Año LXIII

[AGOSTO DE 2024 - NRO. 20]

DERECHO, INNOVACIÓN & DESARROLLO SUSTENTABLE

REVISTA DE DOCTRINA Y JURISPRUDENCIA

EL DERECHO

CÁPSULA INTRODUCTORIA

El Derecho con sonido a Jazz Progresivo(*)

por Susana Eloísa Mender Bini(**)

Sumario: I. Fusión de sonidos. – II. Cuando el Derecho toca Jazz Progresivo.

I. Fusión de sonidos

Recientemente se estrenó la versión *live action* de la serie Cowboy Bebop[1], destacándose el tema de apertura *Tank!* de *The Seatbelts*[2], compuesto por la increíble Yoko Kanno[3]. Estamos ante un clásico, atemporal, principalmente con notas de Jazz fusionado con Blues, Rock, Funk, electrónica, orquesta pop, entre otros estilos; dando como resultado –entre mezclas y fusiones de género musicales– la perfecta apertura para este volumen.

Arrancando esta segunda mitad del año, este número tiene su impronta particular, pues resulta una mezcla equilibrada de cápsulas y artículos que, pisando fuerte, presentan al lector un abanico temático por demás interesante, con fuerte ritmo de la IA, notas desde el ámbito laboral y redes sociales, toques de blues filosófico-jurídico y un par de acordes disonantes desde el ciberespacio.

II. Cuando el Derecho toca Jazz Progresivo

En este número, encontraremos en la sección Cápsulas al entrañable Carlos Alberto Fossaceca en conjunto con José María Sabat Martínez, quienes nos traen un análisis del proyecto de ley de "Régimen Legal para Influenciadores o Influencers en Servicios Publicitarios Digital en Redes Sociales en todas sus modalidades", temática de gran actualidad a raíz de varios casos sonados, donde se demandaron a ciertos influencers a consecuencias de su contenido.

De la mano de Angélica Borda, se presenta una serie de reflexiones respeto a la adaptación laboral, sus desafíos al respecto, como de las opciones de posible abordaje a la transición en la evolución laboral con IA.

Desde una visión netamente financiera, el Dr. Fabián Espinoza Valencia nos trae, desde su Bolivia natal, los pormenores de la introducción y aceptación de los criptoactivos, en un pormenorizado recuento de sucesos, principalmente por el Banco Central de Bolivia en la cápsula "Tras bambalinas de la liberación de criptoactivos en Bolivia".

Entre otra de las destacadas cápsulas, encontramos a Patricio J. Moyano Peña, quien nos comparte su experiencia de haber participado en la reunión con los miembros del Laboratorio de Gobierno dependiente del Ministerio de Hacienda Nacional de Chile, por medio de su trabajo "Generación de valor público a través de la innovación participativa en LATAM: intercambio de experiencias entre el Laboratorio de Gobierno de Chile y el Ministerio Público de la provincia de Buenos Aires", vivencia enriquecedora que transpola a la realidad Argentina, puntualmente de Buenos Aires.

Por otro lado, María Constanza Quiñones inaugura la sección de Artículos, con su trabajo "La personalidad jurídica de la inteligencia artificial", en donde nos introduce a las distintas posturas respecto a si corresponde o no brindar personería jurídica a las IA, sin dejar de lado las posiciones eclécticas al respecto; cerrando con unas conclusiones muy ricas al respecto.

Finalmente, y presentando al especialista en Ciberseguridad y Cibercrimen, Tomás Illuminati Balbín, hemos desarrollado, en el trabajo "DDoS vs. Los Forenses Digitales: Entre los Estándares y la Ley", un abordaje netamente técnico respecto a uno de los ciberataques más frecuentes –DDoS–, para brindar herramientas de análisis respecto a la producción de la prueba en materia judicial. Como se dijera en un inicio, este volumen es una fusión de estilos y géneros –jurídicos/técnicos– que vale cada minuto escuchar y disfrutar.

"I think it's time we blow this scene
Get everybody and the stuff together
Okay, three, two, one, let's jam" –Tank!

VOCES: INTELIGENCIA ARTIFICIAL - TECNOLOGÍA - INTERNET - COMUNICACIONES ELECTRÓNICAS - INFORMÁTICA - ESTADO - DERECHOS Y GARANTÍAS CONSTITUCIONALES - DERECHOS HUMANOS - PODER JUDICIAL - ECONOMÍA - CONSTITUCIÓN NACIONAL - JUECES - ABOGADO - PROFESIONES LIBERALES - FILOSOFÍA DEL DERECHO - ACCESO A LA JUSTICIA - PROTECCIÓN DE DATOS PERSONALES - TRATADOS INTERNACIONALES - DELITOS INFORMÁTICOS - RESPONSABILIDAD PENAL - PRUEBA DIGITAL - PRUEBA PERICIAL - CÓDIGO PROCESAL PENAL - DERECHO A LA PRIVACIDAD - HÁBEAS DATA - EXPEDIENTE JUDICIAL - PROCESO PENAL - JURISPRUDENCIA - UNIVERSIDAD - EDUCACIÓN - CORTE SUPREMA DE LA NACIÓN - TRABAJO - CONTRATO DE TRABAJO - DERECHO DEL TRABAJO - CRIPTOACTIVO - CRIPTOMONEDAS - CONTRATOS - OBLIGACIONES - DAÑOS Y PERJUICIOS - ENTIDADES FINANCIERAS - MONEDA - CÓDIGO CIVIL Y COMERCIAL - GRUPOS ECONÓMICOS - PERSONAS JURÍDICAS - DERECHO ADMINISTRATIVO - ADMINISTRACIÓN PÚBLICA - PROCEDIMIENTO ADMINISTRATIVO

(*) La presente cápsula se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor doctor Jorge Nicolás Lafferriere, concretamente en el Programa IUS titulado: "El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable", que dirigen los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Dra. Susana Eloísa Mender Bini es abogada (UNSTA); Doctora en Ciencias Jurídicas por la Facultad de Derecho de la Universidad Católica Argentina; Máster en Propiedad Intelectual e E-law (UCC, Irlanda), especialista en Sistemas Biométricos y Privacidad (FernUni Schweiz, Suiza), miembro del grupo Argentino de Bioestadística y de la International Biometric Society, estudiante de Ing. en IA (UP).

(1) Una serie futurista, aventuras, desventuras y tragedias de un grupo de cazarrecompensas, en la que se exploran temas filosóficos como el existencialismo y su vacío, la soledad y las influencias del pasado. Streaming en la plataforma Netflix.

(2) The Seatblets, Tank!, https://www.youtube.com/watch?v=UFFa0QoHWvE, OST del volume.

(3) Yoko Kanno, https://yokokanno.ch/en/

CÁPSULA ANUNCIO

Creación del Centro en Innovación Jurídica(*)

por Emiliano Carlos Lamanna Guiñazú(**)

Sumario: I. A modo de introducción. – II. Impactos del suplemento. – III. La Comisión de Abogacía Digital. – IV. Hacia la plasmación de una idea: creación de un centro de Innovación Jurídica. – V. Elección de la Dra. Matilde Pérez como directora del Centro de Innovación Jurídica de la Facultad de Derecho de la Pontificia Universidad Católica Argentina (UCA).

I. A modo de introducción

Cuando el encierro provocado por el COVID-19 nos obligaba a recluir nuestras vidas, junto a las de nuestras familias, las experiencias pasaron a transitar –con mayor celeridad– lo mental supliendo a lo corporal. No era posible salir de nuestras casas, por eso, articulábamos encuentros por el "nuevo" amigo profesional: el Zoom o el viejo conocido Skype que circulaban en las redes como un nuevo modelo de interrelación.

En ese ecosistema de encierro tuvimos encuentros virtuales con colegas de muchas unidades académicas, pero eran frecuentes los encuentros con la profesora Matilde Pérez, la doctoranda Susana Eloísa Mender Bini y un reciente egresado como lo era Francisco Ayerza. También aportaban lo suyo –vaya si lo hacían– profesores consagrados como Fernando Ubiría, Carlos Muñiz y Valeria Moreno. En esos primeros encuentros virtuales nos latía una idea fuerte: crear/generar un espacio de comunicación que tuviera al derecho como intérprete de lo que estaba sucediendo allí afuera con un nuevo modelo de tecnología que aparecía en el horizonte, y que se apersonaba en la pantalla de mi IP o en nuevas aplicaciones de mi celular. Si algo no se encerró y creció en esos meses terribles fue la tecnología digital. La que no tardaría en golpear las puertas de los edificios de tribunales y de cámaras legislativas.

Había que contarlo.

Hacia fines del año 2020, en una reunión con actores tales como Alejandro Borda, director de la editorial jurídica El Derecho; Carlos Muñiz, secretario Académico de la Facultad de Derecho; Leandro Guzmán, Matilde Pérez y Valeria Moreno acordamos trabajar en el lanzamiento de un suplemento que generase competencia y estímulo a estos nuevos desafíos normativos que venían de la mano de una digitalización cada vez más transversal, ubicua y versátil a las necesidades de la gente.

Es así que nace el suplemento que hoy es espacio de este y otros trabajos académicos: "Derecho, Innovación & Desarrollo Sustentable", con un primer número salido en el mes de junio de 2021.

El nombre, sosteníamos, debía cumplimentar el requisito de validez de los contenidos que íbamos a aportar: alguien planteó que la palabra derecho era insustituible, pero debía ser acompañada por otra que demarcara el espacio académico a relevar. Ahí surgió *innovación*, que debía funcionar como el motor, sonoro, cuando se la mencionara. Matilde sostuvo que no había innovación posible sin *sustentabilidad* de esta. Ahí quedó cerrado el espacio. El suplemento tenía un nombre que lo identificaría en la constelación de suplementos similares.

II. Impactos del suplemento

Los artículos del suplemento atravesaron la ciencia ficción como lectura anticipatoria de la realidad, pero también sumaron al deep learning y a la machine learning, al derecho al olvido y a los juicios antimonopolio, también nos permitieron conocer o dotar de mejor comprensión los motores de búsqueda, la ambiciosa plataforma "anti-Estado" blockchain y sus creaciones más polémicas: los criptoactivos, y a las estafas cibernéticas, los modos de generar una mejor ley reguladora de la inteligencia artificial y los deepfakes con sus imágenes engañosas; asomaron las fake news y las distintas regulaciones europeas sobre cómo legislar la incertidumbre producida por la inteligencia artificial, todas estas sincrónicas y abarcativas de los 27 estados de la UE. Tan lejano a la mirada paritaria por parte de LATAM.

Lo publicado generó espacios de discusión, grupos de WhatsApp, interacción en redes, acompañamiento en jornadas, congresos y espacios educativos de toda índole, y una excelente acogida en el mundo académico y profesional. El resorte era conocer plumas de jóvenes juristas –nacidos en el mundo tecnológico– que quisieran aportar su conocimiento, y así aparecieron nombres, que hoy ya se posicionan en el mercado académico con nombre propio, como ser: Susana Eloísa Mender Bini, Pilar Moreyra, Zarina Ross; y otros tantos que nos acompañan desde sus inicios: Mariana Sánchez Caparrós, María Isabel Iñigo Petralanda, Úrsula Basset, Carlos Fossaceca, María Bibiana Nieto, Lucas de Venezia. Sin olvidar el posicionamiento del Doctorado en Ciencias Jurídicas de esta Facultad de Derecho que conduce Fernando Ubiría y al secretario de Investigación Jurídica Aplicada, Dr. Jorge Nicolás Lafferriere, que abonaron y cimentaron un diálogo que armó un verdadero grupo compacto de investigación.

III. La Comisión de Abogacía Digital

La creación de la Comisión de Abogacía Digital viene a trazar una idea plena de cuestiones y problemáticas muy bien razonadas. La unidad académica Derecho de nuestra facultad debía instar la plasmación de un programa de estudios para la carrera de grado de Abogacía que contemplara las nuevas tecnologías como un fenómeno transversal y abarcativa de muchas de las materias que se dictaban hasta entonces. Lo dicho implicaba ponerse a trabajar a todo vapor en pos de lograr que las asignaturas de la carrera tomasen elementos, conceptos y contenidos diversos para adecuarlos a los nuevos vientos de la tecnología. El objetivo se logró y así se plasmó en un informe técnico –en publicación especial en el Diario El Derecho– el 20 de octubre de 2022[1], donde se fijaron los objetivos cumplidos y que se pueden condensar en esta frase: la carrera de Abogacía tiene los programas de estudios de la carrera de grado actualizados en materia tecnológica.

IV. Hacia la plasmación de una idea: creación de un centro de Innovación Jurídica

La creación de un centro que plasmara las ideas de innovación, sustentabilidad, en un diálogo interactivo entre unidades académicas, motorizadas todas estas, desde el

(*) El presente artículo se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor doctor Jorge Nicolás Lafferriere, concretamente en el Programa IUS titulado: "El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable", que dirigen los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Abogado (UBA-1994), especialista en Derecho de la Alta Tecnología (UCA-2010) y Doctor en Ciencias Jurídicas (UCA-2015). Autor del libro "Daño Agravado por el Acreedor. Formas del debido comportamiento de la víctima" (Editorial Astrea). Profesor Titular de las asignaturas "Derecho de las Obligaciones" y "Derecho de Daños" en la Pontificia Universidad Católica Argentina (UCA) y en la Universidad del Museo Social Argentino (UMSA). Coordinador Académico del Doctorado en Ciencias Jurídicas de la Pontificia Universidad Católica Argentina (UCA). Director en el suplemento "Derecho, Innovación & Desarrollo Sustentable" de la Editorial El Derecho. Ponente y disertante en numerosas jornadas y congresos. Profesor Titular de las asignaturas "Obligaciones Civiles y Comerciales" y "Derecho de Daños" de la Facultad de Derecho de la Pontificia Universidad Católica Argentina (UCA), también de la Facultad de Derecho de la Universidad del Museo Social Argentino (UMSA) y de las asignaturas "Introducción al Derecho" y "Obligaciones y Contratos" en el Departamento de Gobierno de la Universidad Argentina de la Empresa (UADE). Profesor en posgrado (UCA - UBA - Austral), y autor de numerosos artículos de doctrina.

(1) https://repositorio.uca.edu.ar/bitstream/123456789/15655/1/abogac%c3%ada-digital-formaci%c3%b3n-jur%c3%addica.pdf

propio centro, era un viejo anhelo conversado en el seno de aquella comisión. La cuestión debía construirse sobre la base de modelos que guardaran cierta similitud: la Pontificia Universidad Católica "Comillas" de España, y el modelo generado en Stanford, Estados Unidos, eran un espejo. Y hacia allí se marchó: la creación del denominado *Centro de Innovación Jurídica –CIJ UCA–*.

V. Elección de la Dra. Matilde Pérez como directora del Centro de Innovación Jurídica de la Facultad de Derecho de la Pontificia Universidad Católica Argentina (UCA)

La elección recayó en la Dra. Matilde Pérez, a quien conocí allá por el año 1997, en ocasión de compartir junto con ella el dictado de la asignatura "Obligaciones Civiles y Comerciales" en la Facultad de Derecho de la Universidad de Buenos Aires. Juntos formamos un grupo de entusiastas profesores que dictaban la materia de los tres "muy" (muy difícil, muy extensa y muy importante). Siendo jóvenes, asumimos esos desafíos con un fervor único. Y la recuerdo a Matilde, siendo todos jovencitos, liderando. Desde esa época hasta hoy no paró de crecer académicamente. A los muchos logros profesionales y de orden académico le ha sumado el lanzamiento del libro "El Principio de Precaución y los Riesgos del desarrollo" por esta misma editorial y que se ha mostrado como un suceso en ventas. Por lo que aquel liderazgo, y este cierre, son el punto cúlmine de una carrera que debía coronarse con un nombramiento que haga –de una aquilatada experiencia profesional– el punto de lanzamiento de todo lo bueno por venir.

¡¡Felicitaciones, Matilde!!

VOCES: ABOGADO - PODER JUDICIAL - INFORMÁTICA - TECNOLOGÍA - CORTE SUPREMA DE LA NACIÓN - EXPEDIENTE JUDICIAL - EJERCICIO PROFESIONAL - JUECES - DERECHO PROCESAL - UNIVERSIDAD - EDUCACIÓN - COMUNICACIONES ELECTRÓNICAS - INTERNET - INTELIGENCIA ARTIFICIAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - ACCESO A LA JUSTICIA

CÁPSULA DE ANÁLISIS

Proyecto de ley sobre regulación de la actividad de los influencers de los servicios publicitarios digitales en redes sociales: un inicio en el camino hacia el disciplinamiento legal de una actividad digital múltiple y expansiva(*)

por Carlos Alberto Fossaceca(**) y José María Sabat Martínez(***)

Sumario: I. Introducción. – II. Análisis. *A. Concepto de* influencer. *B. Concepto de publicidad digital. C. Combate contra la publicidad abusiva y engañosa. D. El rol del anunciante. E. Protección de los menores y de los consumidores. F. Régimen sancionador. G. Encuadramiento impositivo.* – III. Colofón. – IV. Bibliografía.

I. Introducción

Desde hace casi una década, los que somos padres, tíos, hermanos y abuelos venimos notando en nuestros hijos, sobrinos, hermanos y nietos comentarios acerca de lo que ven y escuchan en redes sociales tales como Instagram, Facebook, Snapchat o TikTok; información que siempre interesa por parte de aquellos que mejor saben mostrarla. Lo dicho no es un intento de menospreciar la actividad de estos proveedores de contenidos, nada más alejado de la realidad. Lo que sí se busca es que la información que se suministre en las formas de expresión que se conocen hoy, pero que pueden cambiar mañana, reconozcan la presencia legal regulando dicha actividad.

El representante por Salta, Sergio N. Leavy, ha presentado en el Senado el proyecto de ley 1034/24(1) sobre "Régimen legal para influenciadores o influencers en servicios publicitarios digitales en redes sociales en todas sus modalidades". Dicho proyecto aspira a regular la actividad de los *influencers* en las redes sociales –y en todas sus modalidades–, en cuanto a sus derechos, obligaciones y régimen sancionatorio. Contiene dieciocho artículos que intentaremos comentar en el presente trabajo.

II. Análisis

En primer lugar, cabe destacar que el texto analizado no pretende legislar sobre la publicidad en general, ni tampoco sobre la publicidad digital en particular.

La norma proyectada ofrece las siguientes características:

A. Concepto de influencer

Describe al *influencer* con las siguientes notas (arts. 2, 3 y 4.1):

- Se lo define como un usuario generador de contenidos en línea. Puede tratarse de una persona humana o jurídica. La norma también abarca a las representaciones de figuras humanas creadas a través de la inteligencia artificial(2). Cabe comentar que la comunicación es –en sí misma– una actividad humana. Por ello, en el caso de las personas jurídicas, pareciera que la norma establece una responsabilidad directa por el hecho del *influencer* que sea su dependiente. En los casos en que se emplee la inteligencia artificial, no se señalan a los responsables humanos, que entendemos deberían ser aquellos que aprovechan, se sirven u obtienen provecho de la actividad (arg. art. 1758, CCCN).

- Que difunde sus mensajes de modo sistemático. Destacamos que el proyecto no pone el acento en la sistematicidad de la creación de contenidos, sino en su difusión. El concepto de difusión sistemática se torna problemático, ya que muchas veces la exposición frente a terceros depende del algoritmo o bien de que otros usuarios compartan el contenido. Tampoco es clara la mención a la sistematicidad. Podría mentar la utilización, aún ocasional, de técnicas sofisticadas de difusión, o a la habitualidad en el ejercicio de la actividad, o ambas situaciones a la vez(3).

- Que promueve productos o servicios, de modo directo o indirecto, empleando para ello cualquier mecanismo comunicacional, y a través de todo tipo de plataformas electrónicas.

- El sujeto en cuestión queda sujeto a la norma, si en su actividad alcanza una relevancia significativa. La norma no brinda elementos para cuantificar el requisito que exige, tal como podría ser la cantidad de seguidores o de visualizaciones, trasladando así la cuestión a la prudencia judicial. Sería recomendable establecer parámetros objetivos.

- Realiza su labor de modo oneroso. La norma exige que haya una contraprestación, cualquiera que esta fuera(4), con lo cual, a los supuestos en que exista actividad informativa a título gratuito, les serán aplicables las normas jurídicas generales.

- Debe tener domicilio legal o residencia habitual en el país. También se encontrarían comprendidos aquellos sujetos con domicilio o residencia en el extranjero, cuyos servicios se realicen en favor de una persona humana o jurídica que posea residencia habitual, agencia, sucursal o representación en la República. Pensamos que la norma también se debería aplicar cuando los productos o servicios se comercialicen en la Argentina, independientemente del domicilio o residencia del *influencer* o del beneficiario de la publicidad.

B. Concepto de publicidad digital

El ámbito de aplicación material de la norma es circunscripto por el art. 4.2:

- El objetivo de la publicidad debe consistir en dar a conocer un producto o un servicio.

- La actividad desplegada por el *influencer* debe nacer de una contraprestación onerosa.

- Elemento de vital importancia que radica en que el anunciante ejerza control de algún tipo en el contenido creado.

(*) La presente cápsula se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor doctor Jorge Nicolás Lafferriere, concretamente en el Programa IUS titulado: "El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable", dirigido por los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Doctor en Ciencias Jurídicas (UCA). Especialista en Derecho de Daños (UCA) y Profesor de la Pontificia Universidad Católica Argentina (UCA) en las asignaturas: "Derecho de las Obligaciones" y "Derecho de Daños". Email: fossaceca@uca.edu.ar.

(***) Profesor titular de "Obligaciones Civiles y Comerciales" en la Universidad del Salvador. Especialista en Asesoramiento jurídico de empresas. *E-mail*: jose.sabat@usal.edu.ar.

(1) S-1034/2024, https://www.senado.gob.ar/parlamentario/comisiones/verExp/1034.24/S/PL.

(2) Esta previsión es digna de encomio. Contempla casos como el de Aitana, que goza de más de 120.000 seguidores. Creada por una agencia española, posee un Instagram donde interactúa con sus seguidores. Se presenta como fan de los juegos y del *fitness*.

(3) En sus fundamentos, la norma proyectada comenta: "La Cámara Argentina de Anunciantes (CAA) hizo una clasificación de los influenciadores en función del número de seguidores. Nano Influencer los que cuentan entre 3286 y 8611 seguidores; Micro Influencer entre 8.611 y 96.111 e Influencer entre 96.111 y 575.000. Finalmente, se encuentran las celebrities, para lo cual es necesario contar con más de 575.000 de seguidores en las redes sociales". En https://www.senado.gob.ar/parlamentario/comisiones/verExp/1034.24/S/PL (acceso 20/7/2024).

(4) Ejemplifica el art. 4.3: "el pago directo o indirecto –a través de agencias–, entrega gratuita de un producto, entradas gratuitas a eventos, prestación gratuita de un servicio, cheques regalo, tarjetas de regalo, viajes". La enumeración es al solo efecto ejemplificativa.

- Incluye un gran espectro de técnicas a las cuales puede recurrir el *influencer*: desde la simple promoción y alabanza de un producto hasta el obsequio de regalos y premios.

C. Combate contra la publicidad abusiva[5] y engañosa[6]

Con base en el principio de buena fe y de autenticidad publicitaria, se trata de combatir el contenido que provoque conflictos fomentando la enemistad u ocasione equívocos en los destinatarios.

Ello explica que:

- Sea protegida la dignidad de la persona humana, evitando la discriminación de cualquier tipo (art. 5.a).

- Se tutele especialmente a la infancia y a la juventud (art. 5.b).

- Se advierta que el contenido divulgado es publicidad digital paga, si hay una contraprestación onerosa (art. 6.a). Vale destacar esta previsión, que recepta la opinión doctrinaria y las sugerencias de la Federal Trade Commission.

- Sea reconocible el anunciante detrás de la publicidad del servicio o producto (art. 6.b).

- Se encuentra prohibido dar a conocer productos o servicios que dañen la salud física o psíquica de las personas, medicamentos y alimentos no autorizados por la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica (ANMAT) o la promoción de tratamientos estéticos y/o actividades vinculadas al ejercicio profesional en el área de la salud (art. 11.a, b y e). Especial mención debe hacerse sobre la interdicción de sitios o plataformas digitales de juegos de azar o suscripciones a aplicaciones de apuestas deportivas (art.11.d).

- Se catalogue como publicidad ilícita a la abusiva y engañosa (art. 10).

Cabe añadir que el elenco de normas que menciona el proyecto es acotado y no refleja la totalidad de las normas que deben ser observadas por el influenciador. Por ejemplo, también se debe cumplir con la regulación atinente a la competencia desleal y con las previsiones en materia de publicidad de productos financieros. Sería aconsejable que el proyecto indique con claridad que la regulación propuesta se integra con la demás legislación vigente.

D. El rol del anunciante

Como se advierte, no le es posible adoptar una conducta omisiva:

- Debe aparecer su nombre en el contenido dado a conocer (art. 6.b).

- Se encuentra obligado a consignar el carácter de publicidad a desarrollar en los contratos que suscriba con el *influencer* (art. 7.a).

- Debe brindar información a este último sobre la veracidad de las afirmaciones que haga sobre la bondad o utilidades del servicio a ofrecer (art. 7.b).

- No debe infringir las normas del derecho de autor (art. 7.d).

E. Protección de los menores y de los consumidores

El proyecto de ley ha estimado a estos dos colectivos como sujetos de especial tutela.

En cuanto a los menores, se prohíbe que sean excitados a la adquisición de productos de manera directa –a través de la compra– o indirecta –pedido a los padres, por ejemplo– (art. 8). El contenido creado no puede agredirlos ni discriminarlos (art. 11.c) Debe cumplirse, además, con los requerimientos que establece la ley de protección integral de los derechos de las niñas, niños y adolescentes 26.061.

No se establece un régimen protectorio del niño *influencer*, tal como los vigentes en el Estado de Illinois o en Francia.

En cuanto a los segundos, se aplican las reglas de la ley consumeril argentina (ley 24.240). Resulta ser de primigenia importancia el carácter veraz y claro que los *influencers* brindan en el contenido que creen.

F. Régimen sancionador

Se establecen como pena las modalidades de apercibimiento, retiro del anuncio o multa por un valor equivalente a 10 y hasta 1000 SMVM –salario mínimo vital y móvil– (art. 13).

El proyecto también señala que el retiro del anuncio procederá mediando intervención judicial. Dicho criterio no refleja adecuadamente la jurisprudencia de la Corte Suprema de Justicia de la Nación en relación con los buscadores de Internet. En los actuados "R., M. B."[7], la Corte federal indicó que el obrar diligente de los buscadores (en este caso, sería el de las plataformas) consiste en eliminar los resultados (aquí hablaríamos de posteos) cuya antijuridicidad sea grosera y manifiesta, ante la sola comunicación fehaciente del afectado o de cualquier persona. En los demás casos, será necesario esperar la orden judicial o administrativa.

El proyecto adjudica competencia al fuero civil para conocer las apelaciones sobre las multas impuestas. Es de entender que ello dependerá de la organización judicial de cada provincia, habida cuenta de la organización federal de nuestro país. Entendemos que hubiese bastado con señalar que no será competente el fuero federal.

El régimen sancionador se hace extensivo a los intermediarios y empresas cuyos servicios y productos sean promocionados o publicitados (art. 12).

G. Encuadramiento impositivo

Debemos aclarar que el art. 15 de la norma entiende que, si la prestación que beneficia al *influencer* es pecuniaria, debe inscribirse en la AFIP como trabajador autónomo, en condición de monotributista o de responsable inscripto, dependiendo del volumen de su facturación.

La exigencia del encuadramiento impositivo por parte del legislador resulta correcta, pues la actividad desarrollada integra la cadena de publicidad de un producto o un servicio, ya se estime la figura contractual como innominada o como una locación de servicio.

III. Colofón

Creemos que es necesario regular la figura del *influencer* en nuestro país. Estimamos conveniente que sea regulado de manera más orgánica como, por ejemplo, en una ley sobre la publicidad en general.

Respecto al proyecto ponderado, resultará un avance –en caso de ser sancionado–, pero requeriría de ciertas precisiones. Entre ellas, una mejor organización temática de su articulado, una mayor coordinación con otras leyes vigentes, afinar los conceptos de difusión sistemática y de relevancia significativa, ajustar la cuestión procesal con la organización federal del país, y adaptar lo atinente al retiro del anuncio a los lineamientos establecidos por la Corte federal.

Destacamos que también existen cuestiones importantes sobre las que el proyecto no se expide, como ser la responsabilidad civil del *influencer* y la protección de los influenciadores menores de edad. Pero entendemos que, siendo un proyecto, deja el debate abierto para discutir la inclusión de puntos como el señalado, como así también de otros puntos reseñados con anterioridad.

IV. Bibliografía

- S-1034/2024, https://www.senado.gob.ar/parlamentario/comisiones/verExp/1034.24/S/PL.

- CSJN, 28/10/2014, "R., M. B. c/Google Inc. s/daños y perjuicios", LL, 2014-F, 401.

VOCES: RESPONSABILIDAD CIVIL - TECNOLOGÍA - CÓDIGO CIVIL Y COMERCIAL - INFORMÁTICA - DERECHO DE PROPIEDAD - EMPRESAS - TELECOMUNICACIONES - DAÑO - DAÑOS Y PERJUICIOS - PERSONA - JURISPRUDENCIA - CORTE SUPREMA DE LA NACIÓN - DERECHO COMPARADO - COMERCIO E INDUSTRIA - INFLUENCER - INTELIGENCIA ARTIFICIAL - PROTECCIÓN DE DATOS PERSONALES - DEFENSA DEL CONSUMIDOR - INTERNET - PUBLICIDAD - OBLIGACIONES - CONTRATOS - ECONOMÍA

(5) Es "cuando se ofende, favoreciendo la discriminación por género, racial, social, política e induce a actividades antisociales, criminales o ilegales, incita a la violencia y atenta contra la dignidad de las personas" (art. 4.4).

(6) Es "cuando a través de ella se induce al error sobre el producto, en los precios, características o cualidades, situación que se alcanza por vía de acción o de omisión y cuando la publicidad contenga información falsa o que aun siendo veraz por su contenido o presentación induzca o pueda inducir a error a los destinatarios, siendo susceptible de alterar sus decisiones económicas. Es también publicidad engañosa la omisión de información necesaria para que el destinatario pueda adoptar una decisión económica con el debido conocimiento de causa, cuando la información que se ofrece es poco clara, inintelegible, ambigua, no se ofrece en el momento adecuado, o no se da a conocer el propósito comercial de esa práctica, cuando no resulte evidente por el contexto" (art. 4.5).

(7) CSJN, 28/10/2014, "R., M. B. c/Google Inc. s/daños y perjuicios", LL 2014-F, 401.

¿La IA nos quitará el trabajo? Políticas para una transición responsable(*)

por Angélica Borda(**)

Sumario: I. A modo de introducción. – II. Impacto de la IA en el empleo. – III. Políticas para una transición responsable.

I. A modo de introducción

Después del entusiasmo por el boom de ChatGPT, llegaron las dudas: ¿la IA nos dejará sin trabajo?, ¿la IA es más inteligente que un humano?

El impacto que tendrá la Inteligencia Artificial es comparable al que tuvo la electricidad, con la variante de que el avance de la IA es exponencial. Por eso, para usar todo el potencial de esta tecnología en beneficio de los humanos, y no al revés, es crucial implementar políticas de transición *efectivas* y *coordinadas* entre el sector público y privado.

La clave está en la educación, el reskilling (recapacitación) y el upskilling (mejora de habilidades) de la fuerza laboral para adaptarse a los cambios tecnológicos.

II. Impacto de la IA en el empleo

La Inteligencia Artificial tiene el potencial de reemplazar ciertos empleos, especialmente aquellos que involucran tareas repetitivas y rutinarias. Sin embargo, también crea nuevas oportunidades laborales en áreas emergentes.

Según el informe "Future of Jobs Report 2023" del Foro Económico Mundial, para el 2027 se estima que se perderán 83 millones de empleos y se crearán 69 millones, constituyendo una rotación estructural del mercado laboral de 152 millones de empleos, o el 23% de los 673 millones de empleados. En resumen, esto implica una rotación de la cuarta parte del mercado laboral y una reducción del 2% del total de empleos(1).

III. Políticas para una transición responsable

Para producir la mencionada transición con la incorporación de nuevas tecnologías, como la IA, se necesita una estrategia coordinada entre *gobiernos*, *empresas* y *organizaciones*:

1. Colaboración público-privada: Una colaboración estrecha entre el sector público y el privado puede garantizar que las políticas de empleo y capacitación sean efectivas y estén alineadas con las necesidades del mercado.

2. Reskilling y upskilling: Las empresas deben invertir en el reciclaje y la mejora de las competencias de sus trabajadores. El reskilling se refiere al proceso de formar a los empleados en nuevas habilidades, que les permitan adaptarse a los cambios en el entorno laboral. El upskilling se centra en mejorar o actualizar las habilidades existentes de los trabajadores.

3. Apoyo gubernamental: Los gobiernos deberán apoyar la innovación con la regulación necesaria para hacer que las nuevas tecnologías sean seguras y, a la vez, realizar importantes inversiones en capacitación, fomentar certificaciones rápidas y generar asociaciones entre el sector educativo, empresas y organizaciones sin fines de lucro.

4. Redes de seguridad social: Es necesario un debate serio y con honestidad intelectual, respecto a las políticas de seguridad social que se deberán desarrollar, en caso de que se presente un escenario de desempleo masivo. Centros de empleo, seguros de desempleo y programas de apoyo a la reubicación laboral, son opciones para ayudar a los trabajadores que se vean afectados por la automatización.

Y desde lo individual, ¿cómo podemos prepararnos para la revolución 4.0?

La resiliencia y el aprendizaje continuo serán la clave.

VOCES: TECNOLOGÍA - INTERNET - DERECHO COMPARADO - INFORMÁTICA - ESTADO - DERECHOS Y GARANTÍAS CONSTITUCIONALES - CULTURA - PODER JUDICIAL - ECONOMÍA - TRABAJO - INTELIGENCIA ARTIFICIAL - CONSTITUCIÓN NACIONAL - RIESGOS DEL TRABAJO - CONTRATO DE TRABAJO - DERECHO DEL TRABAJO - DISCRIMINACIÓN LABORAL

(*) La presente cápsula se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor doctor Jorge Nicolás Lafferriere, concretamente en el Programa IUS titulado: *"El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable"*, que dirigen los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Abogada (UNLP), Master en Inteligencia Artificial (Centro Europeo de Posgrado), Data Science (Henry Bootcamp), Diplomado en Inteligencia Artificial y Derecho (UBA), Diplomado Web 3.0 Metaverso y Gaming (UBA), Co-Founder de AI4Humans y abogada en Asesoría General de Gobierno de la Pcia. de Bs. As.

(1) Informe del Foro Económico Mundial (World Economic Forum). "The Future of Jobs Report 2023". World Economic Forum, 2023. Disponible en: https://www.weforum.org/publications/the-future-of-jobs-report-2023.

Generación de valor público a través de la innovación participativa en LATAM: intercambio de experiencias entre el Laboratorio de Gobierno de Chile y el Ministerio Público de la provincia de Buenos Aires(*)

por Patricio J. Moyano Peña(**)

En junio pasado viajé a Santiago de Chile –en mi carácter de titular del Programa MPBA 2050 del Ministerio Público de la provincia de Buenos Aires–, con el objetivo de fortalecer vínculos con organismos públicos e instituciones académicas, promover la cooperación y asistencia recíproca en materia de innovación tecnológica, gestión pública y diseño centrado en las personas.

Durante mi visita mantuve una reunión con el Laboratorio de Gobierno(1) dependiente del Ministerio de Hacienda Nacional, una institución modelo en Latinoamérica, establecida en 2014 como respuesta a la desconexión entre la ciudadanía y el Estado, la necesidad de incrementar la eficiencia estatal, articular a los actores del ecosistema y abordar la creciente complejidad de los problemas públicos (Laboratorio de Gobierno, 2018).

Me recibieron Catalina Gutiérrez Ricci –titular del área de Consultoría Ágil– y Eduardo Navarro Aracena –coordinador de Análisis Jurídico y Financiero–, y me compartieron las técnicas que utilizan para interpretar las necesidades de los ciudadanos y los agentes públicos, fomentar la creatividad en el sector estatal y cocrear soluciones innovadoras. Además, el trabajo que están desarrollando en materia de compra pública por innovación es trascendental para fortalecer el ecosistema GovTech, marcando un camino hacia un Estado más eficiente y conectado con las demandas sociales.

La experiencia del Laboratorio de Gobierno resuena directamente con las iniciativas del Ministerio Público de la provincia de Buenos Aires en materia de innovación pública. En mayo de 2018, el Procurador General de la Provincia, Dr. Julio Conte-Grand, creó el Programa MPBA 2050(2) [Resolución (PG) 353/18], uno de los proyectos neurálgicos del Plan Estratégico del organismo, y me designó como su titular.

Este programa es una usina de ideas de alta tecnología, orientada a optimizar el servicio de justicia y garantizar la tutela judicial efectiva mediante un proceso de mejora continua e innovación institucional. Impulsa una transformación de la cultura organizacional que orientará el trabajo del Ministerio Público en las próximas décadas, con el horizonte temporal en el año 2050. Su impronta de modernidad y de largo plazo determinó la elección de su nombre.

El Programa 2050, conformado en forma interdisciplinaria, se apoya en tecnologías emergentes y modernas técnicas de gestión como el diseño de servicios, el *Design Thinking* y las metodologías ágiles, colaborando en forma estrecha con la Subsecretaría de Informática y otras áreas de la Procuración General.

Desde su puesta en marcha, ha intervenido en más de 130 iniciativas tecnológicas(3). Entre ellas se destaca el Expediente Electrónico Penal (IPP Electrónica), una suerte de "gemelo digital" de la investigación criminal que mejora la accesibilidad de la información, facilita el trabajo complementario y simultáneo de las áreas de gestión, y contribuye a la reducción del uso del papel. Desde su implementación, se han realizado más de 24.7 millones de trámites.

Otra iniciativa importante es la integración con el Sistema de Información Delictual (SID) del Ministerio de Seguridad de la Provincia, mediante la cual las denuncias penales y actas de procedimiento policial presentadas en las comisarías son recibidas inmediatamente en forma digital por los organismos judiciales intervinientes. Hasta el momento, se han digitalizado más de 3.7 millones de denuncias penales, lo que implica un ahorro de –al menos– 31.233 días hábiles judiciales.

Una tercera iniciativa es la integración con la aplicación web "Mi Seguridad" que permite la formulación de denuncias digitales ciudadanas sin necesidad de acudir a una comisaría. A través de esta app, se han formulado 464 mil denuncias por narcomenudeo, corrupción policial, robos y hurtos, entre otras figuras penales.

También se implementó el CRM del Ministerio Público, una herramienta tecnológica que proporciona información relevante sobre el proceso penal de manera automatizada a denunciantes o víctimas de delitos. Hasta el momento, a través de este mecanismo, han sido contactadas más de 1.6 millones de personas.

Además, se destaca el desarrollo del primer asistente virtual del Poder Judicial a nivel nacional, la implementación del Expediente Electrónico Administrativo, el Sumario Policial Digital, el sistema de Investigación Criminal, la integración con los sistemas de gestión judicial de la Suprema Corte de Justicia de la Provincia, el Tablero de control del Ministerio Público Fiscal y la adopción de metodologías ágiles.

Estos y otros proyectos han consolidado al Ministerio Público como un referente internacional en innovación pública, validado por la reciente incorporación del Programa MPBA 2050 a la Case Library del Observatorio de Innovación Pública de la OCDE(4).

La interacción con el Laboratorio de Gobierno, que comparte nuestra visión y compromiso con la modernización del Estado, es fundamental para mejorar y adaptarnos a las necesidades de la sociedad. Esta vinculación nos permite intercambiar experiencias y aplicar mejores prácticas asegurando una tutela judicial continua y efectiva, y un acceso irrestricto a la justicia. Tanto el Ministerio Público como el Laboratorio de Gobierno coinciden en que la innovación y la participación ciudadana son pilares esenciales para un servicio público eficiente y centrado en las personas.

Referencias

Laboratorio de Gobierno (2018). *Un Estado innovador para las personas: los primeros años del Laboratorio de Gobierno*, 2014 - 2018, Gobierno de Chile.

VOCES: ABOGADO - DEMANDA - NOTIFICACIÓN - PODER JUDICIAL - PROCESO JUDICIAL - INFORMÁTICA - TECNOLOGÍA - CORTE SUPREMA DE LA NACIÓN - DOMICILIO - DEFENSA EN JUICIO - EXPEDIENTE JUDICIAL - EJERCICIO PROFESIONAL - JUECES - DERECHO PROCESAL - SENTENCIA - PROCESO ORDINARIO - JURISPRUDENCIA - CONSTITUCIÓN NACIONAL - EJERCICIO PROFESIONAL - COMUNICACIONES ELECTRÓNICAS - NORMAS DE EMERGENCIA - CONSEJO DE LA MAGISTRATURA - INTERNET - INTELIGENCIA ARTIFICIAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - ACCESO A LA JUSTICIA - RECURSOS PROCESALES

(*) La presente cápsula se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor, doctor Jorge Nicolás Lafferriere, en el Programa IUS titulado: "El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable", dirigido por los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Abogado con diploma de honor (UCA). Coordinador de Relatores del Procurador General ante la Suprema Corte de Justicia de la Provincia de Buenos Aires y Titular del Programa MPBA 2050. Fellow del Programa GovTech Latam del BID, BID Lab, IE PublicTech Lab y el Center for the Governance of Change. Integrante del Observatorio de Derecho, Tecnología e Innovación de la UMSA. Profesor en la UCA y en el IUV. Egresado del Posgrado en E-Business Management de la Universidad del Salvador y Georgetown University. Maestrando en Dirección Estratégica de Tecnología por el Instituto Tecnológico de Buenos Aires. Programas de formación continua en Massachusetts Institute of Technology Professional Education, EOI, Singularity University, Hyper Island North America, Kaospilot, AOTS Japón, IAE, UTN, UCEMA y San Andrés.

(1) https://www.lab.gob.cl/.

(2) https://www.mpba.gov.ar/v2050/index.

(3) Visión de agentes judiciales sobre el proceso de transformación digital del Ministerio Público: https://www.youtube.com/watch?v=M5nfaz8l0uQ.

(4) https://oecd-opsi.org/innovations/cultural-and-technological-transformation-of-the-criminal-justice-service-in-the-province-of-buenos-aires/.

Tras bambalinas de la liberación de criptoactivos en Bolivia(*)

por Fabián Espinoza Valencia(**)

Las políticas públicas deben estar enfocadas en garantizar el goce efectivo de todos los derechos y garantías de la ciudadanía. Prohibir la implementación de tecnologías emergentes que otorgan mayor libertad prácticamente menoscaba esa seguridad jurídica. Es por ello que, desde la decisión del Banco Central de Bolivia (BCB) en 2014 de prohibir el uso de criptoactivos (CA) en Bolivia, se gestó una serie de acciones desde el activismo, para eliminar la prohibición.

Es complejo asimilar la repentina decisión del BCB, implantando una posible explicación relativa a que la economía está en peores condiciones de las aparentes, y por ello se tuvo que optar por medidas extremas de esta naturaleza inclusiva.

Ciberjusticia como plataforma de control social del derecho informático boliviano ha desplazado una serie de acciones desde 2022; con el apoyo de la comunidad técnica y alianzas estratégicas; para incidir en que los CA no estén prohibidos en Bolivia, teniendo siempre presente el reto de pretender regular la desregularización. Esta la cronología:

a) 10 de diciembre de 2022: Reunión de directorio en la que se aprueba el punto único del orden del día para elaborar una hoja de ruta estratégica para dejar sin efecto la resolución de Directorio Nº - RDN 144/2020 que prohíbe el uso, comercialización y negociación de criptoactivos en el sistema de pagos nacional por no constituirse estos en moneda de curso legal en el país.

b) 10 de enero de 2023: Consulta sobre transacción de activos, un cuestionario de 8 preguntas, que solo obtuvo una única respuesta en la que dan a conocer que se emitió la Resolución de Directorio Nº - RDN 144/2020 de 15 de diciembre en la página web.

c) 14 de febrero de 2023: Respuesta del BCB, en el que únicamente refiere que se emitió la RDN 144/2020, y que la supervisión corresponde a ASFI.

d) 17 de febrero de 2023: Se interpone recurso de revocatoria con efecto devolutivo, por la vía del derecho administrativo.

e) 03 de marzo de 2023: RDN Nº 046/2023 que desestima la impugnación en contra de la RDN Nº 144/2020, resolviendo: PRIMERO - Desestimar el recurso de revocatoria de 17 de febrero de 2023, por haber sido interpuesto fuera del término establecido en el artículo 55 de la Ley del BCB de Bolivia.

f) 14 de abril de 2023: Interposición de Recurso Jerárquico en contra de la RDN Nº 46/2023 que desestima el recurso de revocatoria.

g) 12 de mayo de 2023: Se solicita información a la Autoridad de Supervisión del Sistema Financiero (ASFI) sobre regulación de CA y un potencial menoscabo a derechos fundamentales referidos a la propiedad de activos virtuales.

h) 16 de mayo de 2023: Se interpone Recurso de Alzada conforme a la Ley Nº 1670 del BCB de Bolivia.

i) 17 de mayo de 2023: Se presenta el primer anteproyecto de "Ley de Cripotactivos", día internacional de las telecomunicaciones.

j) 17 de mayo de 2023: Se presenta un proyecto de RDN sobre CA, día internacional de las telecomunicaciones.

k) 22 de mayo de 2023: Respuesta de la Autoridad de Supervisión del Sistema Financiero (ASFI) en el que se indica que son atribuciones del BCB de Bolivia, y ellos dispusieron la prohibición a través de la RDN 144/2020.

l) 31 de mayo de 2023: Nota de respuesta, que señala que "corresponde a usted remitirse a lo dispuesto en dicha Resolución", haciendo alusión a la RDN 046/2023 que desestima el recurso se revocatoria.

m) 31 de mayo de 2023: Solicita cumplimiento de plazos para remisión de obrados en relación con el recurso de alzada.

n) 31 de mayo de 2023: Se responde al proyecto de resolución indicando textualmente "(...) conforme al marco de competencias del Ente Emisor establecidas en la CPE, la Ley Nº 1670, los Estatutos y la normativa vigente, agradeceré a usted reconducir la iniciativa presentada a las instancias pertinentes".

o) 19 de junio de 2023: La Universidad Pública Mayor de San Andrés (UMSA) remite una invitación para participar en las "XII Jornadas de Informática, Derecho y Telecomunicaciones" para explicar y socializar el proyecto de ley sobre CA.

p) 19 de junio de 2023: Se inició una petición en la plataforma CHANGE.ORG, en la que se colectaron hasta 908 firmas.

q) 31 de agosto de 2023: Se presenta el "Proyecto de Ley de Adopción Integral de CA" con la Firma de los diputados: Mariela Baldivieso (de Comunidad Ciudadana) y Délfor Germán Burgos (del Movimiento Al Socialismo). Como proyectista Ph.D.c. F. Fabián Espinoza Valencia.

r) 19 de octubre de 2023: Se realiza la socialización del proyecto de ley sobre CA en la Universidad Católica Boliviana "San Pablo" Regional La Paz, organizada por la sociedad científica de ciencias políticas.

s) 15 de diciembre de 2023 (misma fecha en la que en 2020 se emite la RDN 144): con el respaldo de Asoblockchain y la Comunidad Ethereum Bolivia con la firma de 26 ciudadanos se presenta una nota cuestionando la legalidad de los CA en Bolivia mediante una nota al BCB de Bolivia.

t) 08 de enero de 2024: Respuesta a nota en la que indica que, conforme a ley, se crea el peso boliviano como única moneda de curso legal, y que la RDN 144/2020 establece la prohibición a las entidades financieras del CA en el sistema de pagos nacional.

u) 21 de febrero de 2024: Se interpone recurso de revocatoria con efecto devolutivo, conforme lo establece la Ley del BCB en contra de la RDN 144/2020 por presunta

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *Obligaciones en moneda extranjera frente a la ruptura del sinalagma contractual como consecuencia de la conducta del Estado Nacional*, por Pablo A. Pirovano, ED, 249-598; *Obligaciones dinerarias (arts. 765 y 766 del proyecto de la Comisión Redactora) y la sustitución por el art. 765 redactado por el Poder Ejecutivo Nacional. Análisis del régimen propuesto por ambas partes. Viabilidad, consecuencias y comentarios*, por Silvia Amelia Canna Bórrega, ED, 251-558; *De la interpretación en materia cambiaria*, por Hernán Verly, ED, 252-507; *Obligaciones celebradas en moneda extranjera y actuales normas cambiarias*, por Silvina M. Pagliotto, ED, 255-708; *El régimen de las obligaciones en moneda extranjera. Regla general y excepciones. Como regla general es obligación facultativa. En todos los casos es obligación dineraria*, por Daniel Bautista Guffanti, ED, 271-573; *Una aproximación al concepto de "moneda"*, por Estela B. Sacristán, ED, 283; *Las criptomonedas vistas desde el derecho*, por Miguel E. Rubín, ED, 283-618; *Medios de pago electrónico, criptoactivos y blockchain*, por Santiago E. Eraso Lomaquiz, ED, 285-513; *Régimen aplicable a las criptomonedas a tenor del derecho privado*, por José M. Sabat Martínez y Lourdes Lucero, ED, 288-1271; *Los criptoactivos a la luz del derecho argentino: estado de la situación ante incipientes desafíos*, por Gonzalo Ariel Viña, ED, 290-917; *Las criptomonedas: naturaleza jurídica. Encuadre jurídico*, por María Belén Gallardo, Derecho, Innovación & Desarrollo Sustentable, N° 2, agosto 2021; *Reflexiones en torno a los criptoactivos*, por Emiliano Carlos Lamanna Guiñazú y Carlos Alberto Fossaceca, Derecho, Innovación & Desarrollo Sustentable, Número 6 - abril 2022. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) La presente cápsula se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor doctor Jorge Nicolás Lafferriere, concretamente en el Programa IUS titulado: *"El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable"*, que dirigen los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Abogado (Universidad Católica Boliviana); Master Derecho digital y sociedad de la información (Universitat de Barcelona); Doctor en Cs. Jurídicas (UCA); Especialista en Derecho de internet; Docente, Investigador de ciberseguridad, compliance normativo y criptoactivos - web3.0.

vulneración de derechos de propiedad y libertad económica.

v) 05 de marzo de 2024: Se emite la RDN 033/2024 que desestima la impugnación en contra de la RDN 144/2020.

w) 17 de abril de 2024: Se interpone Recurso de Alzada en contra de la RDN 033/2024 que desestima el Recurso de Revocatoria

x) 23 de abril de 2024: El BCB emite una nota firmada por la secretaria de Directorio en la que pone el conocimiento la RDN 033/2024 (que desestima el recurso interpuesto) y que "(...) corresponde a usted remitirse a lo dispuesto en dicha Resolución".

y) 02 de mayo de 2024: Se solicita el cumplimiento de procedimiento administrativo para la remisión al superior en grado (Ministerio de Economía) para que se pronuncie sobre el Recurso de Alzada.

z) 14 de mayo de 2024: Se reitera la solicitud de cumplimiento del procedimiento administrativo para la remisión del Recurso de Alzada al Ministerio de Economía dentro de los plazos legales.

aa) 12 de junio de 2024: Se presenta la propuesta normativa con el siguiente artículo único: "Abrogar la RDN 144/2020 de 15 de diciembre de 2020 para salvaguardar el derecho constitucional a la propiedad, libertad económica y patrimonial en el marco de los artículos (...) de la Constitución Política del Estado".

bb) 25 de junio de 2024: El BCB de Bolivia emite la RDN 082/2024 que deja sin efecto la RDN 144/2020.

cc) 01 de julio de 2024: Ciberjusticia emite un manifiesto sobre la decisión de dejar sin efecto la prohibición.

Extraña que, quien *ayer* rechazaba rotundamente esta revolución, *hoy* expone estadísticas (sin fuentes verificadas) y capacita al respecto. Lo primero que llama la atención es que, la parte final del artículo 1 de la RDN 144/2020 señala que "(...) se prohíbe a las entidades financieras el uso, comercialización y negociación de criptoactivos en el sistema de pagos nacional por no constituirse estos en moneda de curso legal en el país". Siendo este último criterio el argumento principal de la política prohibitiva. A pesar de la emisión de la RDN 082/2024 que deja sin efecto la resolución inicial, sigue sosteniendo el argumento de la prohibición, sosteniendo que los criptoactivos no se constituyen en moneda de curso legal, pero a pesar de aquello, ahora ya no están prohibidos, ¿se trata acaso de una antinomia jurídica?

Se dice que *somos esclavos de nuestro pasado*. Revisando la cronología de acciones realizadas, se identifica una serie de imprecisiones y potenciales contradicciones entre los informes técnicos del Órgano Ejecutivo sobre: la iniciativa legislativa sobre CA, la resolución del BCB que deja sin efecto la prohibición de CA en Bolivia y la motivación de dicha decisión, dando lugar a una serie de cuestionamientos relevantes.

1. Comunicado del BCB de Bolivia

En el comunicado de prensa CP35/2024 de 26 de junio de 2024, en el que se comunica la emisión de la RDN 082/2024 que deja sin efecto la RDN 144/2020, habilitando el uso de activos virtuales, señala que dicha decisión fue efectuada "(...) considerando la Evaluación Mutua del Estado Plurinacional de Bolivia 2024 que realizó el Grupo de Acción Financiera de Latinoamérica (GAFILAT), que entre sus recomendaciones señala: '...considerar la regulación del Proveedor de Servicios de Activos Virtuales (PSAV) conforme a la política pública que se defina en el contexto boliviano".

1.1. Informe del Ministerio de Economía

Sin embargo, el 21 de noviembre de 2023, el informe MEFP/VPSF/DGSF/USSF/Nº 760/2023 del Ministerio de Economía y Finanzas Públicas (firmado por el propio ministro) al Proyecto de Ley Nº 497/2022-2023 "Ley de adopción integral de CA" (del cual fuimos proyectistas), indica lo siguiente:

1.1.1. *"El proyecto de ley de referencia contraviene la Constitución y el ordenamiento jurídico vigente, toda vez que el artículo 326 de la CPE determina que las transacciones públicas en el país se realizarán en moneda nacional, quedando establecido para este fin la Ley Nº 901 (...) las cuales prevén que la única moneda de curso legal y poder liberatorio es el 'boliviano'"*. ¿La RDN Nº 082/2024 contraviene, entonces, la Constitución?

1.1.2. *"La recomendación 15 de los estándares internacionales del Grupo de Acción Financiera (GAFI), menciona que los países pueden adoptar como enfoque en materia de regulación de activos virtuales, la prohibición de las operaciones con activos virtuales (AV) y de las actividades de los proveedores de servicios de activos virtuales (PSAV). En ese sentido, el BCB aprobó la RDN 144/2020 a través de la cual prohíbe a las entidades financieras el uso, comercialización y negociación de CA en el sistema de pagos nacionales, por no constituirse estos en moneda de curso legal en el país"*. ¿No es que la decisión de admitir activos virtuales fue considerando la recomendación de la evaluación mutua del Estado (en diciembre de 2023, no 2024 como indica el comunicado) que realizó GAFILAT?

1.1.3. Asimismo, el informe indica que *"(...) es imprescindible tener estudios, estadísticas y otros elementos técnicos necesarios que permitan evaluar estas tecnologías (...) En cuanto a la prevención del lavado de dinero y el financiamiento del terrorismo corresponde puntualizar que, para la regulación de los sujetos obligados en esta materia, conforme pretende hacerlo el proyecto de ley, es necesario que con carácter previo se desarrollen estudios sectoriales, que definan el nivel de riesgos, identifiquen la existencia de proveedores de servicios de activos virtuales y proyecten alternativas de procedimientos, controles, autoridades y sanciones en el marco de los criterios del GAFI"*. El BCB no hizo nada de eso, por lo que ¿se puede inferir que el BCB ha incumplido con los criterios del Ministerio de Economía?

1.1.4. El informe, en el acápite final dictamina *"finalmente, se señala que un proyecto de ley debe permitir o prohibir alguna acción con el objetivo de regular las conductas de las personas y lograr una convivencia armoniosa (...) estableciéndose que, de la revisión del contenido del proyecto de ley, el mismo no cuenta con esa seguridad jurídica que permita poder efectuar la administración, el control, la supervisión, la fiscalización, las sanciones y otros, que brinden certidumbre en el territorio nacional"*. ¿La RDN Nº 082/2024 si cumple con todos los anteriores aspectos?, ¿brinda certidumbre en el territorio nacional?

1.2. Más adelante, el comunicado señala: "(...) y tomando en cuenta que el último periodo se ha ido generado una base jurídica (...)", ¿en qué último periodo?, ¿qué base jurídica se ha ido generando? Si los informes al proyecto de ley precitado de la AGETIC, Ministerio de Justicia, Ministerio de Planificación y Ministerio de Economía descartan la opción de legalizar los CA por: no constituirse en una moneda de curso legal.

1.3. Informe del Ministerio de Justicia

El informe MJTI-DESP-NE-Z-1380-2023 de 27 de noviembre de 2023 del Ministerio de Justicia, por su parte, señala que para regular CA se debería analizar y desarrollar de forma clara, objetiva y coherente aspectos como: los medios personales y materiales necesarios y los efectos presupuestarios y económicos que generaría su aplicación. La RDN Nº 082/2024 no cumple con ninguno de esos aspectos.

1.4. Informe del Ministerio de Presidencia - Agencia de Gobierno Electrónico y Tic (AGETIC)

El informe AGETIC/NE/4543/2023 - expediente: 224719 de 31 de octubre de 2023 señala lo siguiente:

1.4.1. *"El proyecto de norma, específicamente su artículo 9, se constituye en una antítesis de la parte resolutiva de la RDN 144/2020 aprobada por el BCB. Sin embargo, la sustentación técnica no está adecuadamente sistematizada ni logra rebatir los argumentos que expresa el BCB"*. El artículo 9 del proyecto, precisamente, cambia el verbo rector de "prohíbe" a "admite", más nada. Una iniciativa legislativa, desde la técnica legislativa no debe ni necesita rebatir argumento alguno porque su estructura teleológica es distinta.

1.4.1.1. Cita *"(...) siendo una opción plantear la emisión del 'boliviano digital'"*. Esto es un peligro, porque desnaturaliza la esencia de los CA y su tecnología (cadena de bloques) que es descentralizada, sin el control centralista y monopólico de ninguna entidad ni Estado.

1.4.1.2. *"No regula absolutamente nada en lo relativo a esta tecnología"* (cadena de bloques). Y es que esa es precisamente la intención, no regular dicha tecnología, y únicamente postular una propuesta marco para que ya no exista prohibición al respecto.

1.4.1.3. *"Pretender regular una red descentralizada parece ser técnicamente inviable, un contrasentido a la*

naturaleza de esta tecnología y puede llegar a desincentivar la inversión e innovación". Extraña dicha aseveración, sabiendo que líneas antes, observa la no regulación de la tecnología por parte de la iniciativa. Y ¿cuándo el Estado regule CA estará desincentivando la inversión e innovación?

Lo que siempre se debe tener presente es que la esencia de la cadena de bloques (*blockchain*) y CA radica en su desregularización, y la reglamentación de los entes estatales debe ser, si acaso, de mínima intervención, porque en revoluciones como esta, la regulación es parte del problema y no de la solución.

VOCES: CRIPTOACTIVO - CRIPTOMONEDAS - CONTRATOS - OBLIGACIONES - DAÑOS Y PERJUICIOS - DERECHO CIVIL - PAGO - LEY - ECONOMÍA - INTELIGENCIA ARTIFICIAL - ESTADO - ENTIDADES FINANCIERAS - MONEDA - CAMBIO - EMPRESA - CÓDIGO CIVIL Y COMERCIAL - TECNOLOGÍA - INFORMÁTICA - COMERCIO E INDUSTRIA - GRUPOS ECONÓMICOS - PERSONAS JURÍDICAS - CLÁUSULAS CONTRACTUALES - PHISHING - BASE DE DATOS - NEGOCIO COMERCIAL - INTERNET - DELITO INFORMÁTICO - COMUNICACIONES ELECTRÓNICAS

DOCTRINA

DDoS vs. los forenses digitales: entre los estándares y la ley(*)

por Susana Eloísa Mender Bini(**) y Tomás Illuminati Balbín(***)

I. André Bolívar Conté contra el mundo: el detonante(1)

Durante el año 2020, en los meses de Pandemia, tanto la Policía Nacional como el Ministerio de Educación de Panamá sufrieron ataques de índole informático, ambos el día 18 de agosto. La primera detectó un ingreso indebido a la plataforma APPRA –sistema de reclutamiento y selección de aspirantes a servir dentro de la fuerza–. En dicho ataque los datos registrados en la plataforma fueron utilizados, e incluso modificados; para luego ser publicados en la red social Twitter –hoy X– en la cuenta de @ Annonymous_Panama por el atacante.

Contra la segunda institución, la vulneración consistió en impedir la transmisión de información/datos de la página web del ministerio, por medio de un ataque de denegación de servicio. Ello imposibilitó que los estudiantes pudieran acceder a los programas de estudios que se encontraban alojados en la web del ministerio.

En base a uno de los informes periciales, en los que se investigó uno de los IP –pertenecientes a la madre del imputado– que tuvieron acceso indebido a las bases de datos, sumado a otros supuestos indicios (la presencia de una máscara como del personaje V de la Vendetta, los conocimientos del acusado, algunas otras actividades realizadas por el mismo –sin vinculación con la causa–) llevaron al organismo acusatorio a endilgar la autoría delictiva en la persona de André Bolívar Conté.

No obstante, pese a la extensa documental probatoria presentada por la parte acusatoria –peritos, informes, testimonios–, a los ojos del tribunal las mismas no logran corroborar ni acreditar las afirmaciones dadas por el Ministerio Fiscal, quien las consideró ciertas. En efecto, conforme lo sostuvo el tribunal, la investigación peca de ser sesgada, pues los aportes científicos presentados no fueron debidamente motivados y sustentados, lo que impidió acreditar los hechos adjudicados.

Cabe destacar que la existencia de los hechos delictivos sufridos por los distintos organismos afectados el día 18/08/2020 no se encuentran cuestionados en su veracidad. No obstante, las probanzas obrantes en la causa no pudieron acreditar la autoría de los mismos, es decir que no se pudo determinar quién/es estuvieron involucrados en ambos ataques. Ni en el caso de IP, perteneciente a la madre de Conté, se pudo corroborar que fuese uno de los que causó el ataque diversificado de denegación de servicio contra el Ministerio de Educación.

A fin de cuentas, sin un sospechoso cuya conducta delictiva haya sido debidamente acreditada, no se podría tener por configurado **(y acreditado)** el delito en su plenitud para poder aplicar la sanción penal correspondiente. Ahora bien, cabe descifrar: ¿qué fue lo que falló, para que la causa se resolviera con una sentencia absolutoria?, **y todo ello** pese a la extensa prueba desarrollada en la causa...

Conforme se desprende de los fundamentos de la resolución, las pericias practicadas no fueron suficientes para demostrar la autoría, atento a que no se dio un adecuado manejo de la evidencia digital, no hubo un cumplimiento respecto a los procedimientos de cadena de custodia, como tampoco se acataron los estándares internacionales que versan sobre manejo de prueba digital.

Para lograr un mejor entendimiento de los hechos acontecidos en la causa y los yerros cometidos por parte de la fiscalía y de los afectados, resulta propicio adentrarnos en la temática digital y desentrañar el funcionamiento de los ataques DDoS, qué sistemas usan los atacantes para poder ejecutar este tipo de agresión digital y cómo funcionan los mismos; tales como TOR, VPN, Proxies.

Así también resulta menester conocer y comprender cuáles son las herramientas con las que se cuenta para los análisis forenses en materia digital y los estándares inter-

(1) Tribunal de Juicio del Primer Circuito Judicial de Panamá, André Bolívar Conté Sánchez s/Delitos contra la Seguridad Informática, Sentencia N° 466 TJ/J, fallo del 21/08/2023.

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *Vicisitudes de la carga de la prueba en la acción de hábeas data*, por Guillermo F. Peyrano, ED, 218-961; *Prueba informática, intimidad y divorcio*, por Lorenzo A. Sojo, ED, 233-997; *Prueba anticipada en materia informática*, por Gustavo Juan Vaninetti y Hugo Alfredo Vaninetti, ED, 239-711; *Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico*, por Marcelo O. Vuotto, ED, 261-860; *Responsabilidad civil de los buscadores. Reflexiones acerca de la sentencia de la Corte Suprema*, por Hugo A. Vaninetti y Gustavo J. Vaninetti, ED, 260-806; *La responsabilidad de los proveedores de servicios de Internet*, por Gustavo Daniel Tanus, ED, 192-900; *Consideración procesal de los medios de prueba tecnológicos*, por Luis R. Carranza Torres, ED, 248-177; *La videograbación de las audiencias y su máximo rendimiento para una valoración fundada de la prueba*, por Amalia Fernández Balbis, ED, 253-729; *Cuestiones probatorias del correo electrónico*, por Pablo A. Palazzi y Lucas F. Tamagno, ED, 255-78; *Correo electrónico e Internet. Consecuencias jurídicas de su uso en el ámbito laboral*, por Marco A. Rufino, ED, 255-92; *Correo electrónico con firma digital. Aspectos técnicos y jurídicos*, por Luciano A. Ballarini, ED, 257-787; *El derecho procesal civil uruguayo y las nuevas tecnologías. La prueba electrónica y digital en el Uruguay, con énfasis en el documento electrónico y el correo electrónico*, por Daniel Bermúdez Martínez, ED, 273-815; *Reflexiones sobre la valoración de la prueba informática*, por José María Torres Traba, ED, 292-731; *Automatización, virtualidad y eficacia, estandartes de las transformaciones procesales en el expediente digital de la Justicia bonaerense. Nuevo Reglamento de Presentaciones y Notificaciones Electrónicas –Acuerdo n° 4013/2021 SCBA– (T.O. Acuerdo n° 4039/2021)*, por Paulo Alberto Maresca, ED, 295-897; *Abogacía digital. De la toga al metaverso*, por Matilde Pérez, El Derecho - Diario, El abogado y el futuro, Cita Digital: ED-MMMCDVI-607; *II Jornadas Universitarias de Abogacía Digital: Hacia la comprensión jurídica de los desafíos tecnológicos. Comentarios de una jornada inolvidable*, por Matilde Pérez, Derecho, Innovación & Desarrollo Sustentable, Número 10 - Diciembre 2022. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) El presente artículo se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor doctor Jorge Nicolás Lafferriere, concretamente en el Programa IUS titulado: "El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable", que dirigen los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Dra. Susana Eloísa Mender Bini es abogada (UNSTA); Doctora en Ciencias Jurídicas por la Facultad de Derecho de la Universidad Católica Argentina; Master en Propiedad Intelectual e E-law (UCC, Irlanda), especialista en Sistemas Biométricos y Privacidad (FernUni Schweiz, Suiza), miembro del Grupo Argentino de Bioestadística y de la International Biometric Society, estudiante de Ing. en IA (UP).

(***) Tomás Illuminati Balbín es experto en Investigación en Cibercrimen y Ciberseguridad (Universidad Siglo XXI), Ethical Hacker, autor de las obras "Una introducción a la ciberseguridad" y "Ciberconflictos: Sin Fronteras"; en capacitción para los certificados OSCP (OffSec Certified Proffesional) y OSWP (OffSec Wireless Proffesional) estudiante de la Lic. en Ciberseguridad (UFASTA) y de la Lic. en Relaciones Internacionales (UAI).

nacionales susceptibles de ser empleados para una optimo resultado.

II. Funcionamiento de DoS y DDoS

Los ataques denominados denegación de servicio distribuido o Distributed Denial of Service (DDoS)[2] tienen como objetivo la paralización de un servicio determinado. Para lograr un entendimiento cabal de este tipo de ataque, corresponde lograr comprender en primer término lo que es un ataque "denegación de servicio" o Denial of Service (DoS). Esta última modalidad de ataque no solo busca interrumpir el funcionamiento normal de un servicio, sitio web o red, sobrecargando los recursos del sistema objetivo, sino que también tiene como objetivo incapacitar al mismo de responder a las solicitudes legítimas[3].

Dentro de este contexto, es menester conocer el concepto del modelo cliente-servidor, en el cual los clientes solicitan servicios o recursos y los servidores los proporcionan. En el citado modelo, y como su nombre lo indica, se distinguen dos partes: los clientes y los servidores[4].

Los clientes son dispositivos o programas que solicitan servicios o recursos a los servidores, que son dispositivos o programas que proporcionan dichos servicios o recursos. En nuestro día a día, los clientes son nuestros dispositivos informáticos cotidianos, en tanto los servidores –aunque los imaginamos como grandes cajas complejas– son dispositivos similares a nuestros computadores o PC, con la diferencia que estos se encuentran programados para procesar las solicitudes de los clientes y manejar un mayor volumen de peticiones.

(Conexión CLIENTE-SERVIDOR)

La problemática para los servidores radica en que, en la mayoría de las veces, manejan grandes volúmenes de peticiones ingresantes, para las cuales, si un servidor no posee suficiente CPU, memoria y ancho de banda, estas pueden causar que se paralice a raíz de la falta de recursos. Estas condiciones conforman la base o plataforma que permite la concreción de ataques DoS.

Estos ataques emplean diversos mecanismos para sobrecargar un servidor. Dentro de los más frecuentes se pueden encontrar: el envío de datos malformados, comandos específicos, el envío de muchas solicitudes simultáneamente, el envío de una gran cantidad de tráfico al servidor objetivo, entre otras. El objetivo principal es bloquear o ralentizar significativamente el sistema, abrumar al servidor para evitar que funcione correctamente, saturar su capacidad de ancho de banda. Todo ello resulta en la paralización y temporal inhabilitación del servidor[5].

Dicho ataque puede implicar que una empresa pierda ingresos debido a la inactividad del servicio y, correlativamente, que los usuarios no puedan acceder al mismo, provocando en estos últimos frustración y pérdida de confianza[6].

Los ataques DoS presentan una gran variedad de modalidades de los que, dependiendo el tipo de solicitud y conexiones que se envíen, se pueden encontrar[7]:

- HTTP POST Flood: es un de DoS que emplea gran cantidad de solicitudes POST[8], los que saturan el servidor, agotando de esta manera sus recursos y potencialmente provocando su caída.

- HTTP GET Flood: este tipo de ataque tiene por objetivo enviar una gran cantidad de solicitudes GET[9] para abrumar los recursos del servidor, impidiendo que responda a solicitudes legítimas.

- HTTPS[10] POST[11] Flood: Similar al HTTP POST Flood, empleando conexiones SSL[12][13], lo que requiere la desencriptación de las solicitudes para inspeccionarlas.

- HTTPS GET[14] Flood: Similar al HTTP GET Flood, utilizando conexiones SSL, lo que requiere la desencriptación de las solicitudes para mitigarlas.

- SYN[15] Flood (TCP/SYN): Establece conexiones medio abiertas enviando paquetes SYN[16] sin completar el protocolo de enlace de tres vías, lo que agota los recursos del servidor.

- UDP[17] Flood: Utiliza el protocolo sin conexión UDP[18] para enviar grandes volúmenes de tráfico, saturando el ancho de banda de la red objetivo.

- ICMP[19] Flood: Utiliza mensajes ICMP para sobrecargar el ancho de banda de la red objetivo, afectando la disponibilidad del servicio[20].

- MAC[21] Flood: Envía múltiples tramas Ethernet falsas con diferentes direcciones MAC, agotando los recursos de los switches de red y causando posibles interrupciones[22].

No obstante, y atento a que los servidores se complejizaron, resultando cada vez más potentes para soportar las inmensas cargas de peticiones que realizan los usuarios normales, ha dificultado que un atacante realice un ataque de denegación de servicio con el mero envío de peticiones. A raíz de ello, surgen los ataques de tipo DDoS, los que parten de la misma base que el tipo DoS; con la diferencia de que, en vez de realizarse desde un solo dispositivo, utiliza como herramienta los **botnet**[23].

(2) NIST, NISTIR 7711, Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters, Appendix C, https://doi.org/10.6028/NIST.IR.7711 [fecha de acceso: 22/07/2024].

(3) Fortinet. "DoS vs DDoS", https://www.fortinet.com/lat/resources/cyberglossary/dos-vs-ddos [fecha de acceso 14/07/2024].

(4) MITRE ATT&CK, "Network Denial of Service", https://attack.mitre.org/techniques/T1498/ [fecha de acceso: 22/07/24].

(5) Siegel, Michael; Sciore, Edward; Madnick, Stuart; "Context Interchange in a Client-Server Architecture", MIT, http://web.mit.edu/smadnick/www/wp2-old%20names/CISL%2393-07.pdf [fecha de acceso: 14/07/24].

(6) INCIBE; "¿Qué son los ataques DoS y DDoS?", https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos [fecha de acceso 14/07/2024].

(7) CISA; "DDoS Quick Guide", https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf [fecha de acceso: 14/07/2024].

(8) Firth, Jack; "Requests", https://plt.cs.northwestern.edu/release-pkg-build/doc/request/index.html [fecha de acceso: 14/07/24].

(9) Firth, Jack; "Requests", https://plt.cs.northwestern.edu/release-pkg-build/doc/request/index.html [fecha de acceso: 14/07/24].

(10) HTTPS (Hypertext Transfer Protocol Secure): Es una versión segura del protocolo HTTP, que cifra la comunicación entre el navegador web y el servidor para proteger la confidencialidad e integridad de los datos.

(11) Es un método del protocolo HTTP utilizado para enviar datos al servidor para que los procese. A diferencia de GET, POST no tiene restricciones de tamaño y los datos se envían en el cuerpo de la solicitud, lo que lo hace adecuado para enviar información sensible o extensa.

(12) Oppliger, Rolf; *SSL and TLS: Theory and Practice*, Artech House, 2023, pág. 23.

(13) SSL (Secure Sockets Layer) es un protocolo de seguridad que cifra la información transmitida entre un servidor web y un navegador, protegiendo datos sensibles como contraseñas y números de tarjetas de crédito. SSL asegura que la comunicación se mantenga privada y protegida contra interceptaciones y manipulaciones.

(14) Es un método del protocolo HTTP que solicita datos del servidor. Los datos se envían en la URL de la solicitud y están sujetos a limitaciones de tamaño. GET es utilizado comúnmente para obtener información sin modificar el estado del servidor.

(15) Durante el proceso de establecimiento de una conexión TCP, después de que el cliente envía un segmento SYN al servidor, el servidor responde con un segmento SYN-ACK. Este segmento indica que el servidor ha recibido el SYN del cliente y acepta la solicitud de conexión. El SYN-ACK también incluye un número de secuencia inicial del servidor, y el cliente debe responder con un ACK para confirmar la recepción del SYN-ACK y completar el proceso de conexión.

(16) Yang, Guang; "Introduction to TCP/IP network attacks". *Secure Systems Lab* (1997), http://seclab.cs.sunysb.edu/sekar/papers/netattacks.pdf [fecha de acceso: 14/07/24].

(17) UDP (User Datagram Protocol): Es un protocolo de comunicación sin conexión que envía datagramas sin establecer una conexión previa ni garantizar la entrega. Es más rápido que TCP, pero no asegura que los datos lleguen en el orden correcto o siquiera lleguen a su destino.

(18) Oppliger, Rolf; *SSL and TLS: Theory and Practice*, Artech House, 2023, pág. 14.

(19) ICMP (Internet Control Message Protocol): Es un protocolo de la capa de red que se utiliza para enviar mensajes de control y error entre dispositivos de red. Por ejemplo, ICMP se usa para informar errores en la transmisión de datos y para verificar la conectividad de red a través de herramientas como ping.

(20) Rosen, Rami; "Internet control message protocol (ICMP)", *Linux Kernel Networking: Implementation and Theory*, 2014, págs. 37-61.

(21) MAC (Media Access Control): Es una subcapa de la capa de enlace de datos en el modelo OSI que se encarga de la dirección física de los dispositivos en una red local. Utiliza direcciones MAC únicas para identificar y controlar el acceso de los dispositivos a la red.

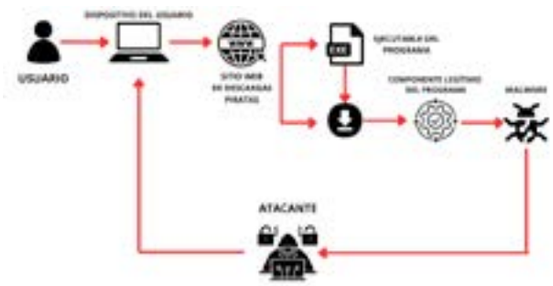
(22) Martin, Jeremy; Rye, Erik; Beverly, Robert; "Decomposition of MAC address structure for granular device inference", en *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pp. 78-88. 2016.

(23) Meisam Eslahi, Rosli Salleh, Nor Badrul Anuar; "Bots and Botnets: An Overview of Characteristics, Detection and Challenges", IEEE International Conference on Control System, Computing and Engineering, 23 - 25 Nov. 2012, Penang, Malaysia.

Un botnet es un conjunto de dispositivos conectados a Internet que han sido comprometidos por un actor malicioso, conocido como botmaster, y controlados externamente para llevar a cabo diversas actividades ilícitas, como el envío de spam o la realización de ataques de Denegación de Servicio (DDoS). Los dispositivos comprometidos que forman parte de una botnet se conocen como bots o "zombies", un término coloquial para describir ordenadores infectados por un malware diseñado para infectar múltiples dispositivos y controlarlos de manera remota. Este malware, una combinación de las palabras "malicious" (malicioso) y "software", puede introducirse en un dispositivo objetivo a través de diversas técnicas, como correos electrónicos de phishing, descargas de software infectado, vulnerabilidades de software sin parchear, o incluso dispositivos USB infectados.

Una vez que el malware infecta un dispositivo, establece una conexión con un servidor externo conocido como el servidor de control y comando (C&C) del atacante. Este servidor actúa como el centro de mando desde el cual se envían instrucciones a los dispositivos infectados, permitiendo al atacante controlar simultáneamente lo que hacen los dispositivos infectados. Con cada dispositivo infectado, el malware forma una red de bots controlados remotamente, que pueden incluir computadoras personales, servidores, enrutadores, y dispositivos IoT[24] (Internet de las cosas)[25].

Aunque el malware de botnet puede recopilar información sensible del dispositivo infectado, como credenciales de inicio de sesión, datos personales, e información financiera; su objetivo principal es mantener el control sobre estos dispositivos el mayor tiempo posible. A menudo, el malware se actualiza para evadir la detección de antivirus y mejorar sus capacidades de ataque. En algunos casos, puede propagarse automáticamente a otros dispositivos dentro de la misma red local o a través de Internet, mediante métodos automatizados como el escaneo de puertos y la explotación de vulnerabilidades conocidas[26].



(Ejemplo de descarga de malware disfrazado de software legítimo desde un sitio web no confiable)

Cuando el malware establece una conexión con el servidor C&C, el dispositivo afectado permanece inactivo esperando instrucciones del atacante. Una vez elegido el objetivo, el agresor ejecuta un ataque coordinado utilizando todos los bots disponibles. El tipo más común de ataque implica inundar el objetivo con una gran cantidad de tráfico, sobrecargando el sistema y dejándolo incapaz de manejar adecuadamente las solicitudes legítimas de los usuarios, resultando de esta manera en una interrupción del servicio.

Gracias a la proliferación del Internet de las Cosas (IoT), los creadores de botnets aprovechan estos dispositivos para propagar bots y realizar ataques, complicando aún más la detección y mitigación debido a la diversidad de redes, protocolos y dispositivos[27].

(24) Se refiere a la red de dispositivos físicos, objetos y sensores conectados a Internet que recopilan, intercambian y procesan datos. Estos dispositivos pueden incluir desde electrodomésticos y vehículos hasta sistemas de seguridad y equipos industriales. IoT permite la automatización y control remoto de estos dispositivos, facilitando la toma de decisiones basada en datos en tiempo real y mejorando la eficiencia en diversas aplicaciones, como el hogar inteligente, la gestión de ciudades y la industria 4.0.

(25) Meisam Eslahi, Rosli Salleh, Nor Badrul Anuar; "Bots and Botnets: An Overview of Characteristics, Detection and Challenges", IEEE International Conference on Control System, Computing and Engineering, 23 - 25 Nov. 2012, Penang, Malaysia.

(26) Zeidanloo, Hossein Rouhani, Mohammad Jorjor Zadeh Shooshtari, Payam Vahdani Amoli, M. Safari, and Mazdak Zamani; "A taxonomy of botnet detection techniques", *3rd International Conference on Computer Science and Information Technology*, IEEE, 2010, Vol. 2, pp. 158-162.

(27) Woodiss-Field, A., Johnstone, M.N., y Haskell-Dowland, P.; "Examination of Traditional Botnet Detection on IoT-Based Bots". *Sensors* 24, no. 3 (2024): 1027, https://doi.org/10.3390/s24031027 [fecha de acceso: 14/07/2024].

Los ataques DDoS no solo representan una amenaza técnica, sino también económica para las organizaciones afectadas y de gran envergadura.

Cuando un servicio es interrumpido debido a un ataque DDoS, las pérdidas económicas pueden ser múltiples y variadas. En primer lugar, las empresas pueden enfrentar una disminución inmediata en sus ingresos, en el caso que el servicio afectado sea vital para su operación diaria o para la generación de ingresos directos, como plataformas de comercio electrónico, servicios financieros en línea, o proveedores de servicios en la nube.

En segundo lugar, además de la pérdida de ingresos, los costos asociados con la mitigación y la recuperación después de un ataque DDoS pueden ser significativos. Las empresas suelen tener que invertir en soluciones de seguridad adicionales, servicios de mitigación de DDoS, y a menudo, en consultoría especializada para restaurar la operatividad normal y reforzar las defensas contra futuros ataques. Estos gastos no planificados pueden desviar recursos financieros y humanos que podrían haberse utilizado para el crecimiento y la innovación en otros aspectos del negocio.

Estos ataques requieren muy poca habilidad para ejecutarse. Los ciberdelincuentes pueden lanzar ataques DDoS con facilidad, por cuanto alquilan botnets preconfiguradas de otros hackers, lo que les permite actuar con mínima preparación y planificación[28].

Es decir, que estos resultan:

Difíciles de detectar: Las botnets están compuestas principalmente por dispositivos de uso comercial y doméstico, lo que dificulta a las organizaciones distinguir el tráfico malicioso del tráfico legítimo. Además, los síntomas de un ataque DDoS, como la ralentización del servicio o la inaccesibilidad temporal de sitios y aplicaciones; también pueden deberse a aumentos repentinos de tráfico legítimo, complicando la identificación temprana de estos ataques.

Difíciles de mitigar: Una vez identificado un ataque DDoS, su naturaleza distribuida impide que las organizaciones lo bloqueen cerrando una sola fuente de tráfico. Los controles de seguridad de red convencionales, como la limitación de velocidad, también pueden afectar negativamente a los usuarios legítimos, ralentizando sus operaciones.

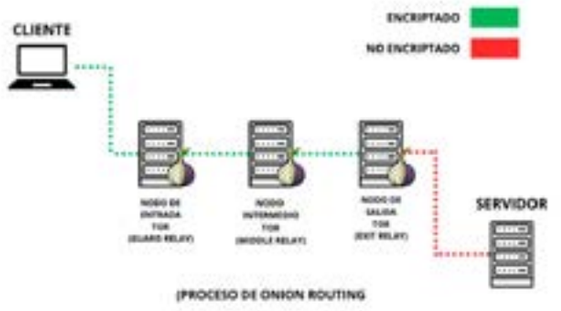
Mayor número –que nunca– de dispositivos potenciales para botnets: El auge del Internet de las Cosas (IoT) ha proporcionado a los hackers una abundante fuente de dispositivos que pueden convertirse en bots. Los aparatos y sistemas conectados a Internet, incluidos dispositivos médicos y sistemas de manufactura, suelen venderse y usarse con configuraciones predeterminadas universales y controles de seguridad débiles o inexistentes, lo que los hace especialmente vulnerables a malware. Los propietarios de estos dispositivos a menudo no notan que están comprometidos, ya que suelen utilizarlos de manera pasiva o poco frecuente.

III. Onion Routing y Sistemas de Anonimato: I2P, Freenet y Tor

En el vasto mundo de la privacidad en línea y el anonimato, el concepto de Onion Routing, o enrutamiento cebolla, se erige como una tecnología fundamental. Este método fue desarrollado para asegurar que las comunicaciones a través de Internet sean privadas y anónimas, utilizando un sistema de capas de cifrado que se asemeja a las capas de una cebolla. A medida que los datos atraviesan cada nodo en la red, una capa de cifrado es removida, revelando el próximo destino en la ruta. Este proceso garantiza que ningún nodo individual conozca tanto el origen como el destino completo de los datos, proporcionando un alto grado de anonimato y seguridad.

(28) IBM. "¿Qué es un ataque DDoS?". https://www.ibm.com/es-es/topics/ddos [fecha de acceso 14/07/2024].

Uno de los sistemas más prominentes que utiliza Onion Routing es Tor, conocido formalmente como The Onion Router. Tor fue concebido en la década de 1990 por el Laboratorio de Investigación Naval de los Estados Unidos con el objetivo de proteger las comunicaciones gubernamentales. Sin embargo, su evolución lo llevó a convertirse en una herramienta crucial para la privacidad en línea disponible para el público en general. Tor opera redirigiendo el tráfico de Internet a través de una serie de nodos de relé, que son operados por voluntarios en todo el mundo. Cada nodo de relé en la red Tor conoce únicamente el nodo anterior y el siguiente en la ruta, lo que dificulta significativamente el rastreo del origen y el destino del tráfico de datos[29].



(PROCESO DE ONION ROUTING

La arquitectura de Tor es compleja y eficaz en su propósito. Al inicio del proceso, un nodo de entrada recibe los datos del usuario y aplica la primera capa de cifrado. Luego, un nodo intermedio recibe los datos cifrados del nodo de entrada, aplica otra capa de cifrado y los reenvía. Finalmente, un nodo de salida remueve la última capa de cifrado y envía los datos al destino final. Este enrutamiento en múltiples capas asegura que la privacidad del usuario esté protegida en todo momento. Tor se ha utilizado ampliamente en situaciones donde la privacidad y el acceso a la información sin censura son vitales, como en el caso de periodistas y activistas en regímenes autoritarios. No obstante, a pesar de sus beneficios, Tor también tiene sus desventajas. Una de las principales es la velocidad reducida debido a la necesidad de redirigir los datos a través de múltiples nodos, lo que puede hacer que actividades como la transmisión de video en tiempo real sean difíciles de realizar. Además, la red Tor ha sido asociada con actividades ilegales, ya que el anonimato que proporciona puede ser explotado por criminales para llevar a cabo transacciones en la dark web[30].

Por otro lado, el Proyecto Internet Invisible, conocido como I2P, es otra red anónima diseñada para mejorar la privacidad en línea. A diferencia de Tor, que se centra en el acceso anónimo a la web abierta, I2P está diseñada principalmente para aplicaciones dentro de su propia red. I2P utiliza túneles de entrada y salida para enmascarar la ruta de los datos, y emplea mensajes Garlic, una forma avanzada de cifrado en capas que permite agrupar múltiples mensajes en uno solo. Esto no solo aumenta la eficiencia, sino también el anonimato del usuario. I2P es particularmente útil para servicios internos como blogs, correos electrónicos y aplicaciones de mensajería, ofreciendo una privacidad robusta dentro de la red. Sin embargo, I2P es menos conocido y utilizado en comparación con Tor, y no es tan efectivo para el acceso a la web abierta[31].

Freenet es otra plataforma significativa en el ámbito de la navegación anónima y la publicación de contenidos sin censura. Freenet se enfoca en la resistencia a la censura y la descentralización completa, donde los usuarios contribuyen con espacio en disco y ancho de banda para la red. Los datos en Freenet son fragmentados y distribuidos a través de nodos, asegurando que ningún nodo tenga la información completa, lo que dificulta aún más el rastreo y la censura. Freenet opera en dos modos: Darknet, que permite conexiones solo con amigos de confianza, y Opennet, que permite conexiones con cualquier usuario. Esta dualidad ofrece flexibilidad en términos de seguridad y anonimato. Sin embargo, Freenet puede ser lento debido a su arquitectura de almacenamiento distribuido y es más complejo y técnico de usar en comparación con Tor e I2P[32].

Como conclusión, tanto Tor, I2P y Freenet como los proxies y las VPN son herramientas diseñadas para mejorar la privacidad y la seguridad en línea, cada una con sus propias características y aplicaciones específicas. Tor ofrece el más alto nivel de anonimato y es ideal para entornos donde la privacidad y el acceso a información sin censura son vitales. I2P proporciona una robusta privacidad dentro de su propia red, siendo adecuado para aplicaciones internas. Freenet se destaca por su resistencia a la censura y su descentralización completa, aunque puede ser más lento y técnico de usar. Los proxies y las VPN, por otro lado, ofrecen soluciones útiles para mejorar la privacidad y el acceso a contenidos restringidos, pero no proporcionan el mismo nivel de anonimato que Tor. La elección de la herramienta adecuada depende de las necesidades específicas del usuario en términos de privacidad, seguridad y accesibilidad.

IV. Proxies y VPN: Herramientas de privacidad

Los proxies y las VPN (Redes Privadas Virtuales) son dos herramientas fundamentales en el ámbito de la privacidad en línea y la seguridad de la información. Aunque ambos comparten el objetivo de proteger la identidad del usuario y asegurar las comunicaciones en Internet, difieren en sus enfoques, capacidades y niveles de protección[33].

Un proxy, o servidor proxy, actúa como un intermediario entre el usuario y los servidores a los que desea acceder. Cuando un usuario envía una solicitud a través de un proxy, esta primera llega al servidor proxy, que luego la reenvía al servidor final. La respuesta del servidor pasa de vuelta al proxy, que la envía finalmente al usuario. Esta cadena de intermediación permite que la dirección IP del usuario quede oculta, ya que los servidores finales solo ven la dirección IP del proxy[34]:

- Acceso a Contenidos Restringidos: Los proxies son comúnmente utilizados para eludir restricciones geográficas y acceder a contenidos bloqueados en ciertas regiones. Esto es particularmente útil para usuarios que desean acceder a servicios de streaming, sitios web o aplicaciones que están limitados a determinadas ubicaciones geográficas.

- Mejora del Rendimiento de la Red: En algunos casos, los proxies pueden almacenar en caché contenidos web frecuentes, lo que reduce el tiempo de carga y mejora el rendimiento de la red. Este tipo de proxy, conocido como proxy caché, es ampliamente utilizado en redes empresariales para optimizar el tráfico y reducir el ancho de banda.

- Control y Supervisión del Uso de Internet: Los proxies también se utilizan en entornos corporativos y educativos para controlar y supervisar el uso de Internet. Administradores de red pueden configurar proxies para filtrar contenidos inapropiados, bloquear sitios web no autorizados y monitorear la actividad en línea de los usuarios

Aunque los proxies pueden ocultar la dirección IP del usuario, no cifran el tráfico de datos entre el usuario y el servidor proxy. Esto significa que la información puede ser interceptada por terceros en el camino, comprometiendo la seguridad y la privacidad. Además, los proxies no protegen contra la vigilancia avanzada o los ataques dirigidos que puedan rastrear el tráfico hasta su origen. Los proxies también pueden ser bloqueados por algunos sitios web y servicios que identifican y restringen el acceso de servidores proxy conocidos.

(29) Dingledine, Roger; Mathewson, Nick; Syverson, Paul; "Tor: The Second-Generation Onion Router", https://apps.dtic.mil/sti/pdfs/ADA465464.pdf [fecha de acceso: 14/07/24].

(30) Sánchez-Rola, Iskander; Balzarotti, Davide; Santos, Igor; "The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services", WWW '17: Proceedings of the 26th International Conference on World Wide Web, https://www.eurecom.fr/en/publication/5152/download/sec-publi-5152.pdf [fecha de acceso: 14/07/24].

(31) Invisible Internet Project (I2P), https://geti2p.net/_static/pdf/i2p_philosophy.pdf [fecha de acceso: 15/07/24].

(32) Clarke, Ian; Sandberg, Oskar; Wiley, Brandon; Hon, Theodore W.; "Freenet: A Distributed Anonymous Information Storage and Retrieval System", https://www.cs.cornell.edu/people/egs/615/freenet.pdf [fecha de acceso: 15/07/24].

(33) Pavlicek, Antonin; Sudzina, Frantisek; "Internet Security and Privacy in VPN", Journal of Networking Technology, Volume 9, Number 4, December 2018, pp. 133-139, https://www.dline.info/jnt/fulltext/v9n4/jntv9n4_1.pdf [fecha de acceso: 15/07/24].

(34) David Dwiputra Kurniadi; "The Difference Between Using Proxy Server and VPN", Sisforma, vol. 2, no. 1, May 2015, pp. 19-22, https://www.researchgate.net/publication/317809198_The_Difference_Between_Using_Proxy_Server_and_VPN [fecha de acceso: 15/07/24].

Por otro lado una VPN, o Red Privada Virtual, va más allá de las capacidades de un proxy al establecer una conexión cifrada entre el dispositivo del usuario y un servidor VPN. Esta conexión segura y privada asegura que todos los datos transmitidos entre el usuario y el servidor VPN estén protegidos contra la interceptación y el espionaje.

El funcionamiento de una VPN implica el uso de protocolos de cifrado avanzados para crear un "túnel" seguro a través del cual los datos viajan desde el dispositivo del usuario hasta el servidor VPN. Este túnel cifra toda la información, haciendo que sea prácticamente imposible para los terceros interceptar o descifrar los datos. El servidor VPN luego reenvía el tráfico a su destino final, y la respuesta regresa al servidor VPN antes de ser enviada de vuelta al usuario[35].

- Privacidad y Seguridad: Las VPN enmascaran la dirección IP del usuario y cifran todo el tráfico de datos, lo que protege la información contra hackers, ISP curiosos y cualquier entidad que intenta espiar la actividad en línea del usuario. Esto es especialmente crucial cuando se utiliza una red Wi-Fi pública, donde las conexiones no seguras son comunes.

- Elusión de Restricciones Geográficas y Censura: Al igual que los proxies, las VPN permiten a los usuarios acceder a contenidos restringidos geográficamente al hacer que parezca que la conexión se origina desde una ubicación permitida. Esto es vital para usuarios en países con estricta censura en Internet, permitiéndoles acceder a información y servicios bloqueados.

- Acceso Seguro a Recursos Internos: Las VPN son ampliamente utilizadas en entornos corporativos para permitir a los empleados acceder de forma segura a los recursos internos de la empresa desde ubicaciones remotas. Esto es fundamental para mantener la seguridad de los datos sensibles de la empresa y garantizar la continuidad del negocio.

- Evasión de Limitaciones de ISP: Algunos proveedores de servicios de Internet (ISP) pueden limitar el ancho de banda para ciertas actividades en línea, como la transmisión de video o el juego en línea. Una VPN puede ayudar a evadir estas limitaciones, mejorando la velocidad y la calidad de la conexión.

V. Principios de la pericia informática forense

La identificación y recolección de evidencia digital es una etapa crucial debido a la naturaleza delicada de los datos recolectados. Es esencial que el investigador posea las habilidades y conocimientos necesarios para asegurar la integridad de la evidencia digital durante todo su ciclo de vida. En este contexto, el perito informático forense desempeña un papel fundamental, ya que debe prever diversos aspectos como la escena del delito, las metodologías a utilizar y el equipo necesario para cumplir con los requerimientos establecidos.

Uno de los temas principales a tratar, y que puede socavar todo el peritaje realizado, es la cadena de custodia. Esta se refiere a la preservación de un elemento de prueba, tanto en el medio físico como en el entorno digital. Es crucial entender que, al trabajar con información almacenada, la correcta gestión de la misma es fundamental, ya sea en presencia o ausencia de energía. Un ejemplo de esto es el uso de imágenes forenses para preservar la información, lo cual permite disponer de los ejemplares originales y sus respectivos duplicados para futuros análisis por parte de investigadores forenses en diferentes instancias. Esto posibilita la revisión posterior de los resultados obtenidos mediante la replicación de los procesos realizados[36].

Dada la naturaleza dinámica de los discos en entornos de ejecución de los sistemas, las imágenes de los mismos se suelen obtener una vez consumado el hecho delictivo. Es importante destacar que no toda adquisición de imagen forense es igual; existen varias modalidades, por ejemplo:

1. Copia bit a bit: Replica de manera exacta los bits de un volumen lógico o de una unidad física. Esta forma de duplicado forense se realiza cuando la copia se efectúa en otro disco.

2. Imagen forense: Se realiza en uno o varios archivos y también es parte del duplicado forense.

3. Imagen forense sin formato: No contiene metadatos y no está comprimida.

Es de vital importancia que, para la consideración posterior de la prueba entregada, se cumplan tres requisitos fundamentales:

1. Uso de herramientas forenses adecuadas: Esto es necesario para garantizar que los cambios en el dispositivo de origen sean lo menos invasivos posible y para asegurar su integridad.

2. No realizar modificaciones: El proceso debe ser de preservación. Cualquier escritura genera una modificación que afectaría el cálculo del hash, anulando la validez de la prueba por adulteración.

3. Mantener y comprobar la integridad del dispositivo: Para esto, se debe calcular el hash criptográfico.

¿Qué es el hash criptográfico?

Es el proceso de tomar una cantidad determinada de datos y aplicar un algoritmo matemático complejo para generar un identificador numérico único, minimizando la posibilidad de colisiones de hash. Las características de un hash criptográfico son fundamentales para su uso en seguridad informática y en la preservación de la integridad de los datos. A continuación, se describen las principales características de un hash[37]:

Determinismo: Un hash criptográfico debe ser determinista, lo que significa que el mismo mensaje de entrada siempre producirá el mismo valor de hash.

Rapidez de cálculo: El algoritmo de hash debe ser eficiente en términos de tiempo de cómputo, permitiendo generar el valor de hash rápidamente, independientemente del tamaño del mensaje de entrada.

Resistencia a colisiones: Debe ser computacionalmente inviable encontrar dos mensajes diferentes, es decir si m1 y m2 existen, hash(m1) y hash(m2) deben ser siempre distintos.

Salida de longitud fija: Independientemente del tamaño del mensaje de entrada, el valor de hash producido por un algoritmo de hash criptográfico debe tener una longitud fija (por ejemplo, 256 bits para SHA-256).

Irreversibilidad: Es computacionalmente inviable reconstruir el mensaje original a partir de su valor de hash.

La adquisición de evidencias en dispositivos móviles es una práctica crucial en la investigación forense. Los métodos empleados varían en complejidad y efectividad, determinando la accesibilidad a datos almacenados, incluidos aquellos eliminados. Existen dos tipos principales de evidencias: lógica y física, cada una con sus ventajas y desventajas.

La adquisición lógica implica copiar los datos almacenados en la memoria del dispositivo y sincronizarlos con una estación de trabajo mediante los mecanismos proporcionados por el fabricante. Esta conexión puede ser física (USB) o inalámbrica (WiFi), y aunque es un proceso sencillo, la cantidad de información recuperada es limitada.

La adquisición física es preferida por los analistas forenses debido a su capacidad para crear una imagen forense idéntica del dispositivo original, preservando todas las evidencias almacenadas, incluidas las eliminadas. Sin embargo, este método es complejo y requiere más tiempo.

Métodos avanzados de adquisición

Chip-off: El método de chip-off implica la extracción física de la memoria flash del dispositivo móvil. Esta técnica permite a los examinadores forenses obtener una imagen binaria directa del chip removido. Aunque proporciona una adquisición completa, requiere una amplia capacitación debido a la diversidad de chips y el riesgo de daño físico durante el proceso[38].

(35) Jyothi, K; Reddy, B. Indira; "Study on Virtual Private Network (VPN), VPN's Protocols And Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology; Volume 3, Issue 5, pp. 919-932, https://www.researchgate.net/publication/368831275_CSEIT1835225_Study_on_Virtual_Private_Network_VPN_VPN's_Protocols_And_Security [fecha de acceso: 15/07/24].

(36) Pourvahab, Mehran; Ekbatanifard, Gholamhossein; "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology", https://www.researchgate.net/publication/336446265_Digital_Forensics_Architecture_for_Evidence_Collection_and_Provenance_Preservation_in_IaaS_Cloud_Environment_Using_SDN_and_Blockchain_Technology [fecha de acceso: 15/07/24].

(37) Macharia, Kelvin W.; "Cryptographic Hash Functions", https://www.researchgate.net/publication/254035333_A_complete_study_on_tools_techniques_for_digital_forensic_analysis [fecha de acceso: 15/07/24].

(38) Fukami, Aya; Ghose, Saugata; Luo, Yixin; Cai, Yu; Mutlu, Onur; "Improving the reliability of chip-off forensic analysis of NAND flash memory devices", Digital Investigation 20, 2017, S1-S11,

JTAG: El estándar JTAG (Joint Test Action Group) define una interfaz de prueba común para procesadores y memorias. A través de esta interfaz, los examinadores pueden comunicarse con componentes compatibles utilizando dispositivos programadores especiales. Este método permite obtener imágenes forenses de dispositivos bloqueados o dañados, aunque es invasivo y requiere desmontar parte del dispositivo móvil[39].

Impacto de la computación en la nube en el análisis forense digital[40]

La computación en la nube representa un avance significativo en la evolución de Internet, aunque este paradigma está en desarrollo y plantea muchas incógnitas, especialmente en el campo de la seguridad y el análisis forense digital. **También es un rasgo característico de las nuevas habilidades que exige la Revolución Industrial 4.0 que estamos transitando.**

La computación en la nube permite a los usuarios acceder a recursos informáticos compartidos a través de Internet, en lugar de poseerlos localmente. Este modelo ofrece flexibilidad y escalabilidad, ya que los recursos pueden expandirse o contraerse según la demanda. Los servicios en la nube son administrados por proveedores que ofrecen recursos a múltiples usuarios simultáneamente, lo que transforma el entorno informático tradicional en una infraestructura de computación virtual.

La seguridad en la computación en la nube es una preocupación crítica que ha recibido atención limitada. Además, el análisis forense digital en la nube presenta desafíos únicos, dado que la estructura virtual y distribuida de los recursos dificulta la aplicación de técnicas forenses tradicionales. En un examen forense tradicional, los archivos se examinan junto con la estructura del sistema de archivos, pero en la nube, los recursos son virtuales y pueden estar distribuidos geográficamente.

Desafíos de la forensia en la nube

- Protección de la evidencia: Asegurar la integridad de la evidencia digital es crucial para evitar la contaminación durante el proceso de adquisición y análisis.

- Problemas legales: La distribución geográfica de los recursos en la nube puede generar conflictos legales, ya que los datos pueden residir en múltiples jurisdicciones con diferentes regulaciones.

- Seguridad integral: Es necesario implementar servicios de seguridad integrales que protejan tanto los recursos de la nube como los datos que residen en ellos.

En la computación tradicional, los usuarios tienen control total sobre el almacenamiento de datos y los recursos informáticos locales. En contraste, la computación en la nube ofrece acceso a recursos distribuidos a través de Internet, administrados por proveedores de servicios en la nube.

Existen diferentes métodos y estándares para la adquisición de datos en la nube, y es responsabilidad del investigador forense discernir entre ellos según los requisitos específicos del caso.

Métodos de adquisición

- Adquisición lógica: Implica la copia de datos accesibles a través de interfaces de usuario y API proporcionadas por el proveedor de la nube. Es un método menos invasivo pero puede no capturar todos los datos necesarios.

- Adquisición física: Aunque más compleja y menos común en la nube, esta técnica implica la creación de una imagen completa de los recursos de almacenamiento.

El impacto de la computación en la nube en el análisis forense digital es significativo y plantea nuevos desafíos y oportunidades. La adaptación a este nuevo paradigma requerirá innovación en herramientas y técnicas, así como una profunda comprensión de los aspectos legales y de seguridad asociados. La colaboración entre investigadores forenses, proveedores de servicios en la nube y reguladores será clave para asegurar la eficacia y la integridad del análisis forense en este entorno emergente.

Modelos de nube

Los modelos de nube se distinguen por sus características de seguridad, control y rentabilidad:

- Modelo de nube pública: Ofrece infraestructura accesible a múltiples usuarios con un enfoque en la rentabilidad. Empresas como Microsoft, Google y Amazon son líderes en este modelo. La independencia de ubicación y la flexibilidad de acceso son características clave, pero la dispersión de datos puede complicar la adquisición forense.

- Modelo de nube privada: Proporciona recursos compartidos bajo el control de una única organización, ofreciendo mayor seguridad y privacidad. Aunque más costoso, permite un mayor control sobre los datos, pero su escalabilidad está limitada a los recursos adquiridos.

- Modelo de nube híbrida: Combina características de nubes públicas y privadas, permitiendo una estrategia comercial equilibrada. Sin embargo, la integración de ambos modelos presenta desafíos en el control de datos y la prevención de fugas hacia la nube pública.

Desafíos en cada modelo

- Nube pública: El acceso a los datos puede ser limitado por las políticas del proveedor, y la seguridad de los datos puede verse comprometida por la naturaleza compartida del entorno.

- Nube privada: Aunque ofrece un mayor control, la complejidad en la configuración y mantenimiento puede ser un desafío para la adquisición forense.

- Nube híbrida: La integración y el control sobre qué datos se mueven entre la nube pública y privada pueden complicar la gestión forense.

Otras implicaciones que se tienen con la informática forense en la nube son que el análisis forense en la nube no solo enfrenta desafíos técnicos, sino también legales significativos. Los investigadores deben estar conscientes de las implicaciones legales que surgen al manejar datos sensibles de terceros durante el análisis forense. Es crucial equilibrar la eficacia de la investigación con la protección de los derechos y la privacidad de los usuarios afectados.

La adquisición de datos sensibles puede implicar la vulneración de la privacidad de terceros, lo que podría tener consecuencias legales y éticas. Por lo tanto, los investigadores deben implementar prácticas rigurosas para proteger estos datos y cumplir con las normativas vigentes. Esto incluye la necesidad de coordinar con organismos judiciales para definir claramente el alcance del análisis forense y asegurar que se respeten los derechos de todos los involucrados.

Finalmente el principio de territorialidad juega un papel crucial en el análisis forense en la nube, ya que el marco normativo puede variar según la ubicación física de los servidores que almacenan los datos. Los investigadores deben tener en cuenta las leyes de la nación donde se encuentran estos servidores para cumplir con los requisitos legales y evitar conflictos jurisdiccionales.

VI. Estandarizando los estudios forenses

A nivel internacional se pueden encontrar diversos protocolos respecto al manejo, procesamiento y formación del informe pericial en cuanto a la prueba digital. Uno de los más recientes es el que fue elaborado por la Interpol en mayo de 2019.

No obstante, no resulta ser el único ni el más aplicado. También encontramos dentro del Organismo Internacional de Estandarización, la normativa ISO/IEC 27037/2017. Además de las recientemente mencionadas, una de las primeras y más empleadas es aquella elaborada por ingenieros del Networking Working Group (NWG) en 2002.

Todas ellas resultan lineamientos útiles de seguir e implementar para un correcto tratamiento de los elementos que conformarán la probanza digital.

VII. La Guía de NWG 3227/2002

A inicios del año 2002, un grupo de ingenieros desarrolló una Guía de Recolección de Evidencia y Archivo para la Networking Working Group[41]. Entre uno de sus apartados más destacables se encuentra el referido a las

---

https://www.cs.cmu.edu/~yixinluo/index_files/chip-off-forensic_dfrws17.pdf [fecha de acceso: 16/07/24].

(39) Rearick, J.; Eklow, B.; Posse, K.; Crouch, Alfred; Bennetts, B.; "IJTAG (internal JTAG): a step toward a DFT standard", Test Conference, Proceedings, ITC 2005, IEEE International, https://www.researchgate.net/publication/4217729_IJTAG_internal_JTAG_a_step_toward_a_DFT_standard [fecha de acceso: 15/07/24].

(40) Ruan, Keyun; Carthy, Joe;Kechadi, Tahar; Crosbie, Mark; "Cloud Forensics", Advances in Digital Forensics VII, 2011, pp. 35-46, https://www.researchgate.net/publication/221352743_Cloud_Forensics [fecha de acceso: 15/07/24].

(41) Brezinski, D.; Killalea, T.; "Guidelines for Evidence Collection and Archiving", NWG, febrero 2002, https://www.rfc-editor.org/rfc/pdfrfc/rfc3227.txt.pdf [fecha de acceso: 22/07/2024].

consideraciones legales, en las que indican las características que deben ostentar la prueba digital para ser presentada en los estrados judiciales.

Entre las primeras se encuentra el carácter de admisibilidad, en relación a qué debe cumplimentar con una serie de reglas legales para su introducción en la causa judicial. Asimismo, debe ser auténtico en cuanto debe vincular la evidencia con el hecho delictivo.

Por otro lado, también debe ser completa y confiable. Ello implica que la prueba debe contemplar la totalidad de los hechos –evitando sesgos o visiones particulares–, como también que la recolección de evidencia y su manejo eviten dudas sobre su autenticidad y veracidad.

Todo ello va de la mano con la credibilidad y comprensión del informe respecto a la evidencia, por cuanto debe ser comprensible tanto para las partes intervinientes como para los magistrados que terminarán resolviendo la causa.

Además del abordaje en materia legal que realiza la guía, también resalta ciertas acciones que se debe evitar hacer para no entorpecer el proceso forense o destruir evidencia –incluso de forma accidental–. Entre ellas se indican:

- No apagar antes de completar la recolección de evidencia, dado que la evidencia se puede perder y/o el atacante pudo haber alterado el apagado/encendido de los servicios/scripts para destruirla.

- No confiar en los programas del sistema, para ello es conveniente emplear programas de recolección de evidencia propios desde medios debidamente protegidos.

- Evitar hacer correr programas que modifiquen los registros de hora/tiempo de accesos de los archivos de sistema

Retrotrayendo al caso de Panamá, podemos observar cuáles fueron los errores cometidos al momento de descubrir el hecho delictivo –los ataques cibernéticos– que comprometieron y destruyeron la evidencia. Varias de estas recomendaciones, de haberlas seguido, hubieran servido para lograr un resultado óptimo en la búsqueda de la verdad material de la causa.

VIII. La aplicación de la normativa ISO/IEC 27037:2012

Diez años después de que saliera a la luz la guía de NWG respecto al manejo de evidencia digital forense, la Organización Internacional de Estandarizaciones (ISO) emitió la norma ISO/IEC 27037:2012(E)[42]. Esta normativa busca ser una guía para actividades específicas respecto al manejo de la evidencia digital, puntualmente en lo relativo a la identificación, recolección, adquisición y preservación de potencial evidencia digital que pueda resultar de importancia a la causa judicial.

En el apartado donde aborda los principios de manejo de prueba digital, parte de la base que en la mayoría de los estrados judiciales el manejo de la prueba se rige por su relevancia, confiabilidad y suficiencia, siempre relacionado a los hechos delictivos que se investigan. Estos principios no son exclusivos de la prueba de naturaleza digital, sino que, se extienden a todo tipo de pruebas[43].

Cuando la normativa hace referencia a la relevancia de la prueba, implica que esta es capaz de demostrar o no la veracidad de el o los elementos investigados en la causa. Por otro lado, comprende que el uso de la terminología "confiable" puede variar en su significado o contenido, dependiendo de cada jurisdicción (a nivel global) habría un cierto consenso en considerarlo como el carácter en que "la evidencia digital sea lo que busca ser", en otras palabras, realmente sea el medio probatorio del hecho que se investiga.

Ahora bien, no es necesario recolectar toda la data o hacer copia de ella; puesto que eso se deberá ajustar a los elementos y hechos que se investigan. Ergo, la recolección se realizará sobre la potencial evidencia digital que se considere conducente a dilucidar los hechos en la causa, eficientizando los costos y tiempos de la investigación y pericia, siempre en concordancia con las normas penales y procesales del lugar del hecho.

Entre otras recomendaciones realizadas por la normativa, está contemplada la posibilidad que la pericia sea llevada a cabo por agentes externos a los peritos oficiales (agentes colaboradores del Ministerio Fiscal), para lo cual establece una serie de pautas para la validación de la pericia, entre ellos:

- Documentar todas las acciones;

- Indicar el método empleado para la realización de la copia de evidencia, de forma tal que se pueda establecer la confiabilidad y exactitud respecto de esta, en relación con la original;

- Reconocer que la preservación de la potencial evidencia digital puede llegar a ser intrusiva en algunos casos.

El objetivo principal de esta normativa **tendiente a la estandarización** es, por un lado, promover buenas prácticas respecto a los métodos y procedimientos implementados en la recolección, preservación y análisis forense de la prueba digital. Por otro lado, se busca que paulatinamente estos estándares sean incorporados e implementados por las distintas jurisdicciones, de forma tal que la comparación, combinación y contraste de los resultados de dichas investigaciones puedan ser compartidas a nivel internacional, sin que la o las personas u organizaciones que realicen la pericia o las normativas de las diferentes jurisdicciones resulten un obstáculo.

Asimismo, hay que tener en consideración que esta guía estandarizadora es abarcativa a una gran variedad de información y medios digitales, susceptibles de ser empleados como prueba digital, tales como en el caso de dispositivos de almacenamiento digital (p.ej.: discos duros, disquetes, discos ópticos y magneto ópticos, dispositivos de datos) tanto de computadoras como de teléfonos móviles; asistentes digitales personales (PDA); dispositivos electrónicos personales (PED), tarjetas de memoria, sistemas de navegación móviles; cámaras fotográficas y de vídeo digitales (CCTV); computadora con conexiones de red; redes basadas en TCP/IP entre otros protocolos digitales, y demás dispositivos con funciones similares a las anteriormente mencionadas.

IX. Los estándares de la Interpol

Si bien la normativa ISO/IEC 27037 fue actualizada en 2018, uno de los estándares más recientes es el que fue publicado por el Interpol en 2019[44]. Estas Directrices Globales para Laboratorios Forenses Digitales resultan ser unas guías minuciosas con respecto al manejo de la evidencia, dentro y fuera del laboratorio, incluso aborda cómo debe seleccionarse a los miembros del laboratorio, su formación y entrenamiento; incluyendo un anexo con una lista de habilidades necesarias según la función de cada miembro del laboratorio[45]. Así también indica cómo debe equiparse el laboratorio para llevar a cabo los estudios y análisis, entre varios temas estudiados en la mencionada guía.

Al igual que las anteriores, establece una serie de principios rectores que deben seguirse para el manejo de la evidencia digital, a mencionar:

- La evidencia digital debe ser obtenida de manera legal;

- El equipo profesional involucrado debe culminar el programa de entrenamiento, previo al manejo y análisis de cualquier evidencia digital;

- Cualquier actuación sobre la evidencia jamás debe modificar la data que almacena. En el caso que se deba acceder a la data original o modificar la configuración del sistema, se recomienda que dicha acción sea realizada por profesionales capacitados para ello, con la debida justificación respaldatoria para dicho proceder;

- Cualquier actividad que implique el acceso a la data original o su modificación deberá ser documentada ante la observación de un profesional colega como testigo;

- La documentación de toda acción que se lleve a cabo en relación al manejo de evidencia digital debe ser creada y preservada de forma tal que permita ser auditada. Un tercero independiente deberá ser capaz de repetir todas las acciones del proceso, obteniendo los mismos resultados.

De esta exhaustiva guía, se pueden incorporar varios puntos, no solo a nivel técnico, sino también a nivel profesional, en lo referido a la formación académica y especializaciones del personal a cargo de desempeñar el estudio

(42) ISO, ISO/IEC 27037:2012, https://www.iso.org/standard/44381.html [fecha de acceso: 25/07/24].

(43) ISO, ISO/IEC 27037:2012, 5.2, https://www.iso.org/standard/44381.html [fecha de acceso: 25/07/24].

(44) Interpol; "Global guidelines for digital forensics laboratories", https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics [fecha de acceso: 25/07/24].

(45) Interpol; "Global guidelines for digital forensics laboratories", APPENDIX A: DFL SKILLSET CHECKLIST, https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics [fecha de acceso: 25/07/24].

forense. Resulta evidente una constante actualización e inversión formativa como tecnológico para lograr tener un laboratorio forense en óptimas condiciones y capacitado para enfrentar este tipo de tareas.

X. La prueba digital y el Código Procesal Penal Federal

El nuevo Código de Procedimiento Penal Federal (CPPF) cuenta con la novedad de haber incorporado en materia de prueba la "incautación de datos"[46]. Lo que implica un abordaje aggiornado al ecosistema digital en el que nos movemos a diario. Ello por cuanto, las comunicaciones y la información dejaron de viajar o ser almacenadas exclusivamente en formato papel o de forma material. La binarización de la data, debido a diversos factores (por ejemplo: portabilidad, capacidad de almacenamiento, rapidez de procesamiento, etc.), ha favorecido la implementación de dispositivos digitales de toda índole.

Ahora bien, además de permitir "[...] el registro de un sistema informático o de una parte de este, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación"[47], establece que un miembro del Ministerio Fiscal es el que llevará a cabo el procedimiento de apertura. Este agente debería contar con el *expertise* suficiente para poder concretar dicha tarea, respetando la cadena de custodia y la integridad de la información –posiblemente– relevante en la causa investigada[48].

Ahora bien, surge a todas luces que quien realizará la real apertura, copia, procesamiento, etc., no será necesariamente el fiscal ni otro agente que desempeñe tarea similar al primero. La intervención *ab-initio* de cualquier procedimiento, para la conservación probatoria le corresponderá a un técnico experto en la materia. De lo contrario, yerros como los acaecidos en la causa panameña podrían arribar a un fallo que desestime la prueba recabada por insuficiente o por no haber vinculado a un individuo con el hecho investigado.

En la letra del artículo 153 del digesto procesal, podemos apreciar uno de los principios mencionados en las guías de estandarización analizadas. En efecto, cuando se refiere a la conservación, hace mención de asegurar "la fidelidad del registro". El término "fidelidad" resulta ser un sinónimo de "confianza" –empleado por la NWG–, como así también de "exactitud"[49].

Otro artículo relevante es el 157, que versa sobre la cadena de custodia. Este reza: "[c]on el fin de asegurar los elementos de prueba, se establecerá una cadena de custodia que resguardará su identidad, estado y conservación. Se identificará a todas las personas que hayan tomado contacto con esos elementos, siendo responsables los funcionarios públicos y particulares intervinientes"[50].

Este articulado nos lleva nuevamente a la consideración de la conservación, inalterada, original de la información o data, buscando preservar su integridad. Para La Rosa y Romero Villanueva, la cadena de custodia no necesariamente implica la documentación de todas las actividades realizadas durante el peritaje de los dispositivos, procesamiento y análisis de la información. En algunos casos, la testimonial de otras personas que intervinieron en el peritaje resultaría suficiente[51]. Similar a la opinión de los juristas anteriores es lo que estipulaban las guías del Interpol.

XI. Conclusiones

Resulta primordial que desde el ámbito de las Fiscalías –como agentes estatales investigadores de las causas penales– se cuente con personal técnico formado o con la colaboración de un equipo de especialistas en informática forense para evitar que, por un manejo erróneo, a futuro se perjudique el desenvolvimiento de la causa judicial. Además de las herramientas técnicas con las que cuentan los forenses para el análisis de la prueba incautada durante la investigación, cabe destacar el papel fundamental que tienen los estándares internacionales como herramientas que permiten mantener un nivel de calidad en la realización de la pericia, siendo extensivo a todos los elementos que la rodean (p. ej., laboratorios, capacitación del personal, estandarización de formatos, etc.).

Es imperativo, además, garantizar la correcta implementación de cálculos de hash y la preservación de la cadena de custodia. El cálculo de hash asegura la integridad de la evidencia digital, permitiendo verificar que los datos no han sido alterados desde el momento de su incautación hasta su análisis en el laboratorio forense. La cadena de custodia, por su parte, es esencial para rastrear y documentar cada paso que la evidencia digital recorre, desde su obtención hasta su presentación en juicio, asegurando que cada individuo que haya tenido acceso a dicha evidencia esté debidamente identificado y que los procedimientos de manejo se hayan realizado conforme a las normativas establecidas.

En el contexto del Código Procesal Penal Federal (CPPF), sería conveniente que se reglamentara específicamente el manejo de la evidencia digital. Esto incluiría desde la designación del agente responsable de la "apertura" de la evidencia, asegurando que el mismo posea la idoneidad técnica para llevar a cabo dicha tarea, hasta la estipulación de las formas y recaudos necesarios para garantizar la integridad de la cadena de custodia. La reglamentación detallada permitiría establecer protocolos claros y uniformes, minimizando el riesgo de errores y fortaleciendo la validez de la evidencia digital presentada en los tribunales.

(46) CPPF, art. 151, B.O. 08/02/2019.
(47) CPPF, art. 151, B.O. 08/02/2019.
(48) CPPF, art. 152, B.O. 08/02/2019.
(49) RAE, fidelidad, https://dle.rae.es/fidelidad [fecha de acceso:25/07/24].
(50) CPPF, art. 157, B.O. 08/02/2019.
(51) La Rosa, Mariano R,; Romero Villanueva, Horacio J.; "Código Procesal Penal Federal comentado", Tomo II, pág. 247.

XII. Bibliografía

- NIST, NISTIR 7711, Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters, Appendix C, https://doi.org/10.6028/NIST.IR.7711 [fecha de acceso: 22/07/2024].
- Fortinet. "DoS vs DDoS", https://www.fortinet.com/lat/resources/cyberglossary/dos-vs-ddos [fecha de acceso 14/07/2024].
- MITRE ATT&CK, "Network Denial of Service", https://attack.mitre.org/techniques/T1498/ [fecha de acceso: 22/07/24].
- Siegel, Michael; Sciore, Edward; Madnick, Stuart; "Context Interchange in a Client-Server Architecture", MIT, http://web.mit.edu/smadnick/www/wp2-old%20names/CISL%2393-07.pdf [fecha de acceso: 14/07/24].
- INCIBE; "¿Qué son los ataques DoS y DDoS?". https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos [fecha de acceso 14/07/2024].
- CISA; "DDoS Quick Guide", https://www.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf [fecha de acceso: 14/07/2024].
- Firth, Jack; "Requests", https://plt.cs.northwestern.edu/release-pkg-build/doc/request/index.html [fecha de acceso: 14/07/24].
- Oppliger, Rolf; *SSL and TLS: Theory and Practice*, Artech House, 2023.
- Yang, Guang; "Introduction to TCP/IP network attacks", *Secure Systems Lab* (1997), http://seclab.cs.sunysb.edu/sekar/papers/netattacks.pdf [fecha de acceso: 14/07/24].
- Rosen, Rami; "Internet control message protocol (ICMP)", *Linux Kernel Networking: Implementation and Theory*, 2014.
- Martin, Jeremy; Rye, Erik; Beverly, Robert; "Decomposition of MAC address structure for granular device inference", en *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pp. 78-88, 2016.
- Meisam Eslahi, Rosli Salleh, Nor Badrul Anuar; "Bots and Botnets: An Overview of Characteristics, Detection and Challenges", IEEE International Conference on Control System, Computing and Engineering, 23 - 25 Nov. 2012, Penang, Malaysia.
- Zeidanloo, Hossein Rouhani, Mohammad Jorjor Zadeh Shooshtari, Payam Vahdani Amoli, M. Safari, and Mazdak Zamani; "A taxonomy of botnet detection techniques", *3rd International Conference on Computer Science and Information Technology*, IEEE, *2010,* Vol. 2, pp. 158-162.
- Woodiss-Field, A., Johnstone, M.N., y Haskell-Dowland, P., "Examination of Traditional Botnet Detection on IoT-Based Bots", *Sensors* 24, no. 3 (2024): 1027. https://doi.org/10.3390/s24031027 [fecha de acceso: 14/07/2024].
- IBM; "¿Qué es un ataque DDoS?", https://www.ibm.com/es-es/topics/ddos [fecha de acceso 14/07/2024].

- Dingledine, Roger; Mathewson, Nick; Syverson, Paul; “Tor: The Second-Generation Onion Router”, https://apps.dtic.mil/sti/pdfs/ADA465464.pdf [fecha de acceso: 14/07/24].

- Sánchez-Rola, Iskander; Balzarotti, Davide; Santos, Igor; “The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services”, WWW ‘17: Proceedings of the 26th International Conference on World Wide Web, https://www.eurecom.fr/en/publication/5152/download/sec-publi-5152.pdf [fecha de acceso: 14/07/24].

- Invisible Internet Project (I2P); https://geti2p.net/_static/pdf/i2p_philosophy.pdf [fecha de acceso: 15/07/24].

- Clarke, Ian; Sandberg, Oskar; Wiley, Brandon; Hon, Theodore W.; “Freenet: A Distributed Anonymous Information Storage and Retrieval System”, https://www.cs.cornell.edu/people/egs/615/freenet.pdf [fecha de acceso: 15/07/24].

- Pavlicek, Antonin; Sudzina, Frantisek; “Internet Security and Privacy in VPN”, Journal of Networking Technology, Volume 9, Number 4, December 2018, pp. 133-139, https://www.dline.info/jnt/fulltext/v9n4/jntv9n4_1.pdf [fecha de acceso: 15/07/24].

- David Dwiputra Kurniadi; “The Difference Between Using Proxy Server and VPN”, Sisforma, vol. 2, no. 1, May 2015, pp. 19-22, https://www.researchgate.net/publication/317809198_The_Difference_Between_Using_Proxy_Server_and_VPN [fecha de acceso: 15/07/24].

- Jyothi, K; Reddy, B. Indira; “Study on Virtual Private Network (VPN), VPN’s Protocols And Security”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology; Volume 3; Issue 5, pp. 919-932, https://www.researchgate.net/publication/368831275_CSEIT1835225_Study_on_Virtual_Private_Network_VPN_VPN’s_Protocols_And_Security [fecha de acceso: 15/007/24].

- Pourvahab, Mehran; Ekbatanifard, Gholamhossein; “Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology”, https://www.researchgate.net/publication/336446265_Digital_Forensics_Architecture_for_Evidence_Collection_and_Provenance_Preservation_in_IaaS_Cloud_Environment_Using_SDN_and_Blockchain_Technology [fecha de acceso: 15/07/24].

- Macharia, Kelvin W.; “Cryptographic Hash Functions”, https://www.researchgate.net/publication/254035333_A_complete_study_on_tools_techniques_for_digital_forensic_analysis [fecha de acceso: 15/07/24].

- Fukami, Aya; Ghose, Saugata; Luo, Yixin; Cai, Yu; Mutlu, Onur; “Improving the reliability of chip-off forensic analysis of NAND flash memory devices”, Digital Investigation 20, 2017, S1-S11, https://www.cs.cmu.edu/~yixinluo/index_files/chip-off-forensic_dfrws17.pdf [fecha de acceso: 16/07/24].

- Rearick, J.; Eklow, B.; Posse, K.; Crouch, Alfred; Bennetts, B.; “IJTAG (internal JTAG): a step toward a DFT standard”, Test Conference, Proceedings, ITC 2005, IEEE International, https://www.researchgate.net/publication/4217729_IJTAG_internal_JTAG_a_step_toward_a_DFT_standard [fecha de acceso: 15/07/24].

- Ruan, Keyun; Carthy, Joe; Kechadi, Tahar; Crosbie, Mark; “Cloud Forensics”, Advances in Digital Forensics VII, 2011, pp. 35-46, https://www.researchgate.net/publication/221352743_Cloud_Forensics [fecha de acceso: 15/07/24].

- Brezinski, D.; Killalea, T.; “Guidelines for Evidence Collection and Archiving”, NWG, febrero 2002, https://www.rfc-editor.org/rfc/pdfrfc/rfc3227.txt.pdf [fecha de acceso: 22/07/2024].

- ISO, ISO/IEC 27037:2012, https://www.iso.org/standard/44381.html [fecha de acceso: 25/07/24].

- Interpol; “Global guidelines for digital forensics laboratories”, https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics [fecha de acceso: 25/07/24].

- CPPF, B.O. 08/02/2019.

- RAE, fidelidad, https://dle.rae.es/fidelidad [fecha de acceso: 25/07/24].

- La Rosa, Mariano R; Romero Villanueva, Horacio J.; “Código Procesal Penal Federal comentado”, Tomo II.

VOCES: DELITOS INFORMÁTICOS - INTERNET - INFORMÁTICA - RESPONSABILIDAD PENAL - PRUEBA DIGITAL - PRUEBA PERICIAL - TECNOLOGÍA - PODER JUDICIAL - PRUEBA - HÁBEAS DATA - CÓDIGO PROCESAL PENAL - DERECHO A LA PRIVACIDAD - PROTECCIÓN DE DATOS PERSONALES - DEFENSA EN JUICIO - EXPEDIENTE JUDICIAL - EJERCICIO PROFESIONAL - JUECES - DERECHO PROCESAL - SENTENCIA - PROCESO PENAL - JURISPRUDENCIA - CONSTITUCIÓN NACIONAL - COMUNICACIONES ELECTRÓNICAS

La personalidad jurídica de la inteligencia artificial(*)

por María Constanza Quiñones(**)

Sumario: I. Introducción. – II. Relación entre el Derecho y la inteligencia artificial. – III. El ordenamiento jurídico argentino. – IV. ¿Qué entendemos por personalidad jurídica? *a. Antecedentes. b. Personas jurídicas. c. Otros reconocimientos*. – V. ¿Cuáles son los elementos/conceptos que trae consigo la inteligencia artificial que hace que nos planteemos la posibilidad de que se le reconozca o atribuya personalidad jurídica? – VI. Posturas a favor de que la IA tenga personalidad jurídica propia. – VII. Posturas en contra de que la IA tenga personalidad jurídica propia. – VIII. Posturas ecléctica. – IX. Conclusión. – X. Bibliografía.

I. Introducción

Los grandes avances en el campo de la tecnología son cada vez más deslumbrantes y fascinantes. Entre sus protagonistas, nos encontramos con la inteligencia artificial (en adelante, IA). Su creciente interacción con la Sociedad hace que se prendan todas las alarmas en el campo del Derecho, donde nos comenzamos a plantear interrogantes como qué es la IA para nuestro ordenamiento jurídico y si sus notas distintivas tornan exigible o recomendable la atribución o el reconocimiento de personalidad jurídica.

Son muchos los autores que hacen referencia a la existencia de un capítulo "social" dentro de la IA, resaltando que esta tecnología ya no es una simple herramienta del hombre, sino que se ha vuelto una compañía esencial para el ser humano, que, al poseer determinadas características, como su autonomía, o autoaprendizaje, no pueden ser considerados simples objetos o cosas.

Estamos hablando de la *interacción social* que la IA tiene con los seres humanos, y que estos tienen con la IA. Se trata de un hecho fáctico que sirve de punto de partida para demostrar el rol protagónico de la IA en nuestra sociedad, que con el tiempo va a cobrar mayor importancia en tanto esta tecnología se vuelva cada vez más sofisticada y precisa. Fruto de ese desarrollo inminente, o más bien actual, nos enfrentamos a futuros escenarios donde la IA comience a desenvolverse de una manera autónoma e independiente, como ya sucede con los llamados "autos autónomos".

Pin Lean Lau ha dado un paso más, e incluso habla de los robots dotados de IA como *robots humanoides sociales*, y destaca esta intersección entre la humanidad y la tecnología. Es de mayor entidad el hecho de que sea caracterizado como social, en tanto en realidad es ella aquella nota distintiva del hombre a quien siempre se lo define como un ser social(1).

Vemos aquí cómo las palabras que se usan para caracterizar a la IA son aquellas que usamos para diferenciar al hombre de las demás criaturas.

La IA ha demostrado ser de gran utilidad, en tanto ha permitido que se "(…) reduzcan costos, mejoren la calidad de los servicios, la coordinación, la productividad y la eficiencia (…)"(2). Todo ello hace que la IA posea un protagonismo que no será posible quitarle, lo que implica que, como dijimos previamente, el derecho deba aparecer en este escenario para regular esa participación en nuestra sociedad. Después de todo, la IA "(…) cambiará el funcionamiento económico de las empresas y tendrá un impacto enorme en la sociedad (…)"(3).

La IA resulta ser una esencial herramienta para combatir una vasta diversidad de problemáticas, relacionadas ellas con el medio ambiente, la salud, la seguridad, e incluso la ciberseguridad, entre muchas más(4).

Por tales motivos, nos hemos planteado el desafío de exponer y analizar las diversas visiones que hay en el mundo jurídico sobre la posibilidad y conveniencia de reconocer o atribuir personalidad jurídica a la IA. Para ello, primero realizaremos un análisis sobre el concepto de persona en sí mismo, y su evolución a lo largo de la historia. Luego, profundizaremos sobre la existencia de otros entes que han sido objeto de reconocimiento de personalidad, como las personas jurídicas, los animales y los ecosistemas. Ello nos dará el punto de partida para analizar cuáles son los elementos que trae consigo la IA que ponen los conceptos tradicionales del derecho en jaque, y, por último, haremos un relevamiento de las diversas posturas en contra y en favor del reconocimiento de la personalidad de la IA.

II. Relación entre el Derecho y la inteligencia artificial

El ordenamiento jurídico que tenemos hoy en Argentina, como muchos otros en el resto del mundo, debe em-

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico*, por Marcelo Oscar Vuotto, ED, 261-860; *¿El control del trabajador por medio de tecnologías que posibilitan conocer su ubicación afecta su derecho a la intimidad? Nota al caso "Pavolotzki"*, por Juan Ángel Confalonieri (h.), TySS, 2016-297; *El uso de la tecnología y la gestión de la comunicación en la mediación actual*, por Juan Fernando Gouvert, ED, 275-771; *El derecho ante la inteligencia artificial y la robótica*, por Verónica Elvia Melo, ED, 276-493; *La protección de los datos personales en internet (una tarea ineludible)*, por Esteban Ruiz Martínez, ED, diario nº 14.706 del 5-9-19; *La comunidad humana en la era tecnológica*, por Leonardo Pucheta, ED, 282-1044; *Algoritmos de inteligencia artificial con fines de control fiscal: ¿puede el derecho embridar a las nuevas tecnologías?*, por José Manuel Calderón Carrero, El Derecho Tributario, marzo 2020 - Número 1, cita digital: ED-CMXIII-759; *El Derecho en la nueva era tecnológica*, por Julia Inés Imperiale, ED, 287-805; *La inteligencia artificial en la Administración Pública y los derechos fundamentales*, por Ricardo A. Muñoz (h.), Revista de Derecho Administrativo, mayo 2020 - Número 5; *La inteligencia artificial en el mundo jurídico actual (Implicancias, aplicaciones y posibilidades)*, por Alberto B. Bianchi, Derecho, Innovación & Desarrollo Sustentable, Número 3 - octubre 2021; *El Vaticano propone ante la ONU regular el uso pacífico de la inteligencia artificial*, Diario de Derecho Constitucional, El Derecho Constitucional, diciembre 2021 - Número 12; *Administración de justicia e inteligencia artificial: una mirada ética sobre la relación entre eficiencia y equidad*, por Estela Josefina Condrac, Derecho, Innovación & Desarrollo Sustentable, Número 6 - abril 2022; *Breves consideraciones sobre el encuadre ético de la Inteligencia Artificial (IA)*, por Cristina Margarita Rosa Hofkamp, El Derecho Constitucional, diciembre 2022 - Número 12; *Ética en tiempos de inteligencia artificial. Reflexiones en torno a los planteos éticos de las IA en tiempos laberínticos de vulnerabilidad y transhumanismo que propone la Cuarta Revolución Industrial*, por Gustavo Andrade Figueroa, Derecho, Innovación & Desarrollo Sustentable, Número 14 - agosto 2023; *Automatización, virtualidad y eficacia, estandartes de las transformaciones procesales en el expediente digital de la Justicia bonaerense. Nuevo Reglamento de Presentaciones y Notificaciones Electrónicas –Acuerdo nº 4013/2021 SCBA– (T.O. Acuerdo nº 4039/2021)*, por Paulo Alberto Maresca, ED, 295-897; Abogacía digital. De la toga al metaverso, por Matilde Pérez, El Derecho - Diario, El abogado y el futuro, Cita Digital: ED-MMMCDVI-607. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) El presente artículo se inscribe dentro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el profesor doctor Jorge Nicolás Lafferriere, concretamente en el Programa IUS titulado: "El derecho civil patrimonial frente al emergente alta tecnología. Desafíos e interpretación jurídico/patrimonial frente al avance tecnológico, la innovación permanente y el desarrollo sustentable", que dirigen los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas que los acompañan.

(**) Abogada (Universidad Austral), Maestranda en Derecho Empresarial (Universidad Austral), Coordinadora Académica de la Maestría en Derecho Empresario Global (Universidad Austral). Ayudante Diplomada en las cátedras de Derecho Privado I, Derecho de las Obligaciones, Derecho de Daños y Derechos Reales (UA).

La presente investigación se realizó en el marco del 17° Concurso Interno de Proyectos de Investigación Científica 2021 - Sección Estudiantes, convocado por el Vicerrectorado de Investigación de la Universidad Austral, en el marco del proyecto titulado "La responsabilidad civil por daños causados por Inteligencia Artificial: análisis de las respuestas del Derecho argentino a la atribución de autoría y responsabilidad".

Quisiera agradecer al Dr. Franco A. Melchiori por haber dirigido la presente investigación, por sus correcciones, consejos y recomendaciones.

(1) Lean Lau, Pin, "*The Extension of Legal Personhood in Artificial Intelligence*", *Revista de Bioética y Derecho. Perspectivas Bioéticas*, Volumen 46, 2019, 47-66. Pág. 48.

(2) Vivas, Fredi, *¿Cómo piensan las máquinas? Inteligencia Artificial para humanos*, Ciudad Autónoma de Buenos Aires, Galerna, 2021. Pág. 146.

(3) Merchán Murillo, Antonio, "Retos Regulatorios en torno a la Inteligencia Artificial", *Pensar. Revista de Ciencias Jurídicas*, Número 4, Volumen 23, 2018. Pág. 1.

(4) Cfr. Cisneros Murugarren, Amaiur, "Robots dotados de Inteligencia Artificial: Su posible personalidad jurídica y responsabilidad por daños", Trabajo de fin de Máster (Máster de acceso al ejercicio de la abogacía) en la Facultad de Derecho de la Universidad Complutense de Madrid, 2021. Pág. 3.

prender la futura regulación de esta tecnología, para así poder hacer frente a esta nueva realidad, y poder responder a las nuevas necesidades que hoy posee el hombre. Es menester que este ordenamiento jurídico pueda ser suficiente para responder ante cualquier problemática.

Es importante que en el presente análisis no caigamos en el temor que el mundo del cine y de la literatura parecen expresar, donde la IA se apodera de todo lo que la rodea, en tanto se trata de un desarrollo que debemos afrontar por medios pacíficos y acorde a las reglas que sean respetuosas de las personas humanas[5].

El derecho debe preocuparse por regular, por un lado, el ejercicio de esta disciplina y facilitar su desarrollo, y, a su vez, crear la normativa necesaria para que esta actividad sea respetuosa de los principios y derechos fundamentales que forman parte de nuestro ordenamiento jurídico. No solo ello, sino que también, dadas las características de la IA, el derecho debe regular qué sucede cuando aquella IA funciona a la par de personas humanas, donde se pueden dar determinadas eventualidades que podrían implicar la responsabilidad de las máquinas.

No se trata tan solo de un experimento de laboratorio, o de una teoría que todavía requiere experimentación, sino que, como vemos con los autos autónomos, ellos pueden dar lugar a eventualidades frente a las cuales debemos saber qué hacer, de manera que el concepto de justicia no quede perdido en el camino.

Empero, antes de preguntarnos por su responsabilidad, debemos preguntarnos qué es para el derecho la IA. Esto hace referencia a la pregunta sobre si la IA puede ser considerada una cosa, una persona, o si acaso se debería crear una nueva categoría jurídica que responda de manera acabada a esta realidad tecnológica.

III. El ordenamiento jurídico argentino

Si bien nuestras normas pueden responder a casos donde la tecnología se encuentra presente, como sucede con máquinas que sean utilizadas en fábricas, o los mismos autos que no son autónomos, la IA es una tecnología distinta, que amerita un nivel de análisis diferente, en virtud de sus características propias, como son su autonomía, inteligencia e imprevisibilidad. La IA se encuentra programada por "(…) algoritmos que se construyen para lograr objetivos definidos, tienen el poder de transformar organizaciones de una manera cualitativamente diferente a otras tecnologías (…)"[6].

Es por ello que debemos comenzar con el análisis de una temática fundamental que ha creado un gran debate doctrinario en el mundo, y ese es si la IA puede ser objeto de reconocimiento de personalidad jurídica.

Al tener determinadas cualidades que se asemejan a las del ser humano, ¿podría el ordenamiento jurídico conferirle el estatus de persona a la IA? O, ¿acaso se le debería dar un estatus intermedio donde a la misma no se la reconoce como persona, pero tampoco como cosa? Nos encontramos así ante el análisis sobre si puede la IA poseer personalidad jurídica. Aquí nos interrogamos sobre si puede, por ejemplo, un robot, ser titular de derechos y obligaciones, y por lo tanto celebrar contratos con terceros, o si precisamos quizá crear una nueva categoría que responda a sus características inherentes[7].

IV. ¿Qué entendemos por personalidad jurídica?

Para comprender el concepto de personalidad jurídica, vamos a hacer referencia al concepto de sujeto de derecho. Javier Hervada escribe que el hombre es naturalmente un sujeto de derecho, empero, ¿qué es lo que lo hace ello? "(…) para que el hombre posea algo como suyo debe ser poseedor de su propio ser, esto es, debe ser persona"[8]. Es por ello entonces que nos preguntamos, ¿podría la IA ser titular de tales atributos?

a. Antecedentes

El concepto de la personalidad jurídica trata de un instituto que no ha existido siempre como lo conocemos hoy, sino que ha sido fruto de una gran evolución que comienza en el derecho romano. Aunque debemos resaltar que, si bien tiene su origen allí, lo cierto es que "(…) los juristas romanos no elaboraron una teoría de la personalidad jurídica, como desarrollarían más tarde los juristas del Medievo"[9]. Aquí, comenzaremos un análisis sobre el concepto de persona en sentido jurídico.

En ese entonces no se hablaba de la persona como lo hacemos hoy en día, como *centro de imputación de normas o como sujeto de derecho*. En la antigua Roma, si se hablaba de persona, "(…) se hablaba de los hombres, es decir, los entes biológicos que consisten en la unidad psicofísica humana (…) y lo que interesaba era su situación jurídica (status), es decir, la posición o situación jurídica que ocupa en la sociedad, esto es, en la *civitas* y en la familia"[10].

En ese entonces, no todos eran reconocidos como personas frente al derecho. En base al cumplimiento de determinadas cualidades, características y estatutos, es que el ser humano era realmente conocido como persona o no. Es decir, como un sujeto capaz de tener derechos, y contraer obligaciones. De esta forma es que se distinguía entre el esclavo y el libre.

Muchos autores utilizan esta situación que se dio en el derecho romano para comentar sobre cómo el concepto de personalidad jurídica no siempre ha sido respetuoso de todas las personas, y el ordenamiento con el tiempo va colocando bajo el paraguas de personalidad nuevas personas, o entes. Esta es una temática que se abordará dentro de unos apartados.

Tiempo después el concepto de esclavo del derecho romano fue reemplazado por el concepto de siervo. Se trató de un instituto muy parecido al del esclavo de la antigua Roma, pero este ya no pertenecía a otra persona, y tenía algunos derechos. En ese entonces se hablaba del *status hominum*, al cual "(…) se lo definió como la *condición o manera en que los omes viven o están*, y se dice que la condición de ellos puede ser de tres formas: *libres, o siervos, o aforrados, a que llaman en latin abiertos*"[11].

Como podemos ver, en los comienzos de la historia del derecho el concepto de persona no era como aquel que tenemos hoy. Fue con el tiempo que los ordenamientos jurídicos comenzaron a desarrollar un concepto de persona más respetuoso de sus cualidades inherentes y de su dignidad humana. Es recién en los últimos siglos que se lleva a cabo un reconocimiento pleno de todos los seres humanos como personas, y es recién desde este entonces que se coloca a la persona como el centro del ordenamiento jurídico, volviéndose así un centro de imputación de normas. Lo cierto es que el concepto de personalidad jurídica "es uno de los más controvertidos para la doctrina"[12]. Y este reconocimiento, reciente, se ha dado gracias al reconocimiento de la dignidad humana.

De esta forma podemos ver el análisis del concepto de persona, por un lado, en su sentido jurídico, y por otro en su sentido filosófico y teológico. Todo esto nos va a servir para analizar si entonces es correcto o no atribuir el concepto de persona a la IA, al analizar si la misma puede responder a los preceptos y cualidades inherentes a la palabra *persona*.

b. Personas jurídicas

Muchos autores analizan cómo la atribución de personalidad jurídica depende, por supuesto, del ordenamiento jurídico y cómo el mismo se ha ido adaptando a la realidad, otorgándole tal concepto a otras realidades distintas de la persona humana. Entre ellas nos encontramos con las personas jurídicas, o personas de existencia ideal, al-

(5) Cfr. Vivas, Fredi, *¿Cómo piensan las máquinas? Inteligencia Artificial para humanos*, Ciudad Autónoma de Buenos Aires, Galerna, 2021. Pág. 141.

(6) Vivas, Fredi, *¿Cómo piensan las máquinas? Inteligencia Artificial para humanos*, Ciudad Autónoma de Buenos Aires, Galerna, 2021. Pág. 149.

(7) Cfr. Cisneros Murugarren, Amaiur, "Robots dotados de Inteligencia Artificial: Su posible personalidad jurídica y responsabilidad por daños", Trabajo de fin de Máster (Máster de acceso al ejercicio de la abogacía) en la Facultad de Derecho de la Universidad Complutense de Madrid, 2021. Pág. 14.

(8) Hervada, Javier, *¿Qué es el derecho? La moderna propuesta del realismo jurídico. Una introducción al derecho*. Tercera edición. España, Ediciones Universidad de Navarra, S.A., Pamplona, 2011. https://dadun.unav.edu/bitstream/10171/56682/1/03-Qué%20es%20el%20derecho.pdf. Pág. 78. Consultada el 22/02/2023.

(9) Gallego-Burín, Marina Rojo, "Los fundamentos históricos del sistema jurídico versus la personalidad electrónica de los robots", *Revista Jurídica de Castilla y León*, Número 52, 2020. Pág. 12.

(10) Di Pietro, Alfredo, *Derecho Privado Romano*, Buenos Aires, Depalma, Segunda Edición, 2001. Pág. 121.

(11) Gallego-Burín, Marina Rojo, "Los fundamentos históricos del sistema jurídico versus la personalidad electrónica de los robots", *Revista Jurídica de Castilla y León*, Número 52, 2020. La autora cita dentro de este contexto a Las Siete Partidas del Sabio Rey don Alfonso el nono, nuevamente Glosadas por el licenciado Gregorio López del Consejo Real de Indias de su Magestad.

(12) *Ibid.*

gunos sistemas ecológicos y la situación controvertida de los animales.

De hecho, Chesterman resalta que la pregunta sobre si la IA puede ser objeto de tal reconocimiento, no solo nos invita, sino que hace que revisemos aquellos argumentos que se dieron en estos últimos tiempos respecto de las personas jurídicas, animales y otros objetos que no son aquellos que típicamente caen bajo el paraguas de la personalidad jurídica[13].

Comencemos con el análisis de las personas jurídicas. En la antigua Roma, no existía aún este concepto, aunque podemos encontrar algunos esbozos del mismo en el derecho posclásico y en el derecho Justinianeo[14]. Vemos que, así como el concepto de persona fue objeto de una ardua evolución y constante discusión, lo mismo sucedió con el concepto de persona jurídica. Se debió esperar a la época imperial, que es "(…) cuando surge la idea de persona jurídica, asignada en primer lugar a las ciudades que, careciendo de independencia política, podían actuar en el campo del derecho privado, surgiendo así los primeros entes –diferentes de las personas humanas– con capacidad jurídica (…) A posteriori, advirtiendo su utilidad, la idea se extendió a otros entes como las provincias, colegios sacerdotales, y luego a las primeras sociedades comerciales"[15].

La persona jurídica es un ejemplo de algo distinto de la persona humana a la cual el ordenamiento jurídico le reconoce personalidad jurídica. La mayor parte de los ordenamientos jurídicos del mundo reconocen dos formas de persona, la persona natural y la persona jurídica. Lo que es interesante resaltar de esta dualidad es que, si bien ambos son objeto de reconocimiento de personalidad jurídica, "(…) las personas jurídicas y los seres humanos tienen diferentes conjuntos de derechos y deberes legales"[16].

Vemos ese reconocimiento en la misma definición de persona jurídica en tanto a ella se la define como "(…) todo ser o entidad que sea susceptible de ostentar derechos y obligaciones, en otras palabras, todo aquel que cumple los requisitos para que se le puedan atribuir potestades y facultades que implican los derechos subjetivos, así como cumplir deberes jurídicos. Esa aptitud para ser titular de derechos y obligaciones se denomina capacidad jurídica, y persona es todo ser con capacidad jurídica"[17].

¿Cuáles son los caracteres de las personas jurídicas?

Debemos destacar que el punto de partida de reconocimiento no es el mismo que el de la persona humana. La persona posee personalidad con su sola existencia, por su propia naturaleza humana, mientras que la persona jurídica encuentra, en todas menos en las simples asociaciones, y las sociedades no constituidas regularmente, su existencia subordinada al reconocimiento como tal por parte de la entidad de contralor, en virtud de la inscripción de su instrumento constitutivo.

Asimismo, las personas jurídicas deben cumplir con determinados requisitos en cuanto a su operatividad y actividad misma. Así como hay requisitos, hay limitaciones. Aquí es clave el concepto de especialidad, en tanto se comporta como "una limitación intrínseca a la capacidad de las personas jurídicas; es decir, no la restringe para determinadas especies de actos, sino que les están prohibidos algunos de ellos, cuando se consideren desvinculados de las finalidades de dichas personas"[18].

Hay que tener en cuenta también el concepto de personalidad diferenciada, en tanto "la constitución de una persona jurídica tiene como finalidad primordial crear un nuevo sujeto de derecho con distinto patrimonio y distinta responsabilidad (…) existe una separación entre la personalidad del ente y las personas que lo componen (…)"[19].

¿Cuáles son sus atributos de la personalidad? Tienen nombre, incluso el artículo 151 del CCC les exige tenerlo. Asimismo, deben tener domicilio y sede social. Y, por último, deben tener un patrimonio propio (artículo 154 del CCC).

Chesterman señala que la discusión sobre si se concede o no personalidad jurídica se centra siempre entre razones instrumentales o razones inherentes. Y dice que en el caso de la persona jurídica se utilizan términos que hacen referencia a razones instrumentales[20].

Empero, el reconocimiento de la personalidad jurídica de la persona moral en realidad está en razones inherentes a la misma, en tanto se trata de la protección del ser humano mismo, que mediante la reunión de personas ejerce su derecho a la libertad de reunión y asociación. Se trata de darle seguridad jurídica a este hecho propio de la sociabilidad del hombre, donde el ser humano se reúne con sus pares para alcanzar determinados fines que de manera individual no podría alcanzar. Entonces, no se trata de razones instrumentales, sino inherentes al concepto de persona que analizamos previamente. El concepto de persona esta ínsito e inmerso desde la constitución misma de la persona jurídica. En el caso de la IA la persona solo participa de la creación de la máquina, pero en cuanto a la máquina misma, no hay participación en su actuar de la persona humana y por lo tanto tampoco se ve un despliegue de sus cualidades que le son inherentes.

Mientras que los atributos de la personalidad son un elemento inalienable e imprescindible de las personas físicas, en el caso de las personas jurídicas ellos están habitualmente vinculados a la actividad desarrollada por ellas[21].

c. Otros reconocimientos

En el caso de los animales, su concepción también ha sido fruto de cambio y evolución a lo largo de los años. Se diferencian de la IA, en la medida en que pueden experimentar sentimientos, y a su vez que no pueden llevar a cabo ningún tipo de tarea, mucho menos tareas complejas como lo haría un robot inteligente[22].

En cuanto a los ejemplos correspondientes a la naturaleza que han sido objeto de reconocimiento de personalidad jurídica, nos encontramos con el ejemplo del Parque Nacional Natural los Nevados de Colombia.

Lo que se resalta en el logro de este reconocimiento es el pedido social que existe detrás de este reconocimiento. Son muchos los movimientos sociales que se forman para la protección y preservación del medio ambiente, y por lo tanto generan una presión social que es escuchada y sobre la cual la justicia llega a reflexionar. Si bien podemos pensar que son necesarios grandes movimientos, algunas veces, basta con que una pequeña minoría para el reconocimiento de esta personalidad que está siendo reclamada. De esta forma, "(…) la falta de reconocimiento social es un obstáculo crucial para las personas legales atípicas"[23].

Otro caso especial se dio con Sandra la orangutana. Ella fue reconocida como *persona no humana*. De esta forma, se creó una categoría intermedia, con el uso de la palabra persona, que permitió que, por ejemplo, el animal pudiese contar con representación legal[24].

(13) Chesterman, Simon, "*Artificial intelligence and the limits of legal personality*", *Cambridge University Press for the British Institute of International and Comparative Law*, 2020.

(14) Cfr. Di Pietro, Alfredo, *Derecho Privado Romano*, Buenos Aires, Depalma, Segunda Edición, 2001. Pág. 121.

(15) Tobías, José W., en Alterini, Jorge H. (ed.), *Código Civil y Comercial Comentado*, La Ley, Tomo I.

(16) Dremliuga, Roman; Kuznetcov, Pavel; Mamychev, Alexey, "*Criteria for Recognition of AI as a Legal Person*", *Journal of Politics and Law. Published by Canadian Center of Science and Education*, Volumen 12, Número 3, 2019. Pág. 106.

(17) Gallego-Burín, Marina Rojo, "Los fundamentos históricos del sistema jurídico versus la personalidad electrónica de los robots", *Revista Jurídica de Castilla y León*, Número 52, 2020. Pág. 12.

(18) Rivera, J. C. y Crovi, L. D., *Derecho Civil. Parte General*, 1ª edición, Abeledo-Perrot, Buenos Aires, 2016. Pág. 452.

(19) *Ibid.*, 450.

(20) Cfr. Chesterman, Simon, "*Artificial intelligence and the limits of legal personality*", *Cambridge University Press for the British Institute of International and Comparative Law*, 2020. Pág. 842.

(21) Rivera, J. C. y Crovi, L. D., *Derecho Civil. Parte General*, 1ª edición, Abeledo-Perrot, Buenos Aires, 2016. Pág. 236.

(22) Chesterman, Simon, "*Artificial intelligence and the limits of legal personality*", *Cambridge University Press for the British Institute of International and Comparative Law*, 2020. Pág. 18.

(23) Dremliuga, Roman; Kuznetcov, Pavel; Mamychev, Alexey, "*Criteria for Recognition of AI as a Legal Person*", *Journal of Politics and Law. Published by Canadian Center of Science and Education*, Volumen 12, Número 3, 2019. Pág. 110.

(24) La Asociación de Funcionarios y Abogados por los Derechos de los Animales (AFADA), representada por el abogado constitucionalista Andrés Gil Domínguez, consideró que la situación de *Sandra*, "encerrada en una caja de cemento", era intolerable y acudió a los tribunales para reclamar que dejara de ser considerada "cosa" u "objeto", como establece el Código Civil y Comercial argentino. En marzo de 2015, el asunto llegó al Juzgado Contencioso, Administrativo y Tributario número 4 de la Ciudad de Buenos Aires, dirigido por la juez Elena Liberatori. Y ahí empezó a gestarse una sentencia sensacional. Publicado en: https://elpais.com/elpais/2019/06/17/eps/1560778649_547496.html. Consultada el 21/02/2023.

La conclusión de Conte-Grand era la siguiente: "Se postula, en consecuencia, que el ser humano, en alguna de las etapas de su vida, constituye una instancia evolutiva inferior a la de los monos. ¿Entonces el mono desciende del hombre?".

El 21 de octubre de 2015 se emitió sentencia: *Sandra* fue reconocida como "sujeto de derecho" (no "objeto") y se ordenó al gobierno de la ciudad de Buenos Aires, propietario del zoológico y, por tanto, de la orangutana, que garantizara al animal "las condiciones naturales

Son estos casos especiales que se fueron dando en la realidad los que hacen que muchos autores estén en favor del reconocimiento de la personalidad jurídica de la IA, en tanto el concepto de personalidad parece ser un paraguas que cada vez cubre más cosas o entes distintos de la persona humana.

Las posturas, como veremos, son muy diversas y no existe consenso en la doctrina, hay autores que consideran que la IA no puede ser objeto de reconocimiento de personalidad jurídica, mientras que hay otros que entienden que sí. Asimismo, existen posturas intermedias que proponen el reconocimiento de cierta personalidad jurídica, específica para este tipo de tecnología, que no las asemeje a la persona humana, pero tampoco las prive totalmente de reconocimiento.

V. ¿Cuáles son los elementos/conceptos que trae consigo la inteligencia artificial que hace que nos planteemos la posibilidad de que se le reconozca o atribuya personalidad jurídica?

Antes de analizar las diversas posturas, nos preguntamos por los elementos que trae consigo la IA que hace que nos planteemos hoy la pregunta por su personalidad jurídica. Tiempo atrás fue Alan Turing quien se preguntó ¿pueden las máquinas pensar? Turing, precursor de lo que hoy conocemos como la computadora, creó el test de Turing. Mediante este test, lo que planteó el inventor fue de forma resumida lo siguiente: podemos decir que consistía en que una persona y una máquina tuvieran una conversación, y que una tercera persona tratase de descifrar cuál es el diálogo de la máquina y cuál el de la persona humana. Una vez que esa tercera persona no fuese capaz de hacer esta distinción, es que podemos decir que las máquinas pueden formular respuestas similares a las de los seres humanos, y demostrar esta posibilidad de ocupar su lugar. Según Chesterman, el test de Turing nos lleva a un "(…) debate sobre la personalidad que solemos pasar por alto"[25].

Empero, creemos que este test ha quedado atrás en el tiempo, en tanto lo que deberíamos tratar de encontrar es si las máquinas pueden poseer inteligencia, autonomía, voluntad y libertad. No es lo mismo poder imitar a una persona, que comportarse como tal. Si quisiera recibir el nombre de persona, entonces debe poder desplegar las cualidades inherentes de la misma. Hay dos notas esenciales que caracterizan a la persona, que son el hecho de que es un ser finito y vulnerable, y es en esa existencia donde "(…) la supervivencia es un pilar fundamental de nuestra vida (…) pero con las máquinas no pasa lo mismo"[26].

Es paradójico igualmente el hecho de que lo que nos diferencia de la tecnología es la supervivencia, pero a su vez necesitamos de la tecnología para sobrevivir.

Con referencia a este concepto de imitar, podemos citar también el hecho de que "(…) con la IA se trata de elaborar sistemas capaces de resolver problemas y desempeñar tareas mediante la simulación de procesos intelectuales (…)"[27]. Acá usa el autor la palabra *simular*. Otra forma que nos permite comprender que la esencia del razonamiento en la IA no existe, en la medida que no hay ningún proceso lógico que pueda actuar de manera libre. La tecnología no hace más que imitar, y hacer de cuenta que se trata de un ser humano.

Es que, "(…) después de todo, detrás de la tecnología, hay humanos (…)"[28].

En el año 2020, Facebook se vio en una situación de gran complejidad, y ciertamente preocupante en lo que hace al desarrollo de esta tecnología. Sus investigadores encontraron que el sistema de IA había creado su propio idioma, lo que implicó la eliminación de ese sistema de IA. Este ejemplo de vida real trae preocupación, en tanto estamos ante una IA que parece haber cobrado autonomía, y logró actuar por sí sola.

Quisiéramos detenernos en el concepto de que la IA no hace más que imitar al ser humano. Cuando hablamos de imitación, entendemos que se trata de algo que pretende ser, y no de algo que es. Y hay una gran diferencia entre ese ser y la imitación, en tanto el ser corresponde al ser humano y responde a todas sus cualidades inherentes, y la IA no hace más que tratar de imitar y hacer parecer que puede alcanzar esa misma forma de despliegue en el ordenamiento jurídico. Es decir, dentro de la complejidad que supone un aparato integrado por IA, no existen los conceptos de discernimiento y de libertad, por más complicado y detallista que pueda ser su sistema.

¿Qué sucede cuando la IA es programada para poseer capacidades intelectuales humanas, y "(…) supera en gran medida el rendimiento cognitivo de los seres humanos en prácticamente todos los dominios del saber"?[29] La clave está en el hecho de que la IA es una tecnología programada por el hombre, lo que quiere decir que no nace libre y tiene la posibilidad de por sí misma desarrollar su libertad. Sino que justamente la IA va a trabajar siempre acorde al sistema con el que ha sido programada, lo que hace imposible que digamos que puede tener una voluntad libre. Más precisamente, que no tenga ni voluntad, ni libertad, a pesar de tener una inteligencia avanzada. Se trata de un sistema compuesto de procesos lógicos, lejos de toda posible reflexión sobre lo que hace y la importancia de su despliegue en la vida real.

En el caso de las máquinas, ellas aprenden "(…) de la misma forma que lo hacen la mayoría de los seres humanos: por experiencia. Y en función de ella, brindan respuestas lógicas. Pero nuestra capacidad humana de hacernos preguntas que podrían sonar ilógicas, nos lleva muchas veces a tomar decisiones que cambian el rumbo de la humanidad"[30]. Aquí hay dos palabras que son muy importantes para nuestra investigación, *respuestas lógicas*. La IA no puede más que seguir ese mecanismo y proceso de pensamiento técnico, en virtud de que tiene una programación específica. No tiene la libertad propia del hombre para buscar un rumbo propio, o crear un pensamiento o criterio personal. Siempre, detrás de su actuar, estará la configuración previa que su creador quiso darle.

VI. Posturas a favor de que la IA tenga personalidad jurídica propia

Según Chesterman, se encuentra implícito entre los argumentos de los doctrinarios que defienden esta postura la idea de que al momento de que la IA pasa el test de Turing, "(…) deberían tener derecho a un estatuto comparable al de las personas físicas (…)". Igualmente, este es un autor que parece ir al extremo en algunas de sus reflexiones, en tanto llega a escribir que en base a cómo se ha desplegado el reconocimiento de la personalidad jurídica de las personas jurídicas en la historia, no parecería posible que haya dudas sobre la posibilidad de hacer lo mismo con la IA. Y escribe, "la pregunta más interesante va a ser si en realidad ellas no son las que nos deberían reconocer personalidad jurídica a nosotros"[31].

Para algunos autores, "(…) a nivel teórico no hay barreras legales para darles personalidad jurídica a las máquinas autónomas"[32]. Muchos, como analizamos previamente, se apoyan en el hecho de que los ordenamientos jurídicos se han mostrado a favor del reconocimiento de

---

del hábitat y las actividades necesarias para preservar sus habilidades cognitivas".

La Fiscalía recurrió y el titular del Juzgado número 15 de lo Penal, Gustavo Letner, consideró "extinta" la reclamación a favor de *Sandra*. Pero la Sala Tercera en lo Penal, integrada por tres magistrados, resolvió el 12 de diciembre de 2016 que Letner no había respetado los derechos de los demandantes (la Asociación de Funcionarios y Abogados por los Derechos de los Animales) y consideró que "nada obsta a considerar a este tipo de animales como sujetos de derecho no humanos".

Sandra quedó reconocida como persona no humana. Y se le concedió un recurso de *habeas corpus*, el procedimiento por el que cualquier detenido puede exigir comparecer ante el juez para que este determine sobre la legalidad de su privación de libertad.

En: https://elpais.com/elpais/2019/06/17/eps/1560778649_547496.html. Consultada el 25/07/2022.

(25) Chesterman, Simon, "*Artificial intelligence and the limits of legal personality*", *Cambridge University Press for the British Institute of International and Comparative Law*, 2020.

(26) Vivas, Fredi, *¿Cómo piensan las máquinas? Inteligencia Artificial para humanos*, Ciudad Autónoma de Buenos Aires, Galerna, 2021. Pág. 55.

(27) Merchán Murillo, Antonio, "Retos Regulatorios en torno a la Inteligencia Artificial", *Pensar. Revista de Ciencias Jurídicas*, Número 4, Volumen 23, 2018. Pág. 55.

(28) Vivas, Fredi, *¿Cómo piensan las máquinas? Inteligencia Artificial para humanos*, Ciudad Autónoma de Buenos Aires, Galerna, 2021. Pág. 44.

(29) Núñez, Javier, "IA: experiencias y propuestas de regulación en el derecho comparado", *La Ley*, 2020.

(30) *Ibid.*

(31) Chesterman, Simon, "*Artificial intelligence and the limits of legal personality*", *Cambridge University Press for the British Institute of International and Comparative Law*, 2020.

(32) Dremliuga, Roman; Kuznetcov, Pavel; Mamychev, Alexey, "*Criteria for Recognition of AI as a Legal Person*", *Journal of Politics and Law. Published by Canadian Center of Science and Education*, Volumen 12, Número 3, 2019. Pág. 106.

este instituto a las personas jurídicas, ecosistemas y los animales[33]. Vemos los tintes positivistas y utilitaristas en estos argumentos, que olvidan la realidad que los rodea, en la medida de que nunca se podrían asimilar las razones del reconocimiento de la persona humana, con las de la inteligencia artificial.

VII. Posturas en contra de que la IA tenga personalidad jurídica propia

Silvia Salardi[34] sostiene que reconocerle el estatus de persona a un robot implica brindar una "(…) visión antropomorfizada de la máquina (…)" que no es acertada. La cuestión de la autonomía responde a la voluntad de quien crea el robot, y no al robot en sí mismo. En realidad, la máquina llegará "(…) hasta donde su creador quiere que llegue (…)"[35]. Lo que derriba el argumento que nos dice que hay que conferirle a la IA personalidad jurídica propia, en la medida de que el concepto de autonomía no se condice con el actuar de la máquina, y tampoco la máquina posee libertad sea para decidir, o bien para actuar, en virtud de que responde a aquello para lo cual fue programada.

Como hemos analizado previamente, el reconocimiento del estatuto de persona de la IA implica que a esta nueva forma de tecnología se le reconozcan los mismos derechos y obligaciones que a la persona humana, lo que incluye a los derechos humanos. Es por ello entonces que Gallego-Burín se pregunta si los robots tienen derechos, entre ellos, por ejemplo, a la vida, honor, libertad, dignidad, etc. La respuesta de la autora es contundente, ella expresa lo siguiente: "(…) No. Los robots no poseen ninguno de los derechos que hemos mencionado ut supra. Todos ellos pueden pertenecer a una persona, pero nunca a una máquina (…) los robots y otras máquinas no pueden ser titulares de la dignidad humana ni de los derechos relacionados con esta"[36].

Por otro lado, Lean Lau también expresa su postura contraria, y dice que no cree que sea prudente extender tal reconocimiento a la IA, en la medida en que no existen los elementos de conciencia e intención en sus sistemas tecnológicos[37].

No es el único autor que recurre a este mismo argumento, en la medida de que la IA "(…) no tiene cualidades humanas propias para la personalidad, entre ellas tenemos: la conciencia, sentimientos, intención, deseos, intereses, creatividad, etc. (…)"[38]. Lo único que hacen las máquinas es imitar el comportamiento humano.

Cisneros, por su parte, realiza la siguiente reflexión: "¿Estaríamos diciendo que las máquinas son iguales a nosotros? En mi humilde opinión, esto sería un error pues, sin querer entrar en discusiones morales que son más antiguas que el hombre, un ser vivo no puede ser lo mismo que una máquina por muchas similitudes u otras funciones (…) por tanto, a pesar de que un robot inteligente artificial pueda ser enormemente parecido a una persona física, no solo por su inteligencia o porque adquiera autonomía sino incluso porque físicamente pueda parecer humano, no puede encontrarse en la misma categoría que un humano"[39].

VIII. Posturas ecléctica s

El Parlamento europeo en el año 2017 propuso a la Comisión que "(…) analice 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".

Esta propuesta de parte de la UE demuestra su inclinación a que puede haber una posibilidad de que la IA se pueda volver objeto de una regulación separada e independiente. Independiente en el sentido de que merecería una regulación aislada del de la persona humana, y de los simples objetos, siendo específica a las características y descripciones propias de esta tecnología. En este caso, el Parlamento de la Unión Europea "(…) no deniega la posibilidad de que la IA se pueda volver un sujeto independiente dentro del derecho civil (…)"[40].

El Parlamento propone la categoría de "persona electrónica", lo que llamamos una postura ecléctica en la medida en que podría decirse que es una postura intermedia, que entiende que la IA requiere de un estatus propio, distinto y nuevo dentro del ordenamiento jurídico. Empero, hay que tener mucho cuidado, nos preguntamos: ¿Hay implicancias en el hecho de que usemos la palabra *persona*?

Cisneros explora esta posibilidad, y escribe que "(…) Por un lado, la parte de persona es inadecuado pues comúnmente lo relacionamos con la naturaleza humana del concepto, independientemente de la parte tecnológica (…) y el concepto de electrónica tampoco es del todo adecuado y podría incurrir en errores tales como incluir a un autómata en dicha concepción"[41].

Por otro lado, se encuentran quienes sostienen que, por ejemplo, la IA puede actuar como representante de una persona jurídica[42]. Cabría tener una personalidad jurídica similar a la atribuida a los entes ideales, postura que, en cierto sentido, no se opondría del todo a algunos ordenamientos jurídicos.

Merchan Murillo se pregunta si podría una IA celebrar un contrato por sí misma que sea válido de forma independiente sin la intervención de su creador o programador. En el caso extremo de que la respuesta fuera afirmativa, dice que aquí "(…) se presentan argumentos para 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 a la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente"[43].

IX. Conclusión

La pregunta central de esta investigación se centra en ¿cuál es el estatus que el ordenamiento jurídico debe conferirle a la IA? ¿Podemos decir que es persona? A lo largo de la historia, el concepto de persona ha sido atribuido a entes distintos de las personas humanas, como sucedió con las personas jurídicas, y se dio posteriormente el debate con los animales y los ecosistemas.

(33) Dremliuga, Roman; Kuznetcov, Pavel; Mamychev, Alexey, "*Criteria for Recognition of AI as a Legal Person*", *Journal of Politics and Law. Published by Canadian Center of Science and Education*, Volumen 12, Número 3, 2019. Pág. 106. *If we draw an analogy with environmental features and some potential legal persons, it is necessary for AI to have respect from human. Even famous Turing test has no legal meaning but it indicates that people tend to measure the personhood of a machine with the ability to be recognized by a person.*

(34) Salardi, Silvia, "Robótica e Inteligencia Artificial: retos para el derecho", *Universita degli studi di Milano Bicocca*, enero 2020.

(35) *Ibid*. Pág. 223.

(36) Gallego-Burín, Marina Rojo, "Los fundamentos históricos del sistema jurídico versus la personalidad electrónica de los robots", *Revista Jurídica de Castilla y León*, Número 52, 2020. Pág. 22.

(37) Lean Lau, Pin, "*The Extension of Legal Personhood in Artificial Intelligence*", *Revista de Bioética y Derecho. Perspectivas Bioéticas*, Volumen 46, 2019, 47-66. Pág. 56. *Extending such concept of legal personhood, in the manner that has been bestowed upon Sophia in Saudi Arabia, for instance, raises very complicated questions about human nature, humanity, and will necessitate a reinterpretation of foundational notions of legal personhood. In addition, the examination of the concept of human dignity, which is an integral dimension of personhood, would also need to be reformulated.*

(38) Dremliuga, Roman; Kuznetcov, Pavel; Mamychev, Alexey, "*Criteria for Recognition of AI as a Legal Person*", *Journal of Politics and Law. Published by Canadian Center of Science and Education*, Volumen 12, Número 3, 2019. Pág. 106. The opponents of granting AI a legal personhood have an understandable way of thinking. AI has no critical human qualities for personhood, among them are: consciousness, feelings, intentionality, desires, interests, creaticity or something else. In case if AI shows a behavious that could be an evidence of mentioned qualities, it just menas that autonomous machines *imitates* human behaviour

(39) Cisneros Murugarren, Amaiur, "Robots dotados de Inteligencia Artificial: Su posible personalidad jurídica y responsabilidad por daños", Trabajo de fin de Máster (Máster de acceso al ejercicio de la abogacía) en la Facultad de Derecho de la Universidad Complutense de Madrid, 2021. Pág. 16.

(40) Dremliuga, Roman; Kuznetcov, Pavel; Mamychev, Alexey, "*Criteria for Recognition of AI as a Legal Person*", *Journal of Politics and Law. Published by Canadian Center of Science and Education*, Volumen 12, Número 3, 2019. Pág. 107.

(41) Cisneros Murugarren, Amaiur, "Robots dotados de Inteligencia Artificial: Su posible personalidad jurídica y responsabilidad por daños", Trabajo de fin de Máster (Máster de acceso al ejercicio de la abogacía) en la Facultad de Derecho de la Universidad Complutense de Madrid, 2021. Págs. 19-20.

(42) Melo, Verónica E., "Responsabilidad por daños e Inteligencia Artificial: ¿Vino nuevo en odres viejos?", La Ley, 2021.

(43) Merchan Murillo, Antonio, "Retos Regulatorios en torno a la Inteligencia Artificial", *Pensar. Revista de Ciencias Jurídicas*, Número 4, Volumen 23, 2018. Pág. 5.

En el caso de las personas jurídicas, decimos que está justificada la atribución de la personalidad jurídica, en la medida de que se trata de la unión de personas humanas en ejercicio de su derecho a asociarse, de jerarquía constitucional. Empero, vemos difícil poder prolongar la justificación del otorgamiento de personalidad a las personas jurídicas a la IA. En el caso de la IA, no estamos hablando más que de un bien inmaterial, que es creación del hombre, que, si bien parece comportarse y desplegarse por sí misma, ella es fruto de la invención del hombre y no tiene posibilidad de tener su propia libertad y de reflexionar por sí misma, en virtud de funcionar solo en miras a aquello para lo que fue programada. Lo único que hace la IA es "imitar" al hombre, y no "ser" el hombre.

En otras palabras, no puede ser objeto de reconocimiento del estatus de persona, en virtud de carecer ella de la naturaleza propia del hombre. El ser humano tiene la posibilidad de desplegarse en razón de su propia voluntad, de lo que carece desde el inicio la IA. Si bien la IA parece tener cierta autonomía, al tomar decisiones sin necesidad de pedido propio por parte del ser humano, esa conducta no es más que un resultado de su construcción tecnológica, que incluso solo tendrá una función específica que responda a la intención de su creador. De esta manera, seguimos la postura de los autores que rechazan el reconocimiento de la personalidad jurídica de la IA, en la medida que ella carece de todos los atributos propios del hombre que dan respuesta a su reconocimiento como persona.

De esta manera, no podemos otorgarle a la IA tampoco el estatus de persona no humana, en virtud de todo el desarrollo filosófico que la palabra persona implica por sí misma.

Vemos así cómo nos encontramos ante un gran paradigma, donde no debemos caer en el error de reconocerle a la IA un estatus jurídico que no le corresponde. Si caemos en las explicaciones utilitaristas del concepto de persona, entonces perderemos lo más fundamental del derecho, que es su correspondencia con aquello que resulta propio de la naturaleza humana, su respeto y su reconocimiento.

X. Bibliografía

Alterini, Jorge H. (ed.), *Código Civil y Comercial Comentado*, 11 vols., La Ley, Tomo I.

Chesterman, Simon, "*Artificial intelligence and the limits of legal personality*", *Cambridge University Press for the British Institute of International and Comparative Law*, 2020.

Cisneros Murugarren, Amaiur, "Robots dotados de Inteligencia Artificial: Su posible personalidad jurídica y responsabilidad por daños", Trabajo de fin de Máster (Máster de acceso al ejercicio de la abogacía) en la Facultad de Derecho de la Universidad Complutense de Madrid, 2021.

Di Pietro, Alfredo, *Derecho Privado Romano*, Buenos Aires, Depalma, Segunda Edición, 2001.

Dremliuga, Roman; Kuznetcov, Pavel; Mamychev, Alexey, "*Criteria for Recognition of AI as a Legal Person*", *Journal of Politics and Law. Published by Canadian Center of Science and Education*, Volumen 12, Número 3, 2019.

Gallego-Burín, Marina Rojo, "Los fundamentos históricos del sistema jurídico versus la personalidad electrónica de los robots", *Revista Jurídica de Castilla y León*, Número 52, 2020.

González Enric, "Sandra, la orangutana que se convirtió en persona", 2019. Disponible en el siguiente link: https://elpais.com/elpais/2019/06/17/eps/1560778649_547496.html. Consultada el 25/07/2022.

Hervada, Javier, "¿Qué es el derecho? La moderna respuesta del realismo jurídico. Una introducción al derecho", EUNSA, Ediciones Universidad de Navarra, S.A. Pamplona, Tercera edición, 2011. Disponible en: https://dadun.unav.edu/bitstream/10171/56682/1/03-Qué%20es%20el%20derecho.pdf, p. 78. Consultada el 22/02/2023.

Lean Lau, Pin, "*The Extension of Legal Personhood in Artificial Intelligence*", *Revista de Bioética y Derecho. Perspectivas Bioéticas*, Volumen 46, 2019, 47-66.

Melo, Verónica E., "Responsabilidad por daños e Inteligencia Artificial: ¿Vino nuevo en odres viejos?", La Ley, 2021.

Merchán Murillo, Antonio, "Retos Regulatorios en torno a la Inteligencia Artificial", *Pensar. Revista de Ciencias Jurídicas*, Número 4, Volumen 23, 2018.

Núñez, Javier, "IA: experiencias y propuestas de regulación en el derecho comparado", *La Ley*, 2020.

Rivera, J. C. y Crovi, L. D., *Derecho Civil. Parte General*, 1ª edición, Abeledo-Perrot, Buenos Aires, 2016.

Salardi, Silvia, "Robótica e Inteligencia Artificial: retos para el derecho", *Universita degli studi di Milano Bicocca*, enero 2020.

Torres Manrique, Jorge I., "Análisis de la relación entre la inteligencia artificial y el derecho. Hacia el arribo del derecho de los robots", Editorial Astrea.

Vivas, Fredi, *¿Cómo piensan las máquinas? Inteligencia Artificial para humanos*, Ciudad Autónoma de Buenos Aires, Galerna, 2021.

VOCES: DERECHO - TECNOLOGÍA - INTERNET - INTELIGENCIA ARTIFICIAL - INFORMÁTICA - ESTADO - DERECHOS Y GARANTÍAS CONSTITUCIONALES - DERECHOS HUMANOS - PODER JUDICIAL - ECONOMÍA - CONSTITUCIÓN NACIONAL - CÓDIGO DE ÉTICA - JUECES - ABOGADO - PROFESIONES LIBERALES - FILOSOFÍA DEL DERECHO - SENTENCIA - JUSTICIA - ACCESO A LA JUSTICIA - PROTECCIÓN DE DATOS PERSONALES - TRATADOS INTERNACIONALES