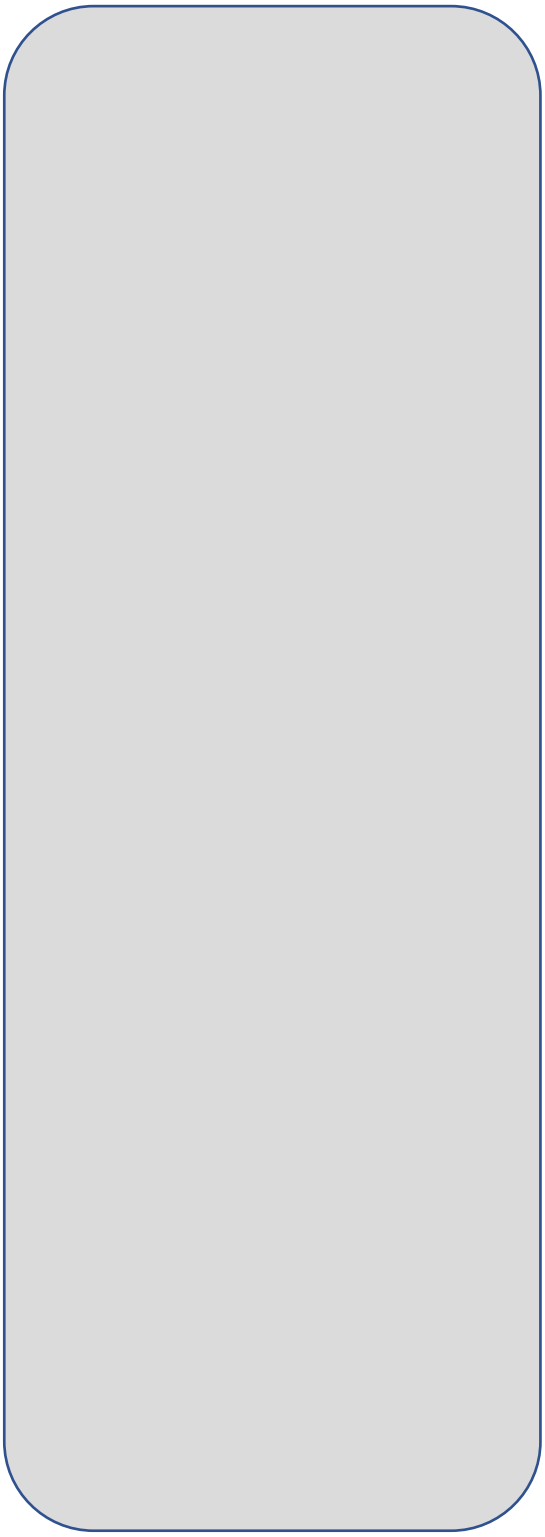
[81] DPO& it law *http://www.dpoitlaw.com/reglamento-general-de-proteccion-de-datos-rgpd/unidad-i-7-1-legitimidad-en-el-tratamiento/*

[82] Véase Revista digital para Profesionales de la Enseñanza. No. 17 – Noviembre de 2011. Alfabetización digital en la educación.

resultados genuinos y de manera gradual.

SEMBLANZA CURRICULAR

Rodolfo Guerrero Martínez. Hombre mexicano, emprendedor y disruptivo. Abogado por la Benemérita Universidad de Guadalajara, actualmente estudiante del posgrado en derecho con orientación en materia Constitucional y administrativo por la misma casa de estudios. Socio Fundador y Representante Legal de la Sociedad Civil Coffee Law "Dr. Jorge Fernández Ruiz". Socio fundador de la Academia Mexicana de Derecho "Juan Velásquez" A.C. Miembro de la Junta Menor y encargado de la Comisión de Legaltech del Ilustre y Nacional Colegio de Abogados de México A.C. Capítulo Occidente. Conferencista en Congresos Nacionales e Internacionales (Colombia, Argentina y Guatemala), conversatorios e impartido diplomado y cursos en temas de derecho informático, derechos humanos y derecho constitucional. Publicaciones: *Patentes: el camino hacia la protección y rentabilidad de nuestros productos* (Talent Republic, 2020); *Elementos a tomar en cuenta en un sitio E-Commerce para la protección de datos* (Talent Republic, 2020); *Derechos humanos de cuarta generación y las tecnologías de la información y la comunicación* (Derechos Fundamentales a Debate, CEDHJ 2020).



Biometría informática y el peligro de la vigilancia en masa

POR LEÓN LANIS V.

La biometría informática es un precedente perfecto para analizar los grandes avances que la tecnología y el uso de la información han experimentado durante estas últimas dos décadas. La biometría informática o 'biometric data' (como originalmente se llama en inglés) se puede definir como aquel proceso de toma de medidas y datos caracterizantes de una persona, o grupo de ellas, en base a características físicas y procesos biológicos que individualizan a la persona del resto. En la actualidad, la biometría informática es procesada de forma masiva, gracias a los procesos modernos y colosales que ha producido el 'big data' y el "machine learning"; cómo se analizará más adelante, la masificación del uso de información biológica individualizante de las personas conlleva efectos muy buenos en distintos ámbitos, pero, como en todo proceso industrial masivo, se ha tendido a generar abusos y malas prácticas.

El uso de la información personal biológica de las personas tiene el gran peligro de ser usada como proceso de vigilancia en masa o cómo se le llama en inglés: 'mass surveillance'; la vigilancia en masa es un proceso moderno por el cual se monitorea de forma masiva a una población, ya sea total o sustancialmente, distinguiéndose de si esta vigilancia es producida por corporaciones, Estados o ambos en apoyo mutuo, la última opción suele ser la más común, ya que estas empresas, como redes sociales,

ISPs, y otros, tienen un mayor acceso a la información personal y sensible de los individuos en monitoreo, pero muchos Estados o actores del mundo político usan esa información para beneficio propio, manipulación, censura, entre otras. La biometría informática es un modo de vigilancia en masa, el cual torna infalible, ya que, a diferencia de casi todo otro tipo de información, la biología y sus procesos son casi imposibles de modificar en su esencia, es decir, la información que rastrea la biometría es vitalicia e inherente a la persona.

Derechos Humanos.

Antes que todo, debemos entender los elementos y forma de operar de la biometría informática. Como bien se definió, la biometría informática opera por la recolección de información biológica que individualiza y caracteriza a una persona, ahora, existen distintas formas de recolección, con distintos objetivos y relacionadas a distintas partes del cuerpo o procesos biológicos; por consiguiente, existen distintas categorías de información biométrica, estas son: químicas (como por ejemplo la búsqueda de ADN, tipo sanguíneo, etc) visuales (tales como el estudio de las formas de orejas, reconocimiento de iris, reconocimiento de retina, reconocimiento facial, huellas dactilares, geometría 3D de la posición de los dedos, reconocimiento de firma y letra, etc), de comportamiento (cómo el movimiento corporal, pulsaciones de teclados o movimiento de lápiz, forma de caminar, reacción ante estímulos, etc), auditivas (por ejemplo el análisis de tono, profundidad, patrones y volumen de la voz), olfatorias (el olor de un individuo), entre otras. La verdad es que con el 'machine learning' la lista va creciendo sola, ya que hoy en día las máquinas pueden por si solas analizar patrones de individuos y estudiarlos y, por tanto, cada vez es más fácil encontrar nuevas técnicas de biometría. La recolección de información biológica se genera tomando muestras de aquello que es necesario para el tipo de biometría en específico, es decir, si buscamos analizar el ADN, se toman muestras de sangre, o para información auditiva se analiza la conversación de un individuo en distintas ocasiones; mientras más variado sea la forma y la situación en que se analiza una muestra más se podrá entender de ella y de la forma en cómo individualiza a las personas, en otras palabras, si se busca analizar la voz de un individuo o de grupos de ellos, se tendrá una muestra mucho más fiable y que abarque más información si es que se analiza la voz en distintos estados de emoción, temperatura de ambiente y situación, como por ejemplo tener muestras de la voz de una persona cuando está enojado y cuando está feliz. Hoy en día, las máquinas con inteligencia artificial tienen la tarea de analizar cada muestra y encontrar, con precisión

quirúrgica, aquello que es único de cada muestra y, por tanto, puede tener mayor utilidad para la supervigilancia, si nos apegamos al mismo ejemplo de la voz, si se interceptan todas las llamadas del grupo de estudio o grupo monitoreado se podrán analizar las distintas etapas que la voz de cada persona y aquello que lo caracteriza o hace único.

La biometría informática presenta distintos peligros o posibilidad de malas prácticas, pero antes de analizar los dos mayores peligros que presenta, debemos entender que el gran problema que nace de el uso de la información biológica proviene de la pobre garantía mínima legal de protección de datos personales que ofrecen las distintas legislaciones y la tendencia moderna a la autorregulación tecnológica, es decir, la inclinación, predominante de hoy en día, a que las empresas de manejo tecnológico se regulan a sí mismas debido a la incapacidad de los legisladores a regular los avances tecnológicos y sus peligros. Teniendo aquello en cuenta, los peligros son:

(A) Falsificación o fraude informático: nuestros sistemas informáticos, sean públicos o privados, son vulnerables y toda vulnerabilidad es o va a ser explotada en algún momento, aquello es, por así decir, una regla básica en la ciberseguridad. Por lo tanto, en ningún momento podemos confiar al 100% en la seguridad de un sistema tecnológico. Casi cualquier tipo de intromisión de la información es recuperable, podemos hacer 'back-ups' de información, cambiar claves, etc. Pero en el caso de la información biométrica no funciona igual; la información que proviene de nuestras características físicas, químicas y otras son vitalicias, en otras palabras, jamás podremos modificar o eliminar la esencia de nuestra identidad, por tanto, legalmente, la biometría informática requiere de una protección legal especial. Si se genera un fraude informático (y este se basa en el uso de información biológica) jamás se podrá retornar o modificar (en su esencia), ya que esa información es inherente a la persona y por cuanto queramos cambiarlo, nuestra composición química y nuestras características físicas, jamás podran ser cambiadas en su esencia. El ejemplo típico es el delito de suplantación de identidad, en este sentido, si le robamos, por ejemplo, las características sanguíneas de una persona, esta se podrá usar eternamente de forma maliciosa.

(B) Malas prácticas en la cosecha de información: este término proviene de su traducción en inglés, information harvesting. Esto se refiere a la recolección masiva de información. El problema de la cosecha d e información se encuentra en su obtención y en el alcance de su uso. El gran problema de la biometría informática, como se

verá más adelante en el caso Patel V Facebook, se encuentra en la forma de obtención de los datos. Muchas veces, entes públicos o privados, consiguen información personal sin el consentimiento o con un consentimiento bastante viciado, ya que los servicios gratuitos de redes sociales (como Instagram, Facebook, entre otros) suelen entregar dichos productos a cambio del uso de información privada. En el caso Patel V Facebook (2019), los demandantes lograron probar que Facebook usaba, sin el consentimiento expreso de los usuarios, la información biométrica provenientes de imágenes y videos subidos a su plataforma. Si bien, en este caso, la finalidad no era maliciosa, muchas veces se pueden producir abusos de esta obtención no consentida de información. Y como veremos más adelante, el peligro más grande de aquello es la vigilancia en masa.

BIPA (Biometric Information Privacy Act 740 ILCS 14/) es una Ley, promulgada por la Asamblea General de Illinois en el año 2008, la cual busca regular la recolección, almacenamiento, uso y explotación de la información biométrica. A grosso modo, esta Ley tiene tres principales pilares: el consentimiento expreso y exacto del usuario, temporalidad (fecha máxima de uso) y garantía de diligencia de seguridad del administrador. En la actualidad, existe un 'pendiente bill' que busca modificar BIPA (SD 3053), ampliamente apoyado por Facebook y Google; lo importante de este pending bill son las excepciones que quiere aportar a la Ley, las cuales buscan eximir a instituciones privadas cuando cumplan las siguientes condiciones:

1. Cuando la cosecha de la información se use exclusivamente para empleos, evitar fraudes o por métodos de seguridad.

2. Que la empresa que consiga, almacene o trate esta información no genera un provecho pecuniario, ya sea en venta, arrendamiento o intercambio comercial, al cosechar la información.

3. Que la empresa que maneje los datos sea diligente en el uso de la información.

Personalmente tengo mis críticas sobre SD 3053, ya que creo que dichas modificaciones presentan peligros directos en la privacidad de los usuarios, estas críticas son:

1. Protección de la privacidad privacidad del trabajador: quitar la necesidad de consentimiento previo para tal información dará la posibilidad de abusos de uso de información, ya que los empleadores podrán tener a su alcance toda la información biométrica que quieran sin que los mismos trabajadores estén de acuerdo con aquello. En materia laboral, es importante proteger la privacidad de los trabajadores.

2. Excepción por diligencia: como bien se mencionó anteriormente, todo sistema tecnológico, sin excepción alguna, es vulnerable. Ningún ente, sea público o privado, puede asegurar que tienen sistemas impenetrables o perfectos. Esto presenta un peligro tanto para los usuarios como a las empresas, ya que por un lado es muy difícil, como empresa, poder probar la diligencia, al fin y al cabo, siempre va a existir una vulnerabilidad que pruebe lo contrario, y por el lado de los usuarios, es difícil poder asegurarse que la información va a estar asegurada. En teoría, esta garantía solo sirve para que un juez pueda juzgar si se cumplió ciertos aspectos para cuidar de la información de los usuarios.

Habiendo analizado bien los peligros de la biometría informática, debemos estudiar cómo se puede (y se ha hecho) usar para la vigilancia en masa. Primero analicemos el caso de China. En este país existen más de dos millones de cámaras de reconocimiento facial, las cuales logran procesar grandes cantidades de información, logrando individualizar a las personas y sus acciones. El gobierno Chino justifica el uso de estas cámaras diciendo que son para la seguridad nacional, pero en la realidad han sido usadas para vigilar en masa a su población y sus acciones. Principalmente se han usado para los créditos sociales, los cuales son un nuevo método de transacción nacional donde las buenas conductas de los ciudadanos los hacen escalar en la jerarquía social, logrando acceder a nuevos bienes y servicios. A través de las cámaras el gobierno Chino logra analizar cada movimiento de los ciudadanos. El problema con esto es que viola la privacidad de los ciudadanos y coacciona las decisiones de los mismos, ya que si no cumplen con ciertas acciones que espera su gobierno, serán degradados y perderán privilegios, por ejemplo, usar transporte público. Por otro lado, también en China se ha usado para el avergonzamiento público, el cual es un sistema de castigo de “malas conductas”, donde quien incumple es publicado en pantallas gigantes, donde se expone su información privada por haber hecho algo “malo”, por ejemplo, cruzar la calle donde no hay paso de peatones. Esto es una reiterada violación a distintos Derechos Humanos, tales como la privacidad, la honra, la protección de datos personales (en chile está consagrado en su Constitución como un Derecho fundamental).

Se estima que a futuro parte de los ‘cookies’ que se recolectan para fines publicitarios (o target publicity), funcionarán con datos biométricos, sobre todo con reconocimiento facial para entender que atrae y lo que no a un usuario; esto parece una idea genial desde un punto económico, pero trae serias consecuencias desde un punto de vista legal.

Además de los peligros ya estudiados del uso de información biológica vinculante, en el caso de el reconocimiento de datos característicos del rostro está el problema del racismo. Los sistemas que funcionan con inteligencia artificial son útiles mientras se les enseñen con patrones de acciones y datos, entonces, si en una determinada red social, usando de ejemplo Facebook, se tiene a discriminar y aislar a gente de determinada raza o etnia, el sistema informático, por default, copiara la secuencia y tenderá a discriminar de misma forma, de hecho, se han intentado acciones civiles en contra de Facebook (remontándose al caso revisado) respecto de cómo la biometría no autorizada de las fotos de usuarios de determinadas razas pueden excluirlos de determinadas publicidades de forma arbitraria, pero generalmente de desestiman dichas causas ya que no existe marco regulatorio al respecto o que al menos esté suficientemente actualizado para entender dichas situaciones. En el caso de la vigilancia en masa, sabemos por eventos históricos, que un gobierno autoritario con control sobre la información y datos que tiene un especial desprecio por una determinada etnia o raza pueden usar dichos datos en su contra; recordemos que la razón por la cuál la protección de datos es considerada dentro de los Derechos Humanos es porque durante la persecución del gobierno Nazi al pueblo Judío, se usaron datos personales adquiridos de plantas de trabajo para saber quien era Judío y quien no.

Teniendo todo lo dicho en cuenta, podemos concluir que las legislaciones modernas no están preparadas para garantizar la debida protección de los datos personales de los usuarios, especialmente cuando hablamos de datos biométricos. Esta falta de protección da paso a muchos peligros, pero de los más peligrosos está la vigilancia en masa (Estatal o privada) la cual, como se analizó en el caso de China, puede traer variadas violaciones a los Derechos fundamentales de las personas. Por tanto, es importante regular esta actividad bajo un riguroso marco legislativo (tanto a nivel nacional como internacional) para garantizar a las personas la debida protección de sus datos biológicos caracterizantes.

Bibliografía:

1. Types of Biometrics - Biometrics Institute. (2019). Retrieved 20 August 2019, from https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

2. Patel v. Facebook, Inc. (2019). Retrieved 20 August 2019, from https://www.chamberlitigation.com/cases/patel-v-facebook-inc

3. Schwartz, A. (2019). Victory! Lawsuit May Proceed Against Facebook's Biometric Surveillance. Retrieved 21 August 2019, from https://www.eff.org/deeplinks/2019/08/victory-lawsuit-may-proceed-against-facebooks-biometric-surveillance-0

4. Biometría. (2019). Retrieved 21 August 2019, from https://es.wikipedia.org/wiki/Biometr%C3%ADa

5. Mark Zuckerberg testifies on Capitol Hill (full Senate hearing). (2019). Retrieved 21 August 2019, from https://www.youtube.com/watch?v=6ValJMOpt7s

6. The Cambridge Analytica Files | The Guardian. (2019). Retrieved 21 August 2019, from https://www.theguardian.com/news/series/cambridge-analytica-files

7. Biometrics | Privacy International. (2019). Retrieved 21 August 2019, from https://privacyinternational.org/topics/biometrics

8. Biometric Information Privacy Act. (2019). Retrieved 21 August 2019, from https://en.wikipedia.org/wiki/Biometric_Information_Privacy_Act

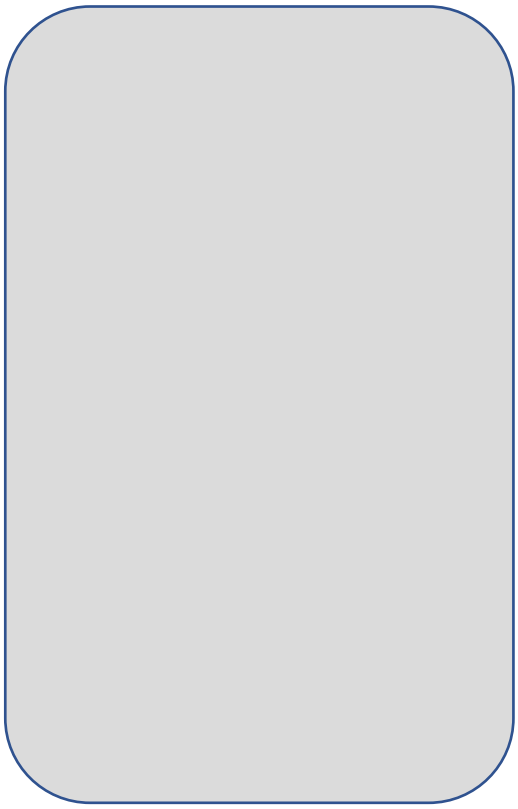
9. Biometrics Information Privacy Act, Illinois General Assembly (3 de Octubre del 2008)

10. SD 3053 (pending bill), Illinois General Assembly

11. Biometrics in Marketing | Hyper-Personalised Advertising | ievo. (2020). Retrieved 2 September 2020, from https://ievoreader.com/biometrics-and-their-place-in-the-marketing-world/

12. The Problem of Racial Profiling and Facial Recognition | Veridium. (2020). Retrieved 2 September 2020, from https://veridiumid.com/racial-profiling-and-biometrics/

13. Argüelles, A., & Argüelles, A. (2020). ¿Qué hay detrás de las recolecciones de datos y la vigilancia? | Derechos Digitales. Retrieved 2 September 2020, from https://www.derechosdigitales.org/12806/que-hay-detras-de-las-recolecciones-de-datos-y-la-vigilancia/



PRÓLOGO
Prof. Dr. Emilio Suñé Llinás
Catedrático de Derecho Informático
Universidad Complutense de Madrid

EL FEDATARIO JURAMENTADO CON ESPECIALIZACIÓN EN INFORMÁTICA

SU IMPORTANCIA EN LOS PROCESOS DE DIGITALIZACIÓN EN EL PERÚ

Carlos Pedroza Barrios

EVIDENCIA DIGITAL, Cómo superar la barrera mental de papel?

SÍNTESIS DEL TALLER HOMÓNIMO BRINDADO POR: **MARÍA JOSÉ QUINTANA DOURADO**, ABOGADA – ARGENTINA; **FERNANDO DÍAZ DURÁN**, ABOGADO – GUATEMALA; **YEHESKEL CLOUGH**; ASESOR Y CONSULTOR EN CIBERINTELIGENCIA – PANAMÁ; **ALEJANDRO FABIÁN** – ABOGADO – PERÚ Y **VANINA KANDYBA**, PSICOPEDAGOGA FORENSE – ARGENTINA EN EL MARCO DE LA "LOCADEMIA EDI JOVEN".

Piense por un momento que está en su despacho y llega a la consulta alguien que necesita denunciar un delito o que ha sido acusado de un delito. Imagine que la evidencia principal con la que cuenta está en soporte digital. Lo que corresponderá será trabajar con esa evidencia en su formato de origen, y aquí aparecen las barreras de papel.

En líneas generales, le evidencia digital es toda la información creada o distribuida desde un sistema informático que puede ser usada como un medio probatorio en un proceso judicial. Es cualquier dato digital que dé un indicio y pueda relacionar a la víctima o su actor con el crimen cometido. La evidencia digital es toda información y datos de valor para una investigación, estos datos necesariamente provienen de un dispositivo electrónico.

La mayoría de las dificultades prácticas que enfrenta el letrado es presentar ante la judicatura o fiscalía una evidencia digital RESPETANDO su formato. No es apropiado pasarla al papel, no sirve de nada imprimir una captura de pantalla de un chat, por ejemplo. Eso sólo es a los efectos ilustrativos, más no hace a la mismidad e integridad de lo que estoy manifestando. Mucho menos se puede suplir con la intervención de un Notario, quien sólo dará fe de aquello que sus sentidos perciban, y como sabemos es fácil fraguar imágenes digitales y chats.

Cuál es el desafío que enfrentan los operadores del derecho cuando llevan ante la justicia una evidencia digital? cómo obtenerla, preservarla y presentarla de forma debida según los estándares internacionales?

Entre las herramientas forenses de código abierto se pueden usar para preservar y analizar una evidencia digital destacamos las siguientes tres:

a) Gaijin Write Protector – protector de escritura USB

b) Generador de imágenes espejo FTK – para copias forenses bit a bit

c) Autopsy herramienta de análisis forense

Para trabajar con evidencia digital respetando los principios de debido proceso y defensa en juicio, nos regiremos por las pautas establecidas en las Normas RFC 3227[83] y OEA. Para ello durante el proceso de análisis forense los pasos a seguir serán los siguientes: **preservación, adquisición, análisis, documentación y presentación.**

La herramienta Write Protector asegura que el dispositivo que se vaya a duplicar mediante copia espejo, no sea alterado, pues lo sella.

Luego, el siguiente paso será la copia espejo en sí, bit a bit, para lo cual utilizamos el software FTK Imager. **Siempre los análisis forenses deben practicarse sobre las copias, los originales deben ser preservados sin modificar.** El principio de integridad es fundamental para que la otra parte en el proceso pueda controlar la prueba. El software FTK Imager nos va a brindar un dato muy importante: el hash que identifica la evidencia original, ese número de sellado identifica de manera única el material digital para su contraste.

En la siguiente etapa, y teniendo la copia espejo, por ejemplo del contenido de un pen drive, trabajaremos sobre esa copia, usando Autopsy. Esta herramienta

[83] Los RFC «Request For Comments» son documentos que recogen propuestas de expertos en una materia concreta, con el fin de establecer por ejemplo una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo. El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento, y puede llegar a servir como estándar de facto para la recopilación de información en incidentes de seguridad. Consultado de: https://www.incibe-cert.es/blog/rfc3227

nos permitirá analizar muchos elementos de la evidencia colectada, por ejemplo los metadatos de una fotografía que se hallaba guardada en el pen drive.

Los ***metadatos*** de una foto pueden contener información muy valiosa, como la fecha en que se tomó, el lugar donde fue tomada la foto, si se la editó, con que programas, etc.

Para qué sirven estos metadatos? muy simple: siguiendo con el ejemplo, si al despacho viene la madre de una supuesta víctima de grooming, y luego de hacer la denuncia por este delito se allana un domicilio encontrándose un pen drive que contenía material de pornografía infantil que involucra al denunciado, mediante los metadatos de esas fotos podemos saber mucho.

Luego de analizar esa copia de dispositivo con Autopsy, tendremos un reporte. La copia espejo y el reporte como los parámetros analizados en concreto deben ser guardados en un soporte tal que garantice la integridad. Lo que se sugiere es grabar todo en un CD no regrabable o DVD.

Finalmente resta, realizar un

reporte de todos los pasos que seguimos para el análisis forense, detallado y cronológico. Es recomendable que se lo haga en leguaje claro y preciso, detallando cada paso. Pensemos que esto será lo que lea el juez, y estamos tratando de superar la barrera mental de papel, y perderle el miedo a la evidencia digital, por lo que es de suma importancia que lo redactemos de modo tal, que pueda ser entendido por un hombre promedio.

Es de suma importancia resaltar que las buenas prácticas en el manejo de la evidencia digital pueden significar la diferencia entre el éxito o el fracaso de un proceso judicial. En casos de delitos como grooming[84] o ESI[85], donde la

[84] Grooming: término que refiere al conjunto de acciones llevadas a cabo por un mayor de edad con el fin de seducir sexualmente a un menor a través de cualquier medio informático.

[85] Explotación Sexual Infantil: Es la forma más grave de delitos contra la infancia, conlleva efectos devastadores en la vida del niñ@ o adolescente. Si no se trata a tiempo, la víctima

principal fuente de pruebas de carácter digital.

A la evidencia digital la debemos trabajar y presentar al juez en su “estado natural” de DIGITOS en el que ha nacido y se desarrolla. Es por eso que bregamos para que cada día sea más posible acudir ante la justicia munidos de este tipo de elementos probatorios y que se puedan hacer valer en su soporte original.

Esto trae un beneficio a los justiciables por una cuestión de celeridad e inmediatez, pero también al servicio de justicia, porque muchas veces las malas prácticas en la presentación de evidencia digital tanto de parte del denunciante como del acusado, lleva a poner en marcha el aparato judicial del Estado, con los costos que ello implica, y luego no se llega a nada, porque se planteas nulidades.

Por lo cual espacios como el que se nos brindó en este taller, a través de los cuales podamos llevar capacitación a los operadores del derecho, y la informática, son sumamente valorables por cuanto son un paso hacia adelante para derribar la barrera mental de papel que aún persiste en los Estrado y que hoy en día va en desmedro del debido proceso.

en la edad adulta puede replicar la conducta que padeció sobre otros niñ@.

Soluciones informáticas

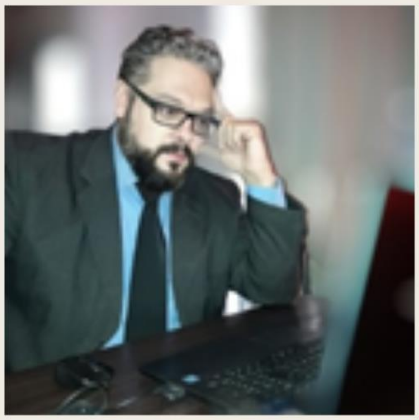
- Criptomonedas
- Tecnología Blockchain
- Servicios informáticos
- Plataformas Web
- Plataformas de Transacciones
- E-Commerce
- Desarrollo de todo tipo de Sistemas y Sofware
- Gestión y Mantenimiento de Servicios en la Nube
- Hosting
- Casillas de Correo Personalizadas
- Seguridad informática
- Soporte a Usuarios
- Community Manager

Pedinos Asesoramiento:
Miguel Grau: magrau@magsistemas.com
Daniel Grau: daniel@magsistemas.com
Trinidad Grau: mtrgrau@c-patex.com
Fernando Grau: fpgrau@c-patex.com
@C_PATEX t.me/cpatex

Cripto Patagonia S.A.

MAG Sistemas

cPatex



EL DELITO INFORMÁTICO RANSOMWARE EN EPOCAS DE PANDEMIA. EL INDICIO DE MALA JUSTIFICACION Y SU CONSTITUCIONALIDAD

AUTORES:
LEONARDO MONTI - EDGARDO VILLORDO
ABOGADOS

Vivimos tiempos de pandemia, una nueva circunstancia que ha pasado a regular y determinar sin muchas opciones gran parte de la vida de las personas del mundo y la Argentina no es la excepción, este triste evento ha hecho que se produzca una migración de muchas actividades, laborales, sociales, incluso de la vida diaria de forma acentuada hacia lo digital, donde todo es vertiginoso y puede resultar peligrosos en muchos sentidos en este entorno, hasta incluso generar la muerte por ataques de los denominados ciberdelincuentes o hackers.

Es así que un ciberataque a un hospital alemán provoca la primera muerte en el mundo por ransomware; así lo informaban medios locales y de internet; de la ciudad alemana de Düsseldorf haciendo saber que se produjo una muerte una paciente en un hospital tras sufrir el centro hospitalario un ataque de hackers contra los sistemas informáticos que complicaron el tratamiento de la enferma.

Puntualmente, el hecho delictivo consistió en un ataque a 30 servidores en el Hospital Universitario de Düsseldorf fueron secuestrados por los ciberdelincuentes con un aviso de rescate dirigido a la dirección. Tras la muerte de la mujer, los investigadores comunicaron a los ciberdelincuentes que habían atacado un hospital. Después, los hackers eliminaron sus demandas de rescate y entregaron la clave para

poner fin al ciberataque de ransomware.

Estamos frente a una modalidad de delito denominada RANSOMWARE, que podemos definirla como un software malicioso (malware) cuyo objetivo es comprometer sistemas informáticos, aplicaciones y datos sensibles cifrándolos (volviéndolos inoperables- y codificándolos de una forma que no pueden recuperarse), solicitando el pago de un rescate principalmente en bitcoins (moneda electrónica) para restituir la disponibilidad y operatividad de estos. Desde un punto de vista técnico informático penal, "el Ransomware es un esquema de negocio ilícito en constante transformación, atípico desde una óptica esencial y penal de la figura que, a través de una pluralidad de etapas de ejecución en el ciberespacio y la conjunción de diversas tecnologías, técnicas de manipulación y coacción psicológica e inteligencia artificial, provoca la afectación simultánea de una multiplicidad de bienes jurídicos, teniendo como objetivo principal pero no único, comprometer la disponibilidad, acceso, integridad, operatividad y privacidad de datos y sistemas informáticos, empleando sobre ellos herramientas criptográficas de última generación, pidiendo tanto para la restitución de los mismos como para la evitabilidad de su divulgación, el pago de un rescate en criptomonedas, todo ello en un marco de alevosía e impunidad digital con características propias del terrorismo."

Esta modalidad se ha acentuado de una forma casi exponencial, así Durante el primer trimestre de este año, se detectaron 907.000 correos de SPAM, 737 tipos de amenazas digitales, y accesos a 48.000 "Links" o "URL" maliciosas, todos ellos relacionados con el coronavirus. También entre febrero y marzo se pudo observar que el SPAM incrementó su cuantía de 4.000 a 900.000 (x200) y el acceso a vínculos maliciosos relacionados con el COVID-19 creció un 260%.

Tomando algunas de las palabras de mi apreciado colega el Dr. Alberto Hernán Saul, puedo decir que el ransomware presenta algunas características esenciales que lo hacen altamente eficiente y único en su especie. Trabaja bajo un proceso de "amenaza de día cero", tanto desde el punto de vista de la generación de nuevas muestras de malware - "polimórfico"-, como la del aprovechamiento de vulnerabilidades no descubiertas en sistemas y aplicaciones. Por otro lado, el "anonimato"; los canales de comunicación utilizados ya sean en sus fases preparatorias como en las de ejecución, se encuentran cifrados –encriptados– lo cual hace imposible la identificación de los ciberdelincuentes. También encontramos diversas particularidades adicionales en su accionar como el desarrollo de una oportuna y efectiva "ingeniería

social" potenciada bajo la automatización que provee la "inteligencia artificial", la utilización de al menos dos módulos de "coacción psicológica" simultánea –compromiso de sistemas informáticos y exfiltración de datos confidenciales– capacidades de distribución a través de "múltiples vectores tecnológicos de infección", llevar a cabo procedimientos de alta complejidad para la evasión de barreras de seguridad, mutación del modus operandi en cada uno de sus ataques -"Familias de Ransomware"- dificultando la determinación de parámetros comunes para su mitigación y el no requerirse altos conocimientos técnicos para su distribución.

Sin lugar a dudas que el hecho mencionado anteriormente genera, un montón de análisis respecto de las estructuras de seguridad de estos servicios, que están sujetos y me atrevería a decir casi presos a lo digital, y la responsabilidad del manejo en pandemia, por otro lado, las normativas en algunos casos obsoletas y sub regulaciones hacen de este momento, algo sumamente peligroso que el mismo continúe sin ningún tipo de tratamiento legislativo.

Por otro lado, mencionar que a raíz del hecho el Ministerio Público Fiscal del lugar ha iniciado acciones legales por un homicidio involuntario o culposo en nuestra legislación.

Puestas algunas cuestiones del hecho ha analizar, deseo mencionar que los delincuentes, han suministrado las herramientas informáticas para poder desafectar la información codificada y que hacia que otras vidas entren en situaciones de peligro similares a la de la víctima.

Aquí ya en el aspecto subjetivo estamos frente a un supuesto, desde la perspectiva del Ministerio Fiscal actuante ante una acción culposa o involuntaria, y es aquí donde pretendo enlazar este trágico hecho del hospital alemán, al texto elaborado con un excelente análisis llevado a cabo por mi apreciado colega el Dr. Leonardo Monti del Indicio de Mala Justificación y su constitucionalidad, dable mencionar que lo analizado se hace respecto del aspecto subjetivo penal, utilizando algunos ejemplos del mundo óntico, y en un caso absolutamente teórico, que pasaría si estas personas que cometieron el hecho son sometidas a las autoridades judiciales argentinas, y la norma penal y procesal penal de nuestro país, más puntualmente al Código Procesal Penal de la Provincia de Córdoba de la República Argentina, y la norma de fondo penal argentina.

No es menor a fin de dar claridad a este análisis mencionar que los medios de prensa alemanes informaron que los ciber delincuentes, manifestaron que no sabían dónde se estaban metiendo y

que las acciones llevadas a cabo resultarían en la muerte de esta paciente, producto de la inutilidad de la información afectada por el Ransomware (entiendo que podría ser un indicio de mala justificación) lo cual podría tomarse como un engaño hacia las autoridades, y por dicho motivo luego suministraron la solución a las autoridades.
Aquí es que entra el análisis mencionado anteriormente, donde se pone de manifiesto como estarían estos sujetos del hecho alemán frente a la normativa penal argentina, si los mismos manifestaran indicios de mala justificación, y si es constitucional a la luz de nuestra Norma Suprema.
Primero diremos que una vez que los supuestos ciber delincuentes sean apresados serán llevados ante las autoridades correspondiente para poder realizar sus actos de defensa.
-
Así la declaración del imputado (la indagatoria): se trata del principal acto de defensa material del imputado. Se trata de un acto procesal ineludible en los primeros momentos de la IPP y que la ley adjetiva regula formalmente en cuanto medio de defensa material del imputado [1] y en la cual éste puede elegir entre declarar o abstenerse de hacerlo sin que ello haga presumir su culpabilidad.

La prueba: siguiendo al maestro cordobés el Dr. Cafferata Nores diremos que es todo aquello que confirma o desvirtúa una hipótesis o afirmación precedente, y más precisamente en el ámbito del proceso penal, seria todo lo que pueda servir para descubrir la verdad respecto de los hechos que son investigados y respecto de los cuales se pretende la aplicación de la ley sustantiva.

El indicio: se trata de un hecho o circunstancia del cual, mediante una operación lógica, es posible inferir la existencia de otro [2]. Por ejemplo, la tenencia de la res furtiva por parte de quien ha sido aprendido en inmediaciones del domicilio de la víctima es un indicio de que fue el autor del hurto o robo de la misma, pero también podría tratarse de un tenedor de buena fe o de un encubridor.

Hechas estas aclaraciones y ya centrándonos en el tema que nos ocupa, nos preguntamos: *¿qué ocurre si el imputado al momento de prestar declaración indagatoria miente?,* y la siguiente pregunta sería *¿es posible utilizar como indicio de culpabilidad en su contra la mendacidad al prestar declaración?*

En definitiva, lo que se trata de dilucidar es si la mentira del imputado como postura defensiva se puede utilizar como prueba de cargo o como agravante.
Desde ya deberíamos descartar como indicio de mala justificación la ya clásica fórmula utilizada en la gran mayoría de las declaraciones

indagatorias iniciales en las que el imputado niega de manera genérica el hecho y se abstiene de seguir prestando declaración. Dice y dice bien Cafferatta Nores, que se trata de una simple negativa que no alcanza el grado de justificación [3].

Suponiendo que el imputado al momento de ejercer su defensa material opte por declarar y al hacerlo mienta, podrían ocurrir dos situaciones: 1) Que se tome la postura defensiva mentirosa como prueba de cargo en su contra o 2) Que no se la admita como prueba de cargo en contra del imputado. Se trataría de una declaración que no pudo refutar el contenido de la acusación.

Las garantías constitucionales relacionadas con el tema en cuestión:

La declaración del imputado es un medio de defensa y no un medio de prueba [4]. En efecto, si consideramos como válida esta afirmación debemos decir que la declaración del imputado es un medio de defensa, y que, como tal, hace a la garantía del debido proceso [5] y más precisamente al **derecho de defensa en juicio** (art. 18 de la constitución nacional, 9 y11 de la DUDH, 14 del Pacto de San José de Costa Rica y 26 de la DADDH).

Entendido éste como *"…una facultad tendiente válidamente a impedir, contradecir, resistir y prevenir cualquier restricción injusta a la libertad individual, y al pleno ejercicio que las personas tienen otorgados por el orden jurídico. Es por ello que, el derecho, poder o facultad de defensa puede conceptualizarse como el ejercicio de la legitima oposición a la persecución penal y como la serie de actividades tendientes a la acreditación de la inocencia o la invocación de circunstancias que atenúen la responsabilidad del imputado, todo dentro de las reglas del debido proceso* ***[6]****.*

No basta el mero cumplimiento de designaciones formales, es necesario el cumplimiento efectivo de las diligencias pertinentes. [7]

En este sentido la Corte Suprema tiene dicho que *"la garantía consiste en la observancia de las formas sustanciales del juicio relativas a la acusación, defensa, prueba y sentencia dictada por los jueces naturales"* ***[8]****.*

La incoercibilidad moral del imputado: En este sentido el imputado debe tener la posibilidad de elegir libremente y sin coacciones o atmosferas intimidantes de ningún tipo si declara o prefiere ejercer su defensa material guardando silencio y sin que ello implique indicio de culpabilidad en su contra (arts.18 CN, 296 y 299 in fine del CPPN y 259 y ss. del CPP de Córdoba).

Es que el imputado no está obligado a producir prueba (puede hacerlo si así lo desea) y puede triunfar en el proceso teniendo un comportamiento procesal pasivo, ya que nada debe probar, sino que es el

órgano encargado de la persecución penal (MPF) quien debe destruir, mediante pruebas legalmente obtenidas, el estado de inocencia que la constitución y los pactos internacionales le garantizan a aquél.

Si el imputado opta por declarar, dicho acto se vincula con la garantía constitucional del **derecho a ser oído.**

En este sentido el maestro procesalista Jorge Clariá Olmedo nos ilustra diciendo que: *"el imputado tiene el derecho de declarar cuantas veces quiera, siempre que su dicho no sea intimidatorio, dilatorio, o perturbador. Declarar significa para él, el acto de exponer libremente ante el tribunal, las afirmaciones y razones, las negativas y oposiciones, relacionadas con el objeto del proceso y con su vinculación con el hecho imputado, que considere convenientes. Si declarar es un derecho se infiere a favor del imputado su facultad de abstenerse de hacerlo sin que esta negativa pueda significarle nada en su contra, como también la de callar o torcer la verdad sin que por ello ocurra en falso testimonio".* ***[9]***

Sobre este derecho la Corte Suprema, en la causa "Bassi Parides, Teodolino S. y otro" del 22/02/2005 tiene dicho que: *"cabe hacer lugar al recurso extraordinario deducido y dejar sin efecto la sentencia que al condenar la imputado como autor del delito de contrabando, atribuyó particular relevancia a cierta prueba impugnada por la defensa – en el caso, un poder por el cual el destinatario de una franquicia aduanera autorizaba al imputado a conducir un vehículo importado-, a pesar de haber eludido el tratamiento de la nulidad planteada respecto de la misma, toda vez que el argumento central de la defensa ha quedado sin respuesta, no obstante su aptitud para modificar el resultado del litigio, configurándose por ende una clara lesión al derecho a ser oído por el artículo 18 de la constitución nacional".*

Por su parte el TSJ de nuestra provincia en la causa "Serafini" del 17/4/84 se expresó manifestando que: *"siendo la declaración del encartado un medio de defensa material y no de prueba, su utilización en contra de aquél por la mera falta de veracidad en sus dichos resulta violatoria de normas constitucionales y legales preservadoras de la garantía de defensa en juicio (art. 18 de la CN, 8 de la C. Prov., y 294 del CPP).*

Nemo tenetur se ipsum accusare (nadie puede ser obligado a declarar contra sí mismo). Dicha garantía se encuentra receptada en el art. 18 de la CN, 8.2.g de la CADH y 14.3.g del PIDP:

Esta garantía no solo prohíbe obligar a declarar (esto se refiere a la indagatoria) sino también obligar a actuar contra uno mismo, serían los

casos en que se pretende obligar al imputado a conformar un cuerpo de escritura para una posterior pericia, participar activamente en la reconstrucción de un hecho, colaborar con una pericia psicológica o psiquiátrica, etc.
Es decir, nos estamos refiriendo a situaciones en las que el imputado seria órgano de prueba (que es lo que la garantía prohíbe) y no objeto de prueba, lo cual no afecta la garantía comentada.
Son ejemplos de este último supuesto; la extracción de sangre (si es que no corre riesgo la salud del incoado), el reconocimiento en rueda de personas, etc...
En el primer caso el órgano de prueba será el perito y en el segundo el sujeto reconociente (Romero).

Sobre la garantía en análisis nos ilustra el Dr. José Milton Peralta al expresar que en otros países esta garantía no tiene los alcances que se le otorga en nuestro sistema: *"en otras latitudes, de hecho, el derecho a no auto incriminarse no tiene tal extensión. Por ejemplo, en Inglaterra y Gales se entiende mayoritariamente que esta prerrogativa solo alcanza al derecho a no ser obligado a testificar y que no debe incluir otros comportamientos activos. Allí no existe una regulación expresa al respecto, pero esto se funda en la Convención Europea de Derechos Humanos que establece que al acusado se le debe garantizar un juicio justo (fair trial, con cita de Maier). La jurisprudencia del tribunal Europeo de derechos Humanos ha avalado sistemáticamente esta forma restringida de ver la prerrogativa, pues considera que otorgándole al acusado la posibilidad de callar (y solo la posibilidad de callar), el procedimiento en su contra es legítimo v.gr. Saunders v United Kingdom.* ***[10]***

Entiende Cafferatta Nores (cuya opinión compartimos) que el denominado indicio de mala justificación, constituye un *modo larvado,* aunque no menos grave de desconocer la garantía constitucional en estudio.[11]

El estado de inocencia: (Art. 18 CN, 8.2.g, CADH, 14.3.g PIDCP).
Tal como lo hemos mencionado en párrafos anteriores, con cita del precedente SERAFINI, surge manifiesta la afectación de esta garantía cuando se recurre al indicio de mala justificación.
Sobre el estado de inocencia nuestra doctrina tiene dicho que: "*Toda persona imputada de un delito, mantiene como persona su estado de inocencia durante todo el proceso penal hasta tanto se demuestre con certeza su culpabilidad y consecuentemente sea condenado por sentencia firme". **[12]***
El máximo órgano judicial de nuestro país, en 1871, en el caso TRISTÁN BROCATE dispuso la libertad del imputado de hurto porque es necesario que *"el proceso muestre una prueba tan clara como la luz del mediodía"* y agrega que *"todo*

hombre se reputa bueno mientras no se pruebe lo contrario".
Se trata el principio de inocencia de una derivación de la garantía de defensa en juicio y su base constitucional la encontramos en el art 18 de la ley suprema. [13]

Tal como lo venimos adelantando en páginas anteriores y en absoluta armonía con el pensamiento del gran maestro procesalista José I. Cafferata Nores, el indicio de mala justificación no puede ser utilizado como presunción de culpabilidad ni como agravante para individualizar la pena que pudiera corresponder, ya que de lo contrario el derecho de defensa que el imputado solo pueda expresar verdades cuya veracidad además debería probar[14], cuestión que es a todas luces inconstitucional y contrario a un estado de derecho liberal respetuoso de las garantías fundamentales.

Volviendo sobre el precedente "Serafini", el TSJ de Córdoba expresa en otro párrafo de la sentencia: *"tampoco la conducta procesal del imputado o de su abogado, en orden al ejercicio del derecho de defensa, puede ser considerada como indicio de culpabilidad, por más que aquella se aparte de las normas rituales vigentes o revista modalidades inapropiadas. Los excesos de cualquier naturaleza, cometidos en el ejercicio de los poderes que el código procesal penal acuerdan, serán pasibles de las correcciones procesales o disciplinarias que correspondan, pero no pueden ser reputadas como circunstancias reveladoras de criminalidad. Lo contrario, y tal como lo acepta el tribunal a-quo, constituye una violación del derecho de defensa, constitucionalmente consagrado".*

A esta altura del análisis crítico del tema que estamos exponiendo, resulta interesante plantarnos lo dicho por la jurisprudencia de nuestros tribunales penales de justicia respecto a **la declaración del imputado como fuente eventual de pruebas**:
Si bien en la causa SIMONCELLI (sentencia nº 45 del 28/7/98) el TSJ local pareciera avalar el indicio de la mala justificación como fuente eventual de pruebas y como elemento valido en el cual fundar la culpabilidad del imputado, también corresponde decir que no se vaso dicho resolutorio solo en las manifestaciones mendaces del imputado sino que los indicios de mala justificación fueron colocados en "paridad" con otros mencionados en la causa, por lo cual aquellos nunca fueron el fundamento principal en la motivación de la sentencia.
No obstante lo dicho, coincidimos con Cafferata Nores[15] en cuanto a que no sería correcto analizar la dirimencia o no de un indicio de mendacidad o mala justificación toda vez que el mismo debe ser calificado como legitimo antes de ser valorado, cosa que a nuestro entender no ocurre ya que como lo hemos venido

sosteniendo implicaría una clara violación de la garantía del debido proceso y constituiría en todo caso una prueba ilícita que debe ser excluida de toda posibilidad de valoración en el proceso.

Ahora bien, años más tarde el alto tribunal en los autos “CHANDLER”, dejo en claro que al momento de individualizar la pena a aplicar al imputado sometido a proceso no se podía tener en consideración como elemento agravante el hecho de que el imputado se abstenga de declarar o que al hacerlo mienta o el modo en que ejerza su defensa. [16]
Esto pone de manifiesto un cambio radical en consideración con la jurisprudencia anteriormente citada.

Respecto a la **prueba ilícita,** a la que nos referimos al criticar el fallo SIMONCELLI, podemos conceptualizarla como aquella que ha sido obtenida o incorporada de manera ilegítima o irregular al proceso. Ej. de lo primero sería el caso de la confesión del imputado obtenida mediante torturas; ej. de lo segundo seria pretender incorporar y valorar como prueba un acto definitivo e irreproducible practicado sin haber notificado previamente a la defensa del imputado.
En ambos supuestos la solución es la misma: La exclusión; no puede valorarse la prueba obtenida violando una garantía constitucional (abordaremos el tema con mayor extensión al referirnos a la doctrina del fruto del árbol venenoso).

En esta materia existe una tensión entre dos valores en juego: 1) el respeto a las garantías individuales 2) el interés de la sociedad en que los delitos sean investigados
Para Carrió, tienen primacía los primeros por tratarse de dictados de la ley suprema. La garantía del debido proceso se vería menoscabada si se permite que se utilicen contra el imputado pruebas obtenidas en violación a sus derechos básicos. [17]
A nivel Europeo la jurisprudencia española se ha manifestado expresando que:
*“cuando el origen de la ilicitud de la prueba se encuentra en la violación de un derecho fundamental, no hay ninguna duda de que tal prueba carece de validez en el proceso y los tribunales habrán de reputarla inexistente a la hora de construir la base fáctica en que haya de apoyarse una sentencia condenatoria. Otra cosa, quizá haya que decir cuando la ilicitud sea de rango inferior, en cuyo supuesto es posible que tenga que prevalecer el principio de verdad material, debiendo hacerse en cada caso una adecuada valoración de la norma violada en consideración a su atentico y real fundamento y a su verdadera esencia y naturaleza”.**[18]*
En los casos mencionados en los que se ha detectado la presencia de una prueba ilícita, es de aplicación la doctrina del **“fruto del árbol venenoso”**.
Esta teoría tiene sus orígenes en el derecho norteamericano (fruit of the

poisonous tree doctrine), sus orígenes se remontan al año 1920 con el caso Silverthorne Lambert Co. V. United States en el cual se prohibió que el estado pueda intimar a una persona a entregar documentación que había sido descubierta por la policía mediante un allanamiento ilegal.

Con posterioridad, en el fallo Nardone v. United States (1939), se dispuso que no solo se debía excluir como prueba la obtenida ilícitamente sino también sus derivadas que en el caso correspondían a evidencias obtenidas mediante grabaciones realizadas sin orden judicial (la que podríamos denominar ilicitud de origen).

Lo relevante de este fallo es que utiliza por vez primera la expresión *"frutos del árbol venenoso".*

Ya en la década del 60 y con la aplicación generalizada de la regla de la exclusión probatoria ya instalada en la doctrina y la jurisprudencia es que se aplica de manera más decidida la doctrina en análisis con base en fundamentos éticos y disuasorios de la ilegalidad estatal.

En Davis v. Mississippi (1969) donde se determinó excluir como prueba las huellas dactilares tomadas a una persona ilegítimamente detenida, aun cuando se correspondieran con las halladas en la escena del crimen, Tal como surge de los casos mencionados, según la doctrina en análisis, el tribunal no puede valerse de pruebas obtenidas ilegalmente (se aplica la regla de exclusión) puesto que se vulnera la garantía de defensa en juicio.

En el caso del derecho anglosajón la contradicción de la prueba ilícita se da con lo dispuesto en la cuarta enmienda de la constitución de los EE.UU. [19]

En nuestras latitudes, los precedentes jurisprudenciales en materia de exclusión probatoria son escasos y podríamos ubicar sus orígenes en el caso "Charles Hnos." de 1891 en la que se declaró la inadmisibilidad de la prueba documental secuestrada en un allanamiento llevado a cabo por funcionarios de la administración nacional de aduanas.

En el citado precedente al corte dijo. *"…porque siendo el resultado de una sustracción y de un procedimiento injustificable y condenado por la ley, aunque se haya llevado a cabo con el propósito de descubrir un delito…la ley, en el interés de la moral, de la seguridad y del secreto de las relaciones sociales las declara inadmisibles…".*

Más cercano en el tiempo, podemos mencionar el caso "Rayford" del año 1986 en donde el máximo tribunal de nuestro país admite la validez de la aplicación de la regla de exclusión probatoria respecto de un coprocesado cuya participación en los hechos fue probada mediando un acto ilegitimo. La participación del recurrente nunca hubiera sido acreditada sin la confesión de

Rayford que fue obtenida ilícitamente.

Lo interesante de este caso es que se hace una interpretación amplia de la regla de exclusión que deriva ni más ni menos que en la aplicación de la teoría del "fruto del árbol venenoso".[20]

Retomando una cuestión que creo que puede generar polémica y que esbozamos en alguna medida en páginas anteriores al referirnos a la prohibición de obligar al imputado a declarar contra sí mismo *(Nemo tenetur se ipsum acussare)* creo conveniente referirnos nuevamente a este instituto por su relación con el tema central de este trabajo y por la particular visión del principio nemo tenetur que tiene el prestigioso jurista de nuestro medio el Dr. Peralta.

El mencionado académico al referirse al tema expone dos concepciones que podríamos decir son las dos caras de una misma moneda pero que dependiendo de qué cara se elija los resultados pueden ser francamente antagónicos.

Se plantea por un lado una denominada *concepción amplia* del principio N T según la cual se prohíbe que el acusado en un proceso criminal pueda ser obligado a prestar cualquier tipo de colaboración en la causa, lo cual incluye desde la conformación de cuerpos de escritura, la entrega de documentos y hasta la no valoración (en contra) de expresiones mendaces por parte del imputado al momento de la declaración indagatoria (este último agregado me pertenece).

Esta concepción amplia es la que se sigue en el ámbito local con apoyatura en el art 18 de la CN, 8.2.g de la CADH y 14 nº3, g del PIDCP.

De la otra vereda tendríamos lo que el citado autor denomina *concepción literal,* seguida en Inglaterra y Gales y con base o fundamento en la convención Europea de Derechos Humanos que establece que **al acusado se le debe garantizar un juicio justo** (fair trial) y la jurisprudencia del tribunal Europeo de Derechos Humanos que viene avalando sistemáticamente esta forma restringida de interpretar el principio.

Partiendo de la idea (citando a ATRIA) que la constitución es *"…un lugar que otorga espacio a la discusión moral o política…",* sería posible entonces la libertad interpretativa, siempre respetando ciertos límites, de algunos conceptos vertidos en nuestra ley fundamental.

A favor de la "tesis amplia" (defendida por la CSJN) se ha dicho que *"…se basa en la necesidad de evitarle al acusado un conflicto moral de tres cuernos. Si el pudiera ser obligado a declarar como testigo de su propio hecho, se vería en la encrucijada de tener que elegir entre una condena por desacato, si no lo hace, una por el hecho cometido, si declara y dice la verdad, o una pena por perjurio, si declara y miente. Y someterlo a semejante situación*

seria una crueldad por parte del Estado…".

Otro fundamento podemos encontrarlo en la *estructura del sistema acusatorio* que tiene como pilar la presunción de inocencia del imputado y que pone en cabeza del MPF la destrucción de dicha presunción o estado.

Con respecto a la tesis que Peralta denomina "literal" (o restringida, denominada así porque según el autor es la que más se ajusta a la literalidad del texto constitucional y agrega que la diferencia entre una y otra postura no es jurídica sino más bien de tipo moral.

Podríamos mencionar como de esa concepción los siguientes: 1) el derecho a no auto incriminarse no puede abracar cualquier colaboración procesal perjudicial para el imputado sin que se refiere a aquellas con carácter comunicativo (el acusado queda en una posición procesal más desfavorable que en la postura amplia). 2) la postura se funda en un riesgo especial que no se encuentra presente en otro tipo de pruebas: Se trata de un riesgo específico consistente en que el tribunal puede ser engañado. El imputado puede a través de la mendacidad de sus dichos manipular el proceso. 3) Las actividades desplegadas por el imputado (mentir bajo cualquier circunstancia) afectaría uno de los fines del proceso penal como es la búsqueda de la verdad

El máximo rendimiento de esta postura denominada "literal" se puede encontrar en los denominados *delitos de cuello blanco.*

Lo relevante de esta concepción es que al abarcar menos conductas se otorga un mayor ámbito de acción al estado y esto se relaciona fundamentalmente por la importancia que tiene la prueba documental en la investigación y juzgamiento de esta clase de delitos.

Como bien señala el profesor Dr. Peralta citando en este aspecto a Andreas Ransiek y a André W. Bielfeld, "…*los argumentos esbozados para defender la concepción literal del nemo tenetur parten de que los seres humanos tienen la capacidad de mentir y que, como agentes racionales en búsqueda de consecuencias favorables, pueden hacerlo si se les obliga a declarar. Esto no ocurre cuando se trata de prueba documental.*

En este sentido el autor que seguimos en este tema hace alusión a el voto del juez Griffiths de la cámara de apelación de Inglaterra y Gales *"el contenido de los documentos va a hablar por sí mismo y no entrañan el riesgo de una falsa declaración, que es lo que subyace en el privilegio en contra de tener que responder preguntas que puedan incriminar a quien habla".*

No obstante, lo dicho, no estamos en el campo de la filosofía del derecho y existe una norma de carácter constitucional que dispone que nadie puede ser obligado a declarar contra sí mismo por lo cual las discusiones

en esta materia se encuentran bastante acotadas más allá de la no poca importancia que tiene plantearnos cuál de las dos concepciones, "la amplia" o "la literal" tienen más sentido [21].

Luego de haber expuesto las distintas teorías y concepciones que se derivan del tema que nos reúne en este breve escrito opino que le asiste la razón al maestro del derecho constitucional, el Dr. Bidart Campos cuando afirma: *"…nadie puede ser obligado a declarar contra sí mismo sin distinguir su ámbito de aplicación.*

"El derecho judicial emanado de la corte suprema es constante en afirmar que la garantía de no ser obligado a declarar contra sí mismo sólo rige en materia penal…no obstante, nos parece que debe extenderse a todo tipo de causas, aunque no con el mismo vigor…". ***[22]***

A mi entender las acciones de omitir, negar e incluso dar falsamente no puede ser pasibles de una sanción contravencional toda vez que claramente en estos supuestos el ciudadano requerido estaría actuando como órgano de prueba (no como objeto) y quedarían amparadas por el la garantía del *nemo tenetur* y esto es así porque tal como lo afirma el maestro Bidart Campos, en opinión que compartimos y lo hemos citado en apartados anteriores *"El derecho judicial emanado de la corte suprema es constante en afirmar que la garantía de no ser obligado a declarar contra sí mismo sólo rige en materia penal…no obstante,… nos parece que debe extenderse a todo tipo de causas, aunque no con el mismo vigor…".*

Ya concluyendo este breve escrito voy a proceder a realizar las consideraciones finales y emitir mi opinión al respecto.

Entiendo que la mendacidad del imputado al momento de ejercer su defensa material en el acto de la indagatoria (que quede claro, la indagatoria es un acto de defensa y no un medio de prueba) no puede ser utilizada como prueba de culpabilidad en su contra y de así ocurrir la el remedio procesal no sería otro que la aplicación de la regla de exclusión probatoria y eventualmente la doctrina de los frutos del árbol envenenado. Para ser más claros, se trataría de una prueba ilícita que debe ser fulminada con la sanción de nulidad y esta será de genérica y de carácter absoluto toda vez que viola garantías constitucionales de imputado sometido a proceso.

Es por ello que creo que la prueba no solo no solo será neutra y tendrá valor cero (Cafferata) sino que en caso de ser valorada en contra del imputado por el tribunal su resultado no puede ser otro que su nulificación y su exclusión como prueba (arts. 185 inc. 3 y 194 del CPP).

Habiendo analizado el hecho desde lo dogmático penal, ha quedado lo suficientemente clara la postura para el delito en cuestión y su relación con lo constitucional; por otro lado, en

palabras propias, estamos frente a un delito complejo, y no es menos decir que la Argentina está frente a esta amenaza inminente, solo por mencionar que nuestro país es el cuarto más vulnerable a Ciberataques, de Latino América, lo cual nos obliga a tomar cartas en el asunto sin más vueltas, y de la forma dinámica que lo exige con normativa dinámica y una legislación con una revisión dinámica y distinta a la de los delitos penales clásicos..

Como corolario, es dable mencionar que el Ransomware, como delito informático está vigente y en boga con circunstancias técnico delictivas que entiendo lo hacen un delito que irá creciendo a medida que las autoridades no logren desarticular su eficacia, por lo que merece un tratamiento especial pero siempre dentro de las garantías constitucionales. Respecto de los sujetos autores que suelen cometer este tipo de delitos, son sujetos que, no siempre tienen acreditado sus aspectos técnicos entendiendo esto como sus capacidades de hackear sistemas y conocimientos informáticos, haciendo muy fácil justificar su accionar doloso, y en su mayoría siendo entendidos como delitos culposos o involuntarios, entiendo que como materia delictiva, debemos ir hacia delitos informáticos culposos o con un tratamiento de política criminal distinto a los delitos clásicos de nuestro Código Penal, y ver al ordenador, no ya como un elemento inerte y de divertimento, sino como un elemento potencial que puede generar un peligro tal como el que surge del hecho del hospital alemán, la perdida de una vida.

Asimismo, dicho esto espero haber hecho un pequeño aporte a la academia, con la Ayuda de los colegas Dr. Monti, y Dr. Saul a los cuales agradezco su material para el presente artículo; sin lugar a dudas que siendo un delito pluriofensivo da para mucho más análisis del llevado a cabo en esta oportunidad en este escueto y humilde artículo, del cual espero poder continuar realizando en otras entregas. –

Bibliografías:

[1] Jorge A. Clariá Olmedo, DERECHO PROCESAL PENAL, tomo II, actualizado por Carlos Alberto Chiara Díaz, Rubinzal-Culzoni Editores.

[2] José I. Cafferata Nores y Maximiliano HaIrabedián, La Prueba en el Proceso Penal, sexta edición, año 2008, editorial Lexis Nexis.

[3] José I. Cafferata Nores, ¿ES CONSTITUCIONALMENTE ACEPTABLE EL INDICIO DE MALA JUSTIFICACIÓN? (Entre el “vuelo de la golondrina” y el “vuelo del murciélago”)

[4] Ibídem

[5] La CSJN en el precedente “VERBEKE” del 10/4/2003 sostuvo que: *“El respeto a la garantía del*

debido proceso, invocable tanto por la persona que se encuentra sometida a juicio como por los demás actores del proceso, consiste en la correcta observancia de estas formas sustanciales relativas a la acusación, defensa, prueba y sentencia (dictamen de la procuración general, al que remitió la corte).

[6] Vázquez Rossi Jorge E., Derecho Procesal Penal, T II, Rubinzal Culzoni, pág. 234, citado por BERRUEZO RAFAEL, Garantías Constitucionales en el Proceso Penal, pág. 58, editorial LERNER

[7] Ibídem

[8] Fallos 125:10

[9] Jorge A.Clariá Olmedo, Tratado de Derecho Penal, T I, editorial, Rubinzal Culzoni, 2008, pág. 254.

[10] José Milton Peralta y otros, Fundamentos del Derecho Penal y delitos de cuello blanco, pág. 244 y ss., año 2019, editorial ALVERONI

[11] José I. Cafferata Nores, ¿ES CONSTITUCIONALMENTE ACEPTABLE EL INDICIO DE MALA JUSTIFICACIÓN? (Entre el "vuelo de la golondrina" y el "vuelo del murciélago")

[12] BERRUEZO RAFAEL, Garantías Constitucionales en el Proceso Penal, pág. 137, (con cita a Jauchen Eduardo), primera edición, año 2020, editorial LERNER.

[13] Ibídem

[14] José I. Cafferata Nores, ¿ES CONSTITUCIONALMENTE ACEPTABLE EL INDICIO DE MALA JUSTIFICACIÓN? (Entre el "vuelo de la golondrina" y el "vuelo del murciélago")

[15] Ibídem

[16] Maximiliano Hairabedián, tomo III de actualización de Cafferata Nores –Tarditti, pág. 51

[17] Citado por Berruezo en: BERRUEZO RAFAEL, Garantías Constitucionales en el Proceso Penal, pág. 154, primera edición, año 2020, editorial LERNER.

[18] Tribunal Supremo Español en STS del 29 de marzo de 1990 –RJA 1990, 2647

[19] "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".

[20] BERRUEZO RAFAEL, Garantías Constitucionales en el Proceso Penal, pág. 152 y ss.,

primera edición, año 2020, editorial LERNER.

[21] José Milton Peralta y otros, Fundamentos del Derecho Penal y delitos de cuello blanco, pág. 243 y ss., año 2019, editorial ALVERONI

[22] María Isabel Zabala, No autoincriminación y mendacidad, Derecho U.N.I.C.E.N., lll Congreso Nacional de Derecho Procesal Garantista, PONENCIA.

#MIS DATOS SOY YO

Está en tus manos aceptar o rechazar ceder el uso de tus datos

Tu privacidad hace tu libertad

EDI

MANOLO RIVERA

Las Fintech En Latinoamérica

Las Fintech en Latinoamérica están desafiando a la industria financiera tradicional, utilizando las TIC existentes para poder ofrecer productos y servicios financieros innovadores; así como ha sucedido en las películas (Netflix, Amazon Prime), en la música (Apple music, Spotify), y otros nichos de mercado que estaban desatendidos (Uber, Airbnb), se está transformando el mundo financiero, y ahora en Latinoamérica está al alcance de un smartphone.

Aunque la utilización de las TIC, implica una mayor vulnerabilidad a los ciberataques, aproximadamente el 80% de las empresas Fintech en América Latina identifican a los ciberataques como una amenaza para sus empresas, el 47% ya tiene un plan de contingencia; en lo que va del 2020 en México, hubo un aumento del 350% en los ciberataques.

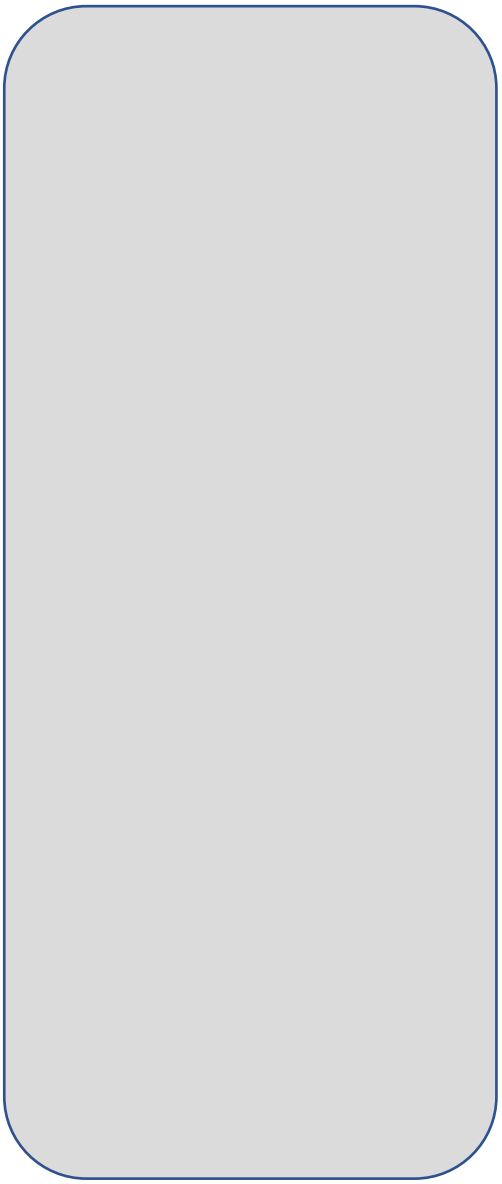
Aun así, cada vez se aperturan menos agencias bancarias grandes, nacen bancos 100% online, y las empresas Fintech ofrecen los mismos servicios a un mejor precio, esto apegado a los cambios generacionales en donde el 26% de los boomers sigue prefiriendo ir a las agencias, la generación x utiliza un 53% la banca en línea o el smartphone, y casi la mitad de los centennials tienen una aplicación de banca móvil (sin tomar en cuenta a los millenial).

Las Fintech en Latinoamérica, se han convertido en un sector de

inversión atractivo, impulsado principalmente por el mercado desatendido, en donde las instituciones financieras tradicionales no han podido llegar; Países como Brasil y México han sido punta de lanza para generar nuevos productos y servicios, y generando nuevos canales que han sido muy bien aceptados por los consumidores.

Mas allá de las pasarelas de pago, las Fintech ofrecen un abanico amplio de productos financieros especialmente para gestionar los costos de las MIPYMES, ofreciendo nuevos modelos de contabilidad digital, inteligencia empresarial, cobros de pagos y especialmente para la obtención de capital, con intereses más bajos y análisis del riesgo crediticio con nuevos algoritmos; mientras que la banca tradicional se ve afectada por la desintermediación financiera, y la carga de regulaciones.

Las Fintech son empresas que crecen a un ritmo acelerado, en donde las entidades reguladoras en Latinoamérica no pueden seguirles el ritmo, por ello se deben crear comités de cumplimiento, sandboxes y normas que protejan a los jugadores, sin que estas normas se vuelvan una limitación para el crecimiento y desarrollo de las Fintech en la región.[86]



https://www.finnovista.com/wp-content/uploads/2020/05/Global-Investors-Target-Latin-American-Fintech-LendIt-Finnovista.pdf

[86] https://www.bbva.com/es/asi-generaciones-habitos-financieros/

https://publications.iadb.org/

https://www.nber.org/papers/w22476.pdf

Código Hash

JUAN MANUEL GINÉS GARCÍA
(UY)

Resumen:

Los Códigos o Funciones Hash (funciones resumen) son herramientas informáticas que cumplen una función criptográfica de datos digitales. Utilizan un algoritmo matemático, para transformar un conjunto de datos en un código alfanumérico de longitud fija. Los usos son variados y en materia informática se utilizan para una gran cantidad de cosas, entre ellas y las que nos interesan, versan en la seguridad y veracidad de los documentos electrónicos.

Palabras clave (keyword)

Documentos electrónicos, Código hash, Prueba Electrónica.

INTRODUCCIÓN

Los códigos hash como adelantábamos, son una herramienta sumamente importante en variadas ramas de la informática como pueden ser en el manejo de datos, recuperación de recursos digitales, en la veracidad y seguridad de los documentos electrónicos por ejemplo en las Historias Clínicas Electrónicas. Pero desde el punto de vista del derecho y el ámbito jurídico nos pueden ser de gran utilidad. Valdés G. Domingo dice *"Las funciones hash resisten particular importancia en entornos donde la seguridad, integridad y privacidad de la información es prioritaria"* [1].

Los juristas tenemos la carga de educarnos en estos aspectos informáticos, con el fin de comprender estas nuevas fuentes y medios probatorios que acarrean nuevas herramientas de contratación, nuevos medios probatorios, nuevas formas de comunicación, etc.

Actualmente el derecho se encuentra confundido entre tanto avance tecnológico. Nos preguntamos cómo validar pruebas electrónicas, si es posible expresar la declaración de voluntades con el fin de contratar a través de mensajes de texto o mails, tenemos nuevos medios y modalidades delictivas, declaraciones de testigos a través de video conferencia o como en Uruguay, las audiencias son registradas en sistemas de grabación digital (AUDIRE). En esta nueva realidad, la sociedad de la información, debemos saber cómo determinar la veracidad de una fotografía, un texto, un video o un archivo de audio digital. De un sinfín de técnicas que existen para determinar la veracidad o falsedad de un documento electrónico, emerge el código hash como una herramienta que nos puede sanear el camino a la veracidad o falsedad de un objeto o recurso digital.

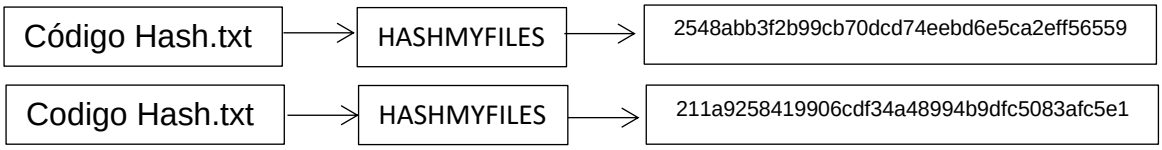
Para que el derecho y los operadores jurídicos puedan utilizar estas herramientas es necesario tomar conocimiento sobre estos temas, de manera casi urgente; ya que el derecho se ve en la necesidad de incluir una gran cantidad de documentos y archivos electrónicos al quehacer diario de los operadores jurídicos. Por eso creemos fundamental conocer herramientas que nos permitan validar o refutar ciertos recursos digitales, una de estas herramientas es el uso de los códigos hash.

CÓDIGO HASH

El código hash o funciones hash son herramientas informáticas que cumplen funciones criptográficas. La palabra *"hash"* es un vocablo anglosajón que significa *"picadillo",* este término hace referencia a la metodología de trabajo de las funciones hash. El código Hash funciona con ciertos datos de entrada, los cuales pica y mezcla para lograr una representación de los datos de entrada, en un código alfanumérico como dato de salida. Esto quiere decir que al ingresar ciertos datos de entrada, como una fotografía digital compuesta de determinada cantidad de pixeles, al ser procesada por un software que realiza la función hash aplicando un algoritmo informático se obtiene como dato de salida un código alfanumérico que representa a los pixeles que componen la fotografía. Este proceso se encuentra presente en la telefonía móvil, e-commerce, e-mails, encriptación, firmas digitales, finanzas, validación de usuarios, transferencias bancarias, etc.

La característica fundamental de los códigos hash es que para determinados datos de entrada se obtiene una representación única e irrepetible en forma de código alfanumérico como datos de salida. Si por alguna razón se modifica un dato de entrada, se modifica en su totalidad el código alfanumérico que nos da como dato de salida.

Como ejemplo creamos dos documentos .txt, uno dice *"Código Hash"* y el otro dice *"Codigo Hash",* a este último se le quitó la tilde correspondiente a la O de Código,



para esta prueba se usó el software HASHMYFILE (uso libre):

Como se puede observar al cambiar algún aspecto interno de los datos de entrada, por más mínimo que sea, se modifica absolutamente el código hash resultante como datos de salida.

A su vez el código hash puede contemplar otros parámetros del documento conocidos como metadatos, el título, el formato, el tamaño, la fecha de creación o el software con el cual se crea un documento electrónico, al cambiar alguno de estos aspectos cambia el código hash de salida. Sin embargo si la copia es exactamente igual al documento electrónico original la función hash entrega el mismo código.

Existen distintos tipos de funciones hash que entregan distintos tipos de código hash, por ejemplo MD5 (Message-Digest Algorithm 5), SHA1 (Secure Hash Algorithm 1) este formato tiene distintas variantes como SHA256, SHA512, etc. Son desarrollados por la Agencia de Seguridad de los EEUU (NSA) Desde el punto de vista criptográfico estos distintos códigos contemplan distintos niveles de seguridad. Se considera el más seguro el SHA256.

USOS JURÍDICOS DEL CÓDIGO HASH

Desde el punto de vista jurídico el código hash puede ser sumamente útil en términos de veracidad de los documentos electrónicos conocemos cada vez más su uso en la firma electrónica avanzada. Desde la actividad probatoria a actividades de contratación electrónica, pasando por bienes informáticos, ciberdelitos, etc. Por ejemplo, si estamos decididos a contratar de forma telemática un servicio determinado y se me envía un texto pdf con términos y condiciones, Si conozco el código hash original antes de descargar el archivo, cuando descargue el archivo, aplico la función hash y podría saber si este fue modificado o contiene algún elemento interno anómalo, dado que el código hash resultante no será igual al original. Con este simple proceso se puede determinar la veracidad del documento y sabré si es el que efectivamente envió el ofertante.

A su vez, puede tener usos como el seguimiento de pruebas electrónicas durante el proceso. Al conocer el código hash de una prueba electrónica como un audio, una fotografía o un video digital de seguridad, una vez que ingresa al proceso se determinan cual es el código hash original. Siendo el código conocido por las partes interesadas, se puede saber que todos tienen acceso al mismo video, fotografía o audio, que no se trata de

pruebas adulteradas, contemplando principios esenciales del proceso, cuando este tiene la actividad probatoria reducida a pruebas electrónicas.

Si bien los usos pueden ser variables y amplios para el ordenamiento jurídico consideramos fundamental que los abogados, notarios, jueces y fiscales se concienticen de estas herramientas para utilizarlas en beneficio de la justicia entendiendo que la nueva sociedad de la información implica nuevos medios para lograr la satisfacción jurídica de una situación determinada.

CONCLUSIONES:

Dado que la sociedad de la información a nucleado casi todas las actividades humanas, es necesario hacer uso de este tipo de herramientas informáticas o al menos entenderlas. En materia de base de datos se utilizan los códigos hash para encriptar los datos que ingresan en texto plano, asignándole un código único. Si la base de datos es atacada, el atacante se encontrara con un sinfín de códigos, haciendo que los datos sean ilegibles para cualquier humano. Este último ejemplo desnuda la realidad de que la informática utiliza estas herramientas como formas de seguridad y veracidad de los documentos electrónicos.

Desde el punto de vista jurídico los juzgados de España han aplicado esta herramienta. En sentencia STSJ ICAN 2013/2019 del Tribunal Supremo de Justicia, en sala de lo civil y penal, ponente Mota Bello dice *"el hash es un programa forense, que garantiza la autenticidad de cada documento, para identificar a cada uno, y que impide que un documento o su copia se pueda sustituir por otra; se trata de un algoritmo matemático que crea una serie de datos en su más pura función algorítmica y genera un número que identifica unívocamente esos datos".* Por otro lado la sentencia 1611/2019, Tribunal Supremo de Justicia, sala de lo contencioso de Barcelona, ponente Gonzales Ruiz dice *"de los citados ficheros se obtiene la huella digital hash con el algoritmo sha-1 para garantizar la integridad de los ficheros y que se adjuntan como anexo al desarrollo de las actuaciones".*

Estas ejemplificaciones de las posibles aplicaciones de las herramientas informáticas al sistema jurídico se hacen cada vez más necesarias, cada vez desde los profesionales de la informática buscan remplazar o actualizar los procesos humanos desde todo punto de vista, hoy en día muchas etapas de las actividades humanas dependen de la tecnología para su realización. Sobre todo después de la pandemia COVID-19 de la cual no conocemos aun los alcances e implicancias que tuvo para todo el ordenamiento jurídico. Pero que sin duda implico una transformación casi total de los paradigmas jurídicos.

A medida que avanza el mundo hacia nuevas tecnologías, el derecho debe conocer y analizar estos nuevos procesos de informatización. Adquiriendo los conocimientos para asegurar los

derechos fundamentales de los ciudadanos desde la construcción de la pretensión como de la defensa, o simplemente para operar estas nuevas herramientas.

BIBLOGRAFÍA:

BAUZA, Marcelo y otros, Manual de Derecho Informático e Informática Jurídica, tomo 1, 2ª Edición, FCU, Montevideo 2018.

BAUZA, Marcelo y otros, Manual de Derecho Informático e informática Jurídica, Tomo 2, 1ª Edición, FCU, Montevideo 2018.

DOMINGO, Valdés, Hashing. Un concepto. Una realidad, Universidad Tecnológica de Panamá, PDF (sin fecha). http://www.laccei.org/LACCEI2018-Lima/student_Papers/SP73.pdf (16/8/2020).

SENSO, José y DE LA ROSA, Antonio, El concepto de metadato. Algo más que descripción de recursos electrónicos, PDF, Brasilia 2003.

https://www.scielo.br/pdf/ci/v32n2/17038.pdf (16/8/2020).

RECURSOS:

Portal Agesic: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/

Portal Wikipedia: https://es.wikipedia.org/wiki/Funci%C3%B3n_hash

Portal CENDOJ: http://www.poderjudicial.es/search/indexAN.jsp

CIBERSEGURIDAD
<LATAM>

Todas las noticias sobre ciberseguridad en un solo lugar

CIBERSEGURIDAD LATAM

www.ciberseguridadlatam.com


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

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

LA RED

somos

ELDERECHOINFORMATICO.COM