Año LXI

[AGOSTO DE 2022 - NRO. 8]

DERECHO, INNOVACIÓN & DESARROLLO SUSTENTABLE

REVISTA DE DOCTRINA Y JURISPRUDENCIA

Director: Dr. Emiliano E. Lamanna Guiñazú
Coordinadoras: Matilde Pérez - Valeria Moreno

60 AÑOS | EL DERECHO

CÁPSULA INTRODUCTORIA

El futuro abrumador

por VALERIA MORENO(*)

Presentamos un recorrido por diversos temas de *interés jurídico* que nos hacen pensar y nos plantean la necesidad adaptar la normativa vigente a los vertiginosos avances tecnológicos.

La *cápsula comentario* que nos acompaña en este número refiere al *sandbox* español y la reciente reforma sucedida en ese país. La *profesora* Mariana Sánchez Caparrós elabora un pormenorizado informe sobre la problemática.

La *cápsula de opinión* a cargo de la *profesora* Karina Salierno que ofrecemos se aboca al fascinante mundo de la *realidad aumentada* o *Metaverso*, donde conviven el *yo real* y el *yo digital* del individuo. Uno de los grandes retos jurídicos consiste en como *unir* ambos mundos bajo el mismo *lazo regulador* de la norma. Un desafío en estos tiempos disruptivos.

El *profesor* José María Sabat Martínez aborda el sistema *free-to-play* de los *videojuegos* y las problemáticas jurídicas que emergen de su *utilización.* Los daños a *consumidores vulnerables*, como es el caso de los *menores de edad* que acceden a este sistema. El autor nos plantea claramente la cuestión y la regulación protectoria de Derecho Comparado. Particularmente en Argentina, y no existiendo regulación específica al respecto, referencia la *normativa protectoria* existente y su aplicación al tema en desarrollo. Con un vasto recorrido sobre la legislación vigente, se brindan herramientas de gran utilidad para abordar la problemática propuesta.

En "Prevención 4.0", los colegas José L. Bettolli y Leonardo L. Pucheta realizan un interesante análisis sobre la necesidad de avanzar hacia una regulación de la implementación de nuevas tecnologías y la *prevención* de las contingencias laborales tales como accidentes de trabajo o enfermedades profesionales. Sostienen la importancia de evaluar los bienes jurídicos a tutelar y los intereses comprometidos, y cuáles son, desde sus perspectivas, los *derechos* e *intereses* fundamentales que requieren protección legal. Nos proponen pensar sobre la importancia de atender a los principios jurídicos rectores, la hermenéutica jurídica, las ramas del derecho comprometidas, el rol del Estado y un enfoque regulatorio necesariamente ético-jurídico.

El colega boliviano, Fabián Espinoza Valencia, nos aproxima a la problemática de los ciberdelitos y la reparación de los daños que se generan, en el marco de la normativa, la jurisprudencia y la doctrina de ese país. Pero, además, *detalla* los *tipos penales* del delito de manipulación informática en el Derecho Comparado, donde puntualiza *comparativamente* la regulación vigente en los países americanos (Argentina, Bolivia, Brasil, Paraguay, Uruguay, entre otros). Realiza un análisis doctrinal exhaustivo del comportamiento de cada criterio de oportunidad reglada en ciberdelitos. Expone la vulneración de los derechos de las víctimas que hace nacer el *derecho a una reparación integral*, y en este aspecto, nos brinda las medidas establecidas según los criterios jurisprudenciales que emanan de la Corte Interamericana de Derechos Humanos.

Finalmente, un interesante comentario sobre los aspectos más destacados de la reciente decisión de la Corte Suprema de Justicia de la Nación en el fallo "Denegri N. R. c/ Google Inc" con relación al "derecho al olvido", a cargo de los profesores Carlos A. Fossaceca y Fátima López Poletti.

¡Ansiamos que sean de su interés y disfrute!

VOCES: INFORMÁTICA - INTERNET - DERECHO INTERNACIONAL - ORGANISMOS INTERNACIONALES - DERECHO PENAL INTERNACIONAL - TECNOLOGÍA - DAÑOS Y PERJUICIOS - INTELIGENCIA ARTIFICIAL - DELITOS INFORMÁTICOS - CIBERSEGURIDAD - IMPUTABILIDAD PENAL - DERECHO COMPARADO - DERECHOS Y GARANTÍAS CONSTITUCIONALES - CULTURA - PODER JUDICIAL - ECONOMÍA - RIESGOS DEL TRABAJO - CONTRATO DE TRABAJO - DISCRIMINACIÓN LABORAL - PROPIEDAD INTELECTUAL - DAÑO MORAL - CÓDIGO CIVIL Y COMERCIAL - DERECHO DE AUTOR - TRATADOS Y CONVENIOS - PERSONAS JURÍDICAS - DERECHOS Y GARANTÍAS CONSTITUCIONALES - OBLIGACIONES - PRENSA - LIBERTAD DE PRENSA - HÁBEAS DATA - DERECHO A LA INTIMIDAD - ACTOS Y HECHOS JURÍDICOS - CORTE SUPREMA DE LA NACIÓN - MENORES - ABUSO SEXUAL - VIOLENCIA - DERECHOS INDIVIDUALES - DERECHOS DEL CONSUMIDOR - UNIÓN EUROPEA - CONTRATOS COMERCIALES - RESPONSABILIDAD CONTRACTUAL

CÁPSULA COMENTARIO

El primer piloto de *sandbox* de regulación de inteligencia artificial de la Unión Europea será en España(*)

por Mariana Sánchez Caparrós(**)

Sumario: I. La presentación. – II. Lo que se regula. – III. Sobre los objetivos y sus ulterioridades.

I. La presentación

El pasado 27 de junio la Secretaría de Estado de Digitalización e Inteligencia Artificial de España presentó el piloto de *sandbox* regulatorio de Inteligencia Artificial, con el propósito general de contribuir al desarrollo responsable de este conjunto de técnicas y tecnologías y de mitigar los potenciales riesgos que presenta para la salud, la seguridad y los derechos fundamentales(1).

La jornada de presentación del *sandbox* contó con la participación de funcionarios de la Comisión y del Parlamento Europeos, así como del Gobierno Español, y también con miembros de la industria tecnológica.

Todos ellos tomaron parte en los dos paneles habilitados en los que se debatió brevemente acerca de cómo los *sandboxes* facilitan la mejor implementación de la regulación, y cuáles son las diversas alternativas disponibles para su implementación, en tanto se trata de un esquema de trabajo novedoso(2).

II. Lo que se regula

Ahora, ¿qué es un *sandbox* regulatorio? Si bien no existe una única definición para este concepto, puede decirse que la idea de *sanbox* regulatorio representa la de un espacio de experimentación y exploración, en el que los desarrolladores y la autoridad regulatoria pueden encontrarse para testear sistemas –en este caso, de IA– que aún no han sido probados o desplegados en el mundo real, sin incurrir, en caso de infracción, en las consecuencias previstas en las normas aplicables, pero también con el objetivo de iterar en su aplicación para eventualmente realizar las modificaciones que fueran necesarias.

En el caso del *sanbox* español, se trata de una iniciativa que persigue que las compañías, especialmente las medianas y las *start-ups*, cuenten con un espacio de exploración y experimentación para implementar los requerimientos que surjan del Reglamento de Inteligencia Artificial *–AI Act–* que está siendo debatido en el seno del Parlamento Europeo.

III. Sobre los objetivos y sus ulterioridades

De este modo, se plantean como objetivos del piloto: (i) proveer claridad sobre los nuevos requisitos que se establezcan en la *AI Act* para los sistemas de IA; (ii) transferir conocimientos técnicos de cumplimiento en la implementación de la *AI Act* a las empresas que desarrollan IA; (iii) fomentar la innovación y permitir el desarrollo de sistemas de IA innovadores y confiables; (iv) construir las capacidades e iniciar las consultas que eventualmente den lugar a la creación de la Autoridad de Supervisión Nacional de Algoritmos; (v) experimentar con las futuras obligaciones y requerimientos en un ambiente controlado y proporcionar experiencia práctica de aprendizaje para apoyar el desarrollo de normas, estándares y herramientas a nivel nacional y europeo(3).

En otras palabras, se pretende *conectar* a las empresas con la autoridad regulatoria española para que, de manera conjunta, encuentren la mejor forma de operacionalizar los requerimientos normativos que surjan de la *AI Act*, y así generar *estándares*, *guías* y *herramientas* que sean de uso para España y el resto de Europa(4).

Con ese objetivo, el Gobierno Español invertirá 4.3 millones de euros por los próximos tres años para *desarrollar* este piloto de *sandbox* regulatorio que, como señaló Carmen Artigas, Secretaria de Estado de Digitalización e Inteligencia Artificial, no es solo un proyecto español, sino un proyecto para todos, que pretende darle impulso a la regulación en materia de inteligencia artificial(5).

VOCES: DAÑOS Y PERJUICIOS - COMERCIO E INDUSTRIA - OBLIGACIONES - DERECHOS DEL CONSUMIDOR- UNIÓN EUROPEA - RESPONSABILIDAD CIVIL - ACTOS Y HECHOS JURÍDICOS - CONTRATOS COMERCIALES - RESPONSABILIDAD CONTRACTUAL - ECONOMÍA - DEBER DE INFORMACIÓN - ESTADO - DAÑO - ORGANISMOS INTERNACIONALES - EMPRESA - TECNOLOGÍA - INFORMÁTICA - INTELIGENCIA ARTIFICIAL

(*) El presente trabajo se inscribe en el Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el Profesor Dr. Jorge Nicolás Laferriere, específicamente en el marco del Proyecto titulado: *"El Daño Resarcible frente al emergente alta tecnología - Desafíos e interpretación jurídica del daño indemnizable frente al avance tecnológico, la innovación permanente y el desarrollo sustentable"* que dirigen los Dres. Emiliano Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas.

(**) Abogada (UBA, Diploma de Honor). Magíster en Derecho Administrativo (UA, Diploma de Honor y Diploma de Mérito por Tesis de Derecho Aplicado). Becaria del Programa de Formación Multidisciplinario en Inteligencia Artificial (UBA, IALAB). Doctorando en Ciencias Jurídicas (UCA). Investigo en materia de Inteligencia Artificial, ética e igualdad y no discriminación. Premio Nacional Julio César Cueto Rúa 2017 (Asociación Argentina de Derecho Comparado). Profesora universitaria de grado (UCES). Profesora universitaria de posgrado (Universidad Austral, UBA). Relatora en el Superior Tribunal de Justicia de la Provincia de Tierra del Fuego AeIAS y colaboradora en el Proyecto de Modernización del mismo Poder Judicial. Coordinadora Editorial en LegalTech Seed y de la Revista Legaltech y Derecho 4.0 de IJ Editores. Coconductora de Millennials Hackeando el Derecho, un Podcast sobre Derecho y Tecnología producido por Legaltech Seed Inteligencia Artificial & Derecho, Blockchain e Innovación en Sector Público.

(1) Cfr. "Spain proposes to pilot an Artificial Intelligence Sandbox to implement responsible AI with human-centric approach", p. 1, en https://digital-strategy.ec.europa.eu/en/events/launch-event-spanish-regulatory-sandbox-artificial-intelligence [accedido el 7/7/2022].

(2) Cfr. "Launch event for the Spanish Regulatory Sandbox on Artificial Intelligence", en https://digital-strategy.ec.europa.eu/en/events/launch-event-spanish-regulatory-sandbox-artificial-intelligence [accedido el 7/7/2022].

(3) Cfr. "Spain proposes to pilot an Artificial Intelligence Sandbox to implement responsible AI with human-centric approach", pp. 1 y 2, en https://digital-strategy.ec.europa.eu/en/events/launch-event-spanish-regulatory-sandbox-artificial-intelligence [accedido el 7/7/2022].

(4) Cfr. "Spain proposes to pilot an Artificial Intelligence Sandbox…", p. 1.

(5) Cfr. https://twitter.com/SEDIAgob/status/1541389237093912576.

CÁPSULA OPINIÓN

Reflexiones sobre el metaverso(*)

por Karina Vanesa Salierno(**)

Luego del auge del mundo cripto y de la tecnología Blockchain, los NFT y la IA, los operadores jurídicos nos enfrentamos a un nuevo desafío tecnológico constituido por un mundo totalmente desmaterializado, un *ecosistema digital* en donde todo es posible desde la constitución de la personalidad representada a través de un avatar. ¿Cómo proteger derechos en este universo alternativo de avatares y cómo evitar que se constituya en un nuevo páramo digital?

El avance de "Meta" plantea una *metamorfosis* rápida de Internet y por lo tanto de nuestras vidas. Metaverso(1) es la *contracción* del prefijo griego *meta*, que significa "*más allá*", y *verso*, que significa *universo*. Más allá de la definición etimológica, el metaverso es la fusión de la realidad física y la realidad virtual aumentada. Como en cualquier ecosistema digital, el derecho busca el encuadre jurídico de los nuevos acontecimientos para establecer los parámetros básicos de la protección de los derechos patrimoniales y extrapatrimoniales fundamentales. ¿Cómo se regulan los activos digitales en el caso del patrimonio de una persona fallecida? ¿Cómo se pueden gravar, regular y proteger la adquisición y transmisión de NFT? ¿Qué autoridad fiscal, qué sistema de justicia podría intervenir en el metaverso, dado que no depende de ningún estado por el momento?

El metaverso es una *representación* de la realidad que incluye una idea de civilización, de sociedad, por ello las normas de convivencia social serán primordiales en estas comunidades. Como vimos, el problema de la *identidad* es uno de los fundamentales en el metaverso, ¿es una realidad paralela, es un mundo autónomo, o es otro mundo? La idea de dos mundos incrementa la falta de responsabilidad, la falta de empatía. ¿Podríamos tener otra identidad en el metaverso? ¿Cómo funcionan las reglas de la responsabilidad y la imputabilidad en el metaverso? ¿Es posible sentir físicamente la agresión sexual en el metaverso? Si veo que mi avatar se quema o se muere en el metaverso, ¿cómo me afectará emocionalmente? ¿Me pueden tocar? ¿Puedo sufrir algún tipo de violencia? Obviamente que todo lo que tenga que ver con *niños, niñas* o *adolescentes, que es uno de los tópicos que más me preocupa,* va a encontrarse *vinculado* con una innumerable cantidad de situaciones altamente riesgosas, como el caso del *acoso* virtual o de una posible utilización de las imágenes de los niños, sus datos personales, su historial de interacción, etc. Pero el posicionamiento de esta nueva realidad nos lleva a extender las ulterioridades en los *actos jurídicos* celebrados en este espacio (y su posible incumplimiento), pues este universo puede ofrecerte *lo inimaginable*. Y hay un punto, el cual, según entiendo, debemos cambiar nuestro pensamiento: solíamos decir que los abogados, como operadores jurídicos, debíamos constituirnos en una suerte de *puente* entre estas dos realidades en *aparente* conflicto, lo *digital* y la *realidad*. Hoy no lo pienso así. Partimos de una idea falsa si pensamos que el metaverso y el mundo real son dos espacios a conjugar. La realidad es una y solamente una, y esta debe *reconocerse* ya sea la experiencia en una u otra *realidad*, pues pensando de esta manera no hacemos sino *minimizar* los perjuicios que podemos sufrir en el espacio virtual. Los daños que podemos experimentar en el Metaverso pueden tener la misma experiencia o carga negativa que los que sufrimos en nuestra cotidianidad analógica. Y desde esta idea, lograr plasmar una *derivación* argumentativa sobre los fundamentos y principios donde debemos edificar la *protección* y esto de pensar si nuestro ordenamiento jurídico reúne la hermenéutica necesaria para regular *hechos* y *actos* sucedidos en este espacio que despierta tantas sensaciones encontradas.

Como vemos, el desafío es enorme, tenemos más preguntas que respuestas, pero lo importante es *adentrarnos* en el camino de la investigación de los aspectos ventajosos y desventajosos de esta nueva tecnología, que puede brindarnos *innumerables* beneficios pero que también puede constituirse en vehículo *potenciador* de riesgos para el desarrollo de la personalidad humana y el goce de los derechos fundamentales.

VOCES: DAÑOS Y PERJUICIOS - DERECHO CIVIL - ECONOMÍA - ESTADO - EMPRESA - CÓDIGO CIVIL Y COMERCIAL - TECNOLOGÍA - INFORMÁTICA - FAMILIA - MENORES - ABUSO SEXUAL - VIOLENCIA - HÁBEAS DATA - DERECHOS INDIVIDUALES - ACTOS Y HECHOS JURÍDICOS - CONTRATOS - OBLIGACIONES - INTERNET – INTELIGENCIA ARTIFICIAL

(*) El presente artículo se inscribe en el marco del Programa IUS de Investigación Jurídica Aplicada que comanda el Profesor Doctor Jorge Nicolás Laferriere, específicamente en el marco del proyecto IUS titulado: "El Daño Resarcible frente al emergente Alta Tecnología - Desafíos e interpretación jurídica del daño indemnizable frente al avance tecnológico, la innovación permanente y el desarrollo sustentable" que dirigen los Dres. Emiliano Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas.

(**) Abogada con Orientación en Derecho Notarial, Registral e Inmobiliario (UBA con Diploma de Honor). Acceso a la función notarial por concurso. Notaria Especialista en Contratación y Documentación Notarial (UNA). Profesora de grado y de posgrado (UBA-UNA). Investigadora (UNA). Posgrado Superior en Derecho de Familia, "Retos Actuales de la Filiación", Universidad de Salamanca (USAL). Maestrando en Máster de Derecho de Familia e Infancia de la Universidad de Barcelona (UB); Doctorando en Ciencias Jurídicas (UCA). Autora de libros, artículos de doctrina, participante y ponente en congresos y jornadas.

(1) El término *metaverso* apareció por primera vez en 1992 en la novela *El samurái virtual*, de Neal Stephenson, pero la primera novela de ciencia ficción que imaginaba un mundo virtual digital fue *Simulacron 3*, de Daniel F. Galouye, publicada en 1964. Por aquel entonces, no hablábamos de avatares sino de unidades de identidad, ni de metaverso sino de simuladores de entorno total. En 1997, los franceses crearon el ancestro de Second Life, pero no consiguieron desarrollarlo. No fue hasta 2003 cuando este juego se puso en línea, ofreciendo, como su nombre indica, una segunda vida a los jugadores a través de avatares que se mueven en un universo 3D. El progreso tecnológico aportará entonces su cuota de innovaciones, como el reconocimiento de movimiento con la Xbox 360, luego el reconocimiento de voz en 2017, hasta que en 2021 Mark Zuckerberg rebautizó su empresa Facebook como "Meta".

NOTA A FALLO

Denegri, Natalia Ruth c/ Google Inc. s/derechos personalísimos. Acciones relacionadas (CSJN)(*)

por Carlos Alberto Fossaceca(**) y Fátima López Poletti(***)

I. Introducción

Nos compete en esta oportunidad ponderar de manera sucinta un fallo resuelto el pasado 28 de junio del corriente año por la Corte Suprema de Justicia de la Nación (CSJN) en los autos: *"Denegri, Natalia Ruth c/Google Inc. s/ derechos personalísimos. Acciones relacionadas"* (CIV 50016/2016/CS1) donde se trató el *derecho al olvido*. Este último puede ser definido como *"un derecho a la supresión de determinados datos personales que ya no son necesarios para la finalidad por la que fueron tratados o por el tiempo transcurrido o por ser inapropiados, irrelevantes o desactualizados, y siempre que no exista interés público basado en el derecho a la libertad de expresión, en que sigan siendo conservados"*[1].

Propedéuticamente, es dable aclarar que no resulta ser el supuesto más idóneo para asentar un precedente acerca del derecho al olvido[2]. En efecto, no se trató de una persona privada, desconocida por la opinión pública[3] [4].

La actora, Natalia Ruth Denegri, que en la actualidad se desempeña como *conductora* y *empresaria* de medios, adquirió notoriedad en los años '90 con el caso "Coppola", donde se ventiló un asunto de interés público –tal como la venta de droga y su consumo por parte de famosos– y, por las irregularidades del proceso, se destituyó al magistrado federal que intervino.

La *parte actora* interpuso una pretensión para que se eliminaran ciertos sitios web que daban cuenta de su relación con el referido caso "Coppola". Tuvo acogida favorable en primera instancia y fue confirmada por el tribunal de Alzada, la Sala H de la Cámara Nacional en lo Civil.

Se entendió que el *derecho al olvido* se tornaba una herramienta útil para tutelar los *derechos a la privacidad* y a la *intimidad*, aunque de interpretación restricta. En este sentido, solo se ordenó la supresión del vínculo a los sitios web que exhibieran escenas o imágenes de la actora con contenidos agresivos, de peleas o de que la accionada hablase de su vida privada. No se impuso una prohibición total ante el resguardo del derecho de la sociedad a ser informado y el ejercicio de la libertad de prensa.

II. Aspectos destacados

El pronunciamiento cuenta con elementos relevantes que debemos señalar y puntualizar a los efectos de un desarrollo abreviado y ordenado de lo decidido por el Alto Tribunal.

II.1. Decisión unánime

El primer aspecto sobresaliente radica en que los cuatro magistrados que integran el más Alto Tribunal de la República votaron de manera concordante.

II.2. Importancia de la libertad de expresión y su relación con el derecho al honor y el derecho a la privacidad

La *libertad de expresión* cumple un rol fundamental para el desarrollo de una democracia sana[5] y la formación de una sociedad vigorosa. Tal función explica que

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *Derecho al olvido en Internet*, por Hugo Alfredo Vaninetti, ED, 242-566; *Derecho al olvido en materia disciplinaria laboral*, por Pablo Mosca, EDLA, 2011-B-1155; *La neutralidad y la libertad de expresión e información en Internet*, por Hugo Alfredo Vaninetti, ED, 246-745; *El derecho al olvido en Internet (un fallo del Tribunal de Justicia de la Unión Europea que contribuye a la preservación de la imagen en los entornos virtuales)*, por Guillermo F. Peyrano, ED, 258-918; *La responsabilidad de las entidades financieras y el "derecho al olvido" de la ley de hábeas data*, por Carlos Enrique Llera, ED, 260-624; *La protección de los datos personales en internet: lineamientos que caben deducirse del fallo de la Corte Suprema*, por Esteban Ruiz Martínez, ED, 260-861; *El miedo a Internet*, por Gregorio Badeni, ED, 265-616; *Los diarios online como legitimados pasivos del derecho al olvido. Diferencias entre la Casación belga y la Casación francesa*, por Pablo A. Palazzi, ED, 269-519; *Difusión no autorizada de imágenes íntimas (revenge porn)*, por Pablo A. Palazzi, ED, 266-837; *Derecho a la privacidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales*, por John Grover Dorado, ED, 268-609; *El debate del derecho al olvido en el Brasil*, por Aislan Vargas Basilio, ED, 273-808; *El derecho al olvido en internet frente a la libertad de expresión*, por Verónica Elvia Melo, ED, 288-968; *El derecho al olvido digital ("RTBF 2.0"). La nueva cara de un derecho polémico. A propósito del caso "Denegri"*, por Oscar R. Puccinelli, ED, 289-1033; *El caso "Denegri": una oportunidad para que la Corte Suprema de Justicia recepte el derecho al olvido*, por Marcela I. Basterra, cita digital: ED-MMDCCIII-174; *La "construcción" jurisprudencial del derecho al olvido. A propósito del caso "Denegri"*, por Guillermo J. Borda y Carlos R. Pereira (h.), cita digital: ED-MMDCCIII-175; *¿Hacia un derecho al olvido argentino? Reflexiones previas al caso "Denegri"*, por Enrique H. del Carril, cita digital: ED-MMDCCIII-176; *Derecho al olvido, memoria selectiva y ocultamiento de información pública*, por Carlos José Laplacette, cita digital: ED-MMDCCIII-177; *Las personas públicas también tienen derecho a la autodeterminación informativa. Comentarios sobre "Denegri, Natalia Ruth c. Google INC s/Derechos personalísimos: Acciones relacionadas"*, por María Bibiana Nieto, cita digital: ED-MMDCCIII-178; *¿Derecho al olvido o a la rehabilitación?*, por Germán J. Bidart Campos, cita digital: ED-MMDCCIII-180. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) El presente artículo se inscribe en el marco del Programa IUS de Investigación jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que comanda el Profesor Doctor Jorge Nicolás Laferriere, específicamente en el marco del Proyecto IUS titulado: "El Daño Resarcible frente al emergente Alta Tecnología - Desafíos e Interpretación Jurídica del Daño Indemnizable frente al avance tecnológico, la innovación permanente y el desarrollo sustentable" que dirigen los Dres. Emiliano Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas.

(**) Doctor en Ciencias Jurídicas y Profesor de la Pontificia Universidad Católica Argentina en Obligaciones y Daños y ex profesor a cargo de la cátedra de Derechos Reales de la Usal, Sede Pilar (2019).

(***) Profesora adscripta de la Pontificia Universidad Católica Argentina (UCA) en las asignaturas "Derecho de las Obligaciones" y "Derecho de Daños".

(1) FERNÁNDEZ DELPECH, Horacio, "*Derecho al olvido en Internet*", La Ley Online, TR LALEY AR/DOC/3149/2015, Punto I.

(2) Por el contrario, adoptando una postura distinta: *"se ha perdido una valiosa oportunidad de receptar jurisprudencialmente un instituto de amplio impacto en la vida del ciudadano de a pie y con profuso tratamiento en la jurisprudencia y legislación europea. Seguramente habrá otra oportunidad, aunque no sabemos cuándo: un olvido, con sabor a poco"*, TOMEO, Fernando, *"Olvido con sabor a poco"*, La Ley Online, TR LALEY AR/DOC/2188/2022, Punto III.

(3) El prestigioso constitucionalista Pedro Caminos ha indicado en este aspecto que la resolución judicial del Tribunal Cimero adquiere rasgos *minimalistas*: *"se trata de una sentencia que, por un lado, tuvo en cuenta las peculiaridades del caso que debía resolver. Así, la Corte puso especial énfasis en que la actora era una persona pública y que había adquirido notoriedad por su conexión con una causa judicial que, también por sus características específicas, revestía de un indudable interés público. Esto significa que la negativa a reconocer jurisprudencialmente un derecho al olvido en este caso no se traduce de manera obvia o automática a casos en los que las personas involucradas no sean públicas y en los que la información no tenga conexión alguna con una cuestión de interés público"*, CAMINOS, Pedro A., *"La Corte frente al 'derecho al olvido'. Un ejercicio de minimalismo judicial"*, La Ley Online, TR LALEY AR/DOC/2189/2022, Punto 6.

(4) Acontecimiento diverso a lo ocurrido en el *leading case*: Tribunal de Justicia de la Unión Europea, "Google Spain SL y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (C-131/12)", 13/05/2014, TR LALEY EU/JUR/2/2014. Versó sobre una publicación de una subasta originada por créditos sociales de 16 años de antigüedad.

(5) Ver Considerando 7.

se hayan creado pretorianamente estándares particulares como la doctrina "Campillay" o de la real malicia[6], que dificultan el ejercicio de las acciones resarcitorias. El derecho de expresión debe ser protegido cuando resulta ejercido en el Internet de las cosas, ya sea en su faz individual, ya sea en su faz colectiva[7].

Por su parte, el derecho al honor merece tutela, tal como se prevé en los Tratados Internacionales[8] que ha suscripto la República Argentina y el derecho común[9] patrio lo hace.

Sin embargo, el Tribunal Cimero hace *prevalecer* la libertad de expresión ante el derecho al honor cuando ocurren tensiones entre ellos siempre que se trate de publicaciones acerca de funcionarios, personas públicas o temas de interés público[10].

Se acentúa en mayor medida la protección cuando se trata de hechos verídicos en los cuales el afectado participó de manera voluntaria[11]. Tal es la razón por la cual los miembros del más Alto Tribunal de la República no encontraron violación alguna al derecho de la privacidad[12].

En última instancia, se interpreta que el temor de los magistrados de la Corte Suprema consiste en permitir estándares imprecisos que se basen en criterios subjetivos[13] que impidan el desenvolvimiento eficaz del debate público.

II.3. Papel de los motores de búsqueda

Desempeñan una función de primigenia significación: ser *intermediarios* entre las noticias y el público que las busca a través de procedimientos automatizados[14]. La *indexación* de datos se ha transformado, en consecuencia, en un elemento indispensable para el ejercicio colectivo de la libertad de expresión.

II.4. Categoría sospechosa

Como consecuencia de la interdicción de censura previa que recoge el artículo 14 de la Constitución Nacional, toda restricción a la posibilidad de informar y de expresar opinión resulta ser de interpretación estricta y se transforma en una *categoría sospechosa*[15]. Implica en la práctica que la labor demostrativa, el *onus probandi,* recae sobre quien la invoca[16].

II.5. La orden de desindexar constituye la ultima ratio

La manda judicial que establezca la prohibición de comunicar al usuario los sitios link que contengan los temas que a él le interesan resulta ser muy excepcional. No es de extrañar que se asevere en el Considerando 12 que: *"tal pretensión configura una medida extrema que, en definitiva, importa una grave restricción a la circulación de información de interés público y sobre la que pesa –en los términos antedichos– una fuerte presunción de inconstitucionalidad"*.

Sin embargo, se admite una hipótesis singular que torna viable el *ejercicio* de la *función preventiva* del derecho de daños: la procedencia del bloque de pedidos de búsqueda cuando se acredita la antijuricidad y se constata la *prolongación* de los efectos del nocimiento ocasionado[17].

No obstante, es pertinente indicar que la orden de desindexación puede resultar en cierta medida ineficaz. Verbigracia, el motor de búsqueda de Google trabaja con un *determinismo local*, vincula su funcionamiento con el IP del usuario[18]. Significa que el bloqueo exitoso para un internauta argentino puede no serlo con un europeo.

II.6. Transcurso del tiempo

El mero paso temporal no quita a la noticia el interés que haya tenido para el debate público, aun cuando su contenido se estime inaceptable y ofensivo en la actualidad[19]. Un suceso que versó sobre un tema de interés colectivo, por las graves consecuencias que conllevó, no puede ser sustraído como material de conocimiento o de opinión. Contrariamente, debe permitirse el escrutinio de manera *permanente* y *libre*[20].

Centrándose la atención en el derecho de daños, la prolongación de la noticia en el tiempo no tiñe de antijuricidad a la publicación realizada[21]. Debe acreditarse un vicio del consentimiento del afectado o la inexistencia de la manifestación de voluntad de este último.

II.7. La importancia de la Inteligencia Artificial en el devenir del Alto Tribunal

La reseña anterior de los aspectos más destacados del fallo cuenta con el respaldo de antecedentes resueltos por la misma Corte Suprema de Justicia de la Nación.

Sin embargo, irrumpe en escena en el considerando 23 la figura de la inteligencia artificial, basada en el desarrollo de algoritmo y en la propia capacidad de aprendizaje[22], el *machine learning*.

No se verifica en el apuntado considerando un gran desenvolvimiento de las características de la mentada figura. Se asienta la advertencia que el *crecimiento desmedido* de la Inteligencia Artificial puede significar un cambio en la jurisprudencia merced a los nuevos retos que presenta.

III. Conclusiones

A nuestro entender, el caso Denegri no constituye el ámbito ideal para asentar doctrina sobre el *derecho al olvido*. Por el contrario, las circunstancias de hecho deben versar sobre publicaciones de aspectos privados de las personas.

El norte que ha guiado a los miembros de la Corte Suprema es prohibir o restringir en la medida máxima criterios que debiliten la posibilidad de un vigoroso debate público. La *libertad de expresión* goza de cierta preeminencia respecto al derecho al honor o a la privacidad cuando la publicación atañe temas de *interés público*. Coincidimos con tales predicamentos.

Por otro lado, nos atrevemos a calificar a la doctrina del fallo en ponderación de provisoria: el desarrollo progresivo de la inteligencia artificial, actor de primigenia importancia del siglo XXI, puede acarrear cambios de extrema envergadura en la jurisprudencia del Tribunal, verbigracia, la aceptación de *criterios objetivos* de *imputación* en la responsabilidad de los motores de búsqueda.

IV. Bibliografía y citas (por orden de aparición)

FERNÁNDEZ DELPECH, Horacio, *"Derecho al olvido en Internet"*, La Ley Online, TR LALEY AR/DOC/3149/2015, Punto I.

TOMEO, Fernando, *"Olvido con sabor a poco"*, La Ley Online, TR LALEY AR/DOC/2188/2022, Punto III.

CAMINOS, Pedro A., *"La Corte frente al 'derecho al olvido'. Un ejercicio de minimalismo judicial"*, La Ley Online, TR LALEY AR/DOC/2189/2022, Punto 6.

Tribunal de Justicia de la Unión Europea, "Google Spain SL y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (C-131/12)", 13/05/2014, TR LALEY EU/JUR/2/2014.

(6) Véase para el desarrollo de la libertad de expresión, el robustecimiento de la democracia y la real malicia en la jurisprudencia norteamericana, FOSSACECA, Carlos Alberto (h), *"La real malicia según la jurisprudencia de la Corte Suprema de Justicia de los Estados Unidos (1964-1990)"*, La Ley Online, AR/DOC/3261/2013.

(7) Ver Considerando 9.

(8) Verbigracia, artículos 11 y 13.2.a del Pacto de San José de Costa Rica; 17 y 19.3.a del Pacto Internacional de Derechos Civiles y Políticos; V y XXIX de la Declaración Americana de los Derechos y Deberes del Hombre y 12 de la Declaración Universal de Derechos Humanos.

(9) Por ejemplo, el artículo 52 del Código Civil y Comercial.

(10) Ver Considerando 17.

(11) Considerando 18: Se descarta allí el argumento de la eventual mortificación que pudiera sufrir el involucrado.

(12) Ver Considerando 20.

(13) Por ejemplo, en el considerando 19 se deja de lado la tesitura de la cualidad precoz, indignante, desmesurado o "de poco gusto" de la noticia de interés público. No puede dejarse la apreciación de tales criterios solamente en la sensibilidad subjetiva del juzgador.

(14) Ver Considerando 10.

(15) La "categoría sospechosa" es un criterio jurisprudencial nacido en las sentencias de la Corte Suprema de Estados Unidos que ante restricciones de derechos personalísimos basadas en ponderaciones poco razonables o verosímiles, tal como la raza, hacen presumir su inconstitucionalidad.

(16) Ver Considerando 11.

(17) Considerando 12. Adviértase que la demostración de los derechos personalísimos no debe dejar dudas, se ha recurrido al vocablo *"claro"*.

(18) Véase el trabajo de investigación digno de encomio, MENDER BINI, Susana Eloisa, *"La indexación bajo la lupa: ¿qué sí?, ¿qué no?, ¿tal vez?*, Revista de Doctrina y Jurisprudencia "Derecho, innovación& desarrollo sustentable", Nro 7, junio de 2022, ED-MMMCLII-513.

(19) Ver Considerando 14.

(20) Idem.

(21) Ver Considerando 22.

(22) Véase FOSSACECA, Carlos Alberto (h) y MOREYRA, Pilar, "Aproximaciones a la responsabilidad civil por la utilización de inteligencia artificial y derecho de los robots. Una mirada jurídica", RCyS 2020-VIII, 20.

FOSSACECA, Carlos Alberto (h), *"La real malicia según la jurisprudencia de la Corte Suprema de Justicia de los Estados Unidos (1964-1990)"*, La Ley Online, AR/DOC/3261/2013.

Pacto de San José de Costa Rica; 17 y 19.3.a del Pacto Internacional de Derechos Civiles y Políticos; V y XXIX de la Declaración Americana de los Derechos y Deberes del Hombre y 12 de la Declaración Universal de Derechos Humanos.

MENDER BINI, Susana Eloisa, *"La indexación bajo la lupa: ¿qué sí?, ¿qué no?, ¿tal vez?,* Revista de Doctrina y Jurisprudencia "Derecho, innovación & desarrollo sustentable", Nº 7, junio de 2022, ED-MMMCLII-513.

FOSSACECA, Carlos Alberto (h) y MOREYRA, Pilar, "Aproximaciones a la responsabilidad civil por la utilización de inteligencia artificial y derecho de los robots. Una mirada jurídica", RCyS 2020-VIII, 20.

VOCES: DERECHO CONSTITUCIONAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - CONSTITUCIÓN NACIONAL - INTERNET - INFORMÁTICA - TECNOLOGÍA - PRENSA - LIBERTAD DE PRENSA - HÁBEAS DATA - PERSONA - DERECHO A LA INTIMIDAD - DERECHO CIVIL - DAÑOS Y PERJUICIOS - JURISPRUDENCIA - ACTOS Y HECHOS JURÍDICOS - CORTE SUPREMA DE LA NACIÓN

DOCTRINA

El modelo *free-to-play* y el costo de los videojuegos(*)

por José María Sabat Martínez(**)

I. Introducción

Los *videojuegos* que aplican el sistema *free-to-play* son aquellos que son *gratuitos* al comienzo del juego, pero que presentan la *necesidad* o la *contingencia* de tener que efectuar pagos durante su desarrollo.

El presente estudio comenzará por *describir* las *características* del sistema *free-to-play*. Luego avanzará con un análisis sobre las ventajas económicas que este modelo presenta para los desarrolladores, siguiendo con una descripción de los *problemas jurídicos* que resultan del mismo.

A continuación, se presentarán las guías más elaboradas que se han formulado en materia de *tutela* a los *menores de edad* y a los *consumidores* en relación con el fenómeno estudiado. Esto es, las *propuestas* y *principios* elaborados, tanto en el Reino Unido como por la Red Europea de Protección a los Consumidores.

El desarrollo continuará con una precisa indicación de las *normas argentinas* que se pueden vincular a la cuestión, y concluirá, finalmente, con el análisis acerca de la *aplicabilidad* de los principios de derecho extranjero antes referidos, y su vinculación con la normativa nacional.

II. El modelo *free-to-play*

Originariamente, el negocio de los desarrolladores de videojuegos estaba basado en la percepción de un *pago único*, o bien, en un esquema sustentado en suscripciones periódicas[1].

Últimamente, la situación descrita se encuentra *virando* hacia un esquema distinto, denominado *free-to-play*, que consiste en permitir la *registración* y *uso* gratuitos de los videojuegos[2]. Pero este esquema de negocios también implica que el *desarrollo ulterior* en el juego, o bien el acceso a *ciertas experiencias* de este, solo sean posibles si se paga por ello[3].

Este último aspecto del sistema es conocido como *game-as-a-service*. Implica la comercialización *sucesiva* de *contenidos*. Esto se logra a través de un diseño de negocios plasmado en los videojuegos que *promueve* que los usuarios realicen las llamadas *microtransacciones*. Estas consisten, básicamente, en que los jugadores deban utilizar dinero fiat para poder acceder a objetos *in-game*, esto es, *bienes virtuales* cuya funcionalidad o atractivo es solamente utilizable en un videojuego[4]. Estas *microtransacciones* pueden observarse en todo tipo de

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *La obra de "software" está amparada en la ley de propiedad intelectual Nº 11.723*, por Inés B. Langenauer, ED, 176-415; *El software, ¿obra protegida?*, por Miguel Ángel Emery y Marcelo García Sellart, ED, 176-241; *Aplicación de los tratados y convenios internacionales a los derechos de propiedad intelectual. Marcas, fonogramas, software*, por Miguel Ángel Emery, ED, 177-601; *La patentabilidad del software llamado "Método de Negocio" (Business Method) en los Estados Unidos*, por Jorge D. Pérez Grandi, ED, 189-740; *Contratos informáticos. Provisión de software. Obligación de resultado. Importancia de la etapa precontractual y del deber de información*, por Hugo Alfredo Vaninetti, ED, 229-452; *Contratos de software y consultoría profesional en la República Argentina. Redacción, análisis e implicancias legales*, por Federico Frachia Sabarís, ED, 261-570; *Armando el rompecabezas: la propiedad industrial e intelectual en el nuevo Código Civil y Comercial*, por Marcelo García Sellart, ED, 264-539; *Los derechos de propiedad intelectual en el marco de los ADPIC*, por Bernan Yamile, Revista de Derecho Penal, Tomo 2018, 5; *El uso de software abierto para el análisis de la evidencia digital*, por Pablo A. Palazzi y Gustavo Presman, ED, 267-653; *Aspectos legales del software en la Argentina*, por Luciano Trippetta, ED, 268-773; *Software as a story (Protegible por derecho de autor)*, por Martina Luski, *Derecho, Innovación & Desarrollo Sustentable*, Número 3 - Octubre 2021. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Este artículo fue escrito en el marco del Proyecto de Investigación titulado "Aproximación al fenómeno del Covid-19 desde la perspectiva de la complejidad jurídica. Derecho y Covid-19", realizado en la Universidad del Salvador y dirigido por los Dres. Alfredo Mario Soto y Ramón Bonell Colmenero; también del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA) que dirige el Profesor Dr. Jorge Nicolás Laferriere, específicamente en el marco del Proyecto titulado: *"El Daño Resarcible frente al emergente alta tecnología - Desafíos e interpretación jurídica del daño indemnizable frente al avance tecnológico, la innovación permanente y el desarrollo sustentable"* que dirigen los Dres. Emiliano Lamanna Guiñazú y Matilde Pérez junto a un grupo de destacados juristas.

(**) Abogado. Profesor Titular de Obligaciones Civiles y Comerciales, y de Responsabilidad Civil en la Universidad del Salvador. Miembro del Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA).

(1) Flunger, Robert - Mladenow, Andreas - Strauss, Christine, "The Free-to-play Business Model", en Indrawan - Santiago, M. - Salvadori, I.L.- Steinbauer M., Khalil I.- Anderst-Kotsis, G. (eds.) - "The 19th International Conference on Information Integration and Web-based Applications & Services (iiWAS) ACM Conference Proceedings Series", 2018, pp. 373-379.

(2) Koksal, Ilker, "Video gaming industry & its revenue shift", Forbes, 08/11/2019, rec. en 29/03/2021 en https://www.forbes.com/sites/ilkerkoksal/2019/11/08/video-gaming-industry–its-revenue-shift/?sh=8ac049e663e5.

(3) Anderton, Kevin, "The ongoing controversy of microtransactions in gaming (infographic)", Forbes, 07/03/2018, rec. en 29/03/2021 en https://www.forbes.com/sites/kevinanderton/2018/03/07/the-on-going-controversy-of-microtransactions-in-gaming-infographic/?sh=15eb678d1d9c.

(4) King, Daniel L. - Delfabbro, Paul H.- Gainsbury, Sally M. - Dreier, Michael - Greer, Nancy - Billieux, Joël, "Unfair Play? Video games as explotative monetized services: An examination from a consumer protection perspective", Computers in Human Behavior 101, 2019, pp. 131-143.

videojuegos, incluidos los deportivos, los juegos de rol y los de acción[5].

Algunos ejemplos de bienes *in-game* cuentan con la posibilidad de obtener *nuevas vidas*, o de adquirir la *moneda digital* que se emplea dentro del juego, o bien la de pasar a etapas del entretenimiento que estarían vedadas para quienes no pagan[6].

III. Beneficios económicos del sistema *free-to-play*

El modelo *free-to-play* se expandió aprovechando la posibilidad tecnológica de descargar contenido de la web, junto con el desarrollo de las *apps* para teléfonos móviles[7].

El aspecto *gratuito* del llamado *free-to-play* toma en cuenta la situación de los jugadores que serían reacios a realizar un gasto inicial para un juego que no conocen y quizás a la postre, no les interese por no ser de su agrado[8]. También permite establecer una base más amplia de usuarios que intercambiarán *información* y *experiencias* del juego, lo cual, genera dos verticales importantes para cualquier negocio que pretenda rentabilidad: *visibilidad* y *prestigio*. En tanto que su lado *oneroso* permite *establecer* un régimen de precios *flexible,* altamente convocante para distintos tipos de jugadores. Asimismo, facilita una *segmentación* entre los usuarios, ya que se pueden crear bienes virtuales que resulten ser a la medida de cada tipo de audiencia[9].

Este sistema ha demostrado ser exitoso, tan así es que la mayoría de las ganancias de los desarrolladores provienen de la *comercialización* de bienes *in-game*[10]. En tal sentido, se ha estimado que la industria de los videojuegos obtiene casi 80% de sus ganancias a través del sistema *free-to-play*[11].

Por su parte, existen *distintos* incentivos para que los usuarios paguen por seguir jugando, o bien, para poder jugar mejor o de distinta manera. Entre estos se encuentra el llamado *pay-to-win*, que consiste en la adquisición de elementos de juego que confieren una ventaja competitiva sobre los demás jugadores, llamados *freemium*[12]. También se puede mencionar al *pay-to-fast* (que significaría el pagar con dinero la posibilidad de avanzar más velozmente en el juego) y al *pay-to-progress* (bonificadores temporales de experiencia)[13]. Se ha mencionado asimismo una serie de experiencias que arroja este modelo de entretenimiento, como ser la voluntad de *completar el juego*, el evitar la *frustración* generada por *barreras artificiales* provistas por el programa, la posibilidad de *sociabilizar*, la *identificación* con un personaje del juego, el ansia de *impresionar* a los demás, etc.[14].

IV. Problemas que puede presentar el modelo *games-as-a-service*

El esquema de negocios descripto presenta una potencialidad dañosa, particular: los *menores de edad*. Entre los *aspectos negativos* se han identificado a los siguientes:

1. El sistema se adapta al jugador para promover un mayor consumo: Ello se debe a que el programa sabe más acerca del jugador que el jugador del programa, y por lo tanto, tiene la capacidad de *anticiparse* a las decisiones del jugador. Amén de ello, el programa aprovecha la información obtenida de los jugadores para diseñar productos *a medida* de sus *personalidades* e *intereses*, y para promover su adquisición. Los costos son *adaptados* al deseo de jugar del usuario y a su capacidad de pago[15].

2. El programa *se ajusta* al estado psíquico del usuario: Estos programas también tienen potencialmente la capacidad de *explotar* económicamente las *vulnerabilidades* o *percepciones* erróneas que los jugadores presenten en determinadas condiciones, como, por ejemplo, las dificultades que algunos experimentan *en diferir* una gratificación, o bien, la creencia que uno ya ha invertido demasiado dinero como para abandonar la actividad, o, tal vez, el entendimiento de que un determinado objeto es más valioso si uno es su titular, etc.[16].

3. La propia competencia incita al gasto: Cuando la adquisición de ciertos bienes *in-game* es necesaria para obtener *mejores resultados*, el éxito de los jugadores ya no dependerá tanto de su habilidad, viéndose incentivados a realizar *mayores erogaciones*[17]. Con semejante sesgo, el sistema se orienta a emplear la *presión social competitiva* en contra de los *intereses económicos del usuario*.

Al mismo tiempo, provoca:

a. Adicción y gasto excesivo: Con este diseño personalizado se torna eventualmente posible que el usuario quede envuelto en una situación de *adicción* y de *peligro financiero*, derivado de la comisión de gastos compulsivos[18]. Trataremos de mencionar los posibles *sesgos* que su utilización produce.

b. Información insuficiente: La provisión sucesiva de elementos de juego y a título oneroso suele ser acompañada por una información ambigua o inexistente acerca de cuáles son los costos a largo plazo resultantes de la actividad. Esto implica una evidente asimetría de información entre el diseño del programa y la percepción del usuario. De tal manera, los verdaderos costos de la actividad se van haciendo evidentes cuando los jugadores ya han quedado comprometidos de modo *psicológico* y *financiero*[19]. Asimismo, en algunos juegos existe una información muy limitada acerca de los efectos o beneficios que se sigan de la adquisición de determinados ítems, o acerca de qué es lo que recibirá exactamente un jugador como resultado de una transacción[20].

c. Vulnerabilidad de los menores de edad: Los videojuegos gozan de una enorme popularidad entre los menores de veintiún años. Así, por ejemplo, en los EE. UU se ha señalado que, solo en 2017, el 75% de los jóvenes de entre 14 y 21 años participaron o fueron espectadores de juegos *online*[21]. El usuario menor de edad suele estar más *desprotegido* frente a la manipulación y cuenta con menos recursos como para resistir la presión social. En general, no son totalmente conscientes acerca del *costo* de las *transacciones.* A ello se suma la dificultad de los adultos para comprender la cultura *gamer*, lo que lleva a una *limitación* en las posibilidades de consejo por parte de los mayores[22].

d. Utilización de monedas *in-game*: al no emplearse moneda fiat, el jugador queda expuesto a una sensación de *inmersión* que puede confundirlo acerca de la real relación entre la moneda del juego y el dinero de la vida real[23].

V. Principios adoptados en el Reino Unido

En el Reino Unido, la Office for Fair Trading (OFT) emitió en 2014 una guía de buen uso[24] referida a los videojuegos, tanto los *online* como aquellos a los que se accede mediante una *app*. Allí se enumeran, mediante *ocho principios*, la visión de la OFT acerca del modo en que los videojuegos deberían cumplir con la *normativa protectoria* del consumidor, a saber:

1) De manera previa a que el consumidor comience a jugar, o a que descargue el juego, o a que se registre o que

(5) Federal Trade Commission, "FTC Video Game Loot Box Workshop. Staff Perspective", agosto 2020, rec. en 21/05/2022 en https://www.ftc.gov/system/files/documents/reports/staff-perspective-paper-loot-box-workshop/loot_box_workshop_staff_perspective.pdf.

(6) Ellison, Erik, "The high cost of free-to-play games: Consumer protection in the new digital playground", SMU Law Review, Volumen 7, segundo ejemplar, artículo 7, 2017.

(7) Federal Trade Commission, op. cit.

(8) Allison, op.cit.

(9) Flunger *et al.*, op. cit.

(10) Koksal, op. cit.

(11) Brugat, Marc, "Los videojuegos 'Free-to-play' generan casi el 80% de los ingresos", La Vanguardia, 07/01/2021, rec. en 21/05/2022 en https://www.lavanguardia.com/videojuegos/20210107/6172128/videojuegos-free-to-play-ingresos-warzone-call-of-duty-superdata.html.

(12) García, José, "'Free to play', 'pay to win', 'pay to fast' y demás jerga gamer: qué significan estos términos (explicados con ejemplos)", Xataka, 08/05/2021, actualizado 10/05/2021, rec. en 16/03/2022 en https://www.xataka.com/videojuegos/free-to-play-pay-to-win-pay-to-fast-demas-jerga-gamer-que-significan-estos-terminos-explicado-ejemplos.

(13) García, op. cit.

(14) Flunger, *et al.*, op. cit.

(15) King, *et al.*, op. cit.

(16) King, *et al.*, op. cit.

(17) Dariani, Omeed; Breyault, John; Fox Johnson, Ariel. Citados por Federal Trade Commission, op. cit.

(18) King, *et al.*, op. cit.

(19) King, *et al.*, op. cit.

(20) King, *et al.*, op. cit.

(21) Guskin Emily, "Teenagers are fueling a competitive gaming tidal wave", Washington Post, 09/03/2018, rec. en 07/06/2021 en https://www.washingtonpost.com/news/sports/wp/2018/03/09/teenagers-are-fueling-an-e-gaming-tidal-wave.

(22) Domoff, Sarah; Fox Johnson, Ariel. Citados por Federal Trade Commission, op.cit.

(23) Federal Trade Commission, op.cit.

(24) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf (16/3/2022).-

realice una adquisición, se le debe brindar información *clara, precisa* y *visible* acerca del costo total, incluyendo: a) el costo inicial para acceder al juego; b) de cualquier otro costo que sea inevitable si el consumidor desea seguir jugando, así como los costos adicionales, tales como las compras de bienes *in-game*; c) en el caso que un costo no pudiere ser razonablemente calculado, se deberá señalar su naturaleza y el modo en que se realiza su cálculo.

2) En las mismas situaciones descriptas en el principio anterior, al proveedor se le deberá suministrar la información concerniente a las *características* del juego y de cualquier *otro elemento* necesario para que el consumidor promedio pueda tomar una decisión informada. Ello incluye: a) una breve descripción del producto; b) cuando fuere relevante, los datos que corresponden a la funcionalidad del contenido digital (por ej., lenguaje, duración, tipo de archivo, tamaño, resolución, actualizaciones, conectividad con Internet y restricciones geográficas); c) cuando tuviere relevancia, la compatibilidad del producto con el hardware y el software respecto del cual el proveedor razonablemente puede esperar que sea empleado; d) dependiendo del contexto, la información debe hacer saber si el juego contiene técnicas de marketing; e) los términos y condiciones relevantes, como –por ejemplo– los mecanismos de cancelación de cualquier tipo de suscripción; f) cualquier tipo de restricciones a los mecanismos de cancelación una vez que ha comenzado la descarga; g) cómo y con qué finalidad se recolecta información personal y cómo es que esta será procesada; h) si el juego contiene algún elemento social o si prevé un modo en el cual el jugador entre en contacto con otros jugadores.

3) La información acerca del negocio subyacente al videojuego debe ser suministrada de un modo claro, preciso y notorio, antes de que el consumidor comience a jugar, o que descargue el juego o a que se suscriba o realice una compra. Debe informarse claramente a quién deberá contactar el consumidor para el supuesto en que requiera realizar consultas, quejas o en que busque satisfacer un derecho. El proveedor debe poder ser contactado rápidamente, en un modo directo y efectivo. El consumidor debe poder acceder a esta información a través de un mecanismo que no sea transitorio.

4) La promoción de cualquier contenido pago, o la promoción de cualquier otro producto o servicio debe ser clara y distinguible del juego en sí mismo. El lenguaje, la presentación y la estructura del juego deben tener presente que, cuanto más joven sea el usuario, mayor será el impacto de dichas prácticas.

5) Un juego no debe confundir a los consumidores, dándoles la falsa impresión de que se deben realizar pagos o de que estos son parte integral del juego, cuando esto no fuere así.

6) Un juego no debe incluir prácticas agresivas, o que potencialmente puedan explotar la inexperiencia propia de un niño, su vulnerabilidad o credulidad.

7) Un juego no debe contener exhortaciones directas dirigidas a niños en las que se los incite a realizar una compra o que se persuada a otros a realizar la adquisición por ellos.

8) No se deben realizar débitos no autorizados de la cuenta del consumidor. Un debito no autorizado es aquel que se efectúa sin que medie un consentimiento expreso e informado del titular de la cuenta. La amplitud del acuerdo y la suma a debitar deben ser claras. El *consentimiento* no debe ser presupuesto (por ej., a través de sistemas *opt-out*), sino que debe ser expresado positivamente. Los proveedores deben asegurar que, en cada operación, el consumidor explícitamente reconozca su obligación de pagar.

VI. Perspectiva de la Red Europea de Cooperación para la Protección de Consumidores

Los Estados miembros de la Unión Europea, en el marco de la Red de Cooperación para la Protección de los Consumidores (CPC), en diciembre de 2013 han adoptado las siguientes posiciones en relación a las prácticas antes descriptas:

1. La posibilidad de confusión acerca del empleo de la palabra "gratis"

Se debe evitar utilizar el calificativo de *gratuito*, cuando esto motiva a la confusión acerca de los costos reales.

La posibilidad de confusión *aumenta* cuando la *naturaleza* y *extensión* de la parte gratuita del juego no es indicada de forma *clara, precisa* y *notoria* antes de que el usuario comience a jugar o a descargar el juego o antes de que realice una adquisición (incluyéndose aquí a las compras *in-app*, esto es, las que se realizan dentro de la propia aplicación).

Se deberá informar en aquellos casos en que se emplee dinero real, indicándose la moneda que se utilizará.

El uso de la palabra "gratis", o semejantes términos inequívocos, desprovisto de las calificaciones apropiadas, solo debe ser permitido cuando los juegos sean verdaderamente gratis en toda su extensión, o sea, cuando no exista la posibilidad de realizar compras *in-app*, ni siquiera de forma opcional.

Por el contrario, la palabra "gratis", o semejantes, es tolerable para juegos que no sean totalmente gratuitos; pero ello será así solo si se utilizan las calificaciones apropiadas, que caractericen *notoria* y *claramente* qué elementos son gratuitos y cuáles pueden ser adquiridos. En tales casos, el consumidor debe poder acceder a partes discretas del juego que no requieran adquisiciones. No será gratis el juego en el que el usuario, sin realizar una erogación, no pueda acceder a una parte integral del juego o bien jugarlo de la manera que razonablemente pudiera esperar

2. Exhortaciones a los niños

Los juegos orientados a los niños, o bien aquellos respecto de los cuales los proveedores puedan razonablemente prever que captarán la atención de los menores de edad, no deben contener exhortaciones directas para que el menor de edad realice una compra. Esto incluye a la presión directa sobre el niño y a la motivación tendiente a persuadir a un adulto para que efectúe una adquisición.

Se debe evaluar la presentación y el contenido de los mensajes dirigidos a niños. Las expresiones "comprá ahora" o "realizá una mejora (*upgrade*) ahora" son consideradas como un incumplimiento a lo aquí dicho.

3. Información y consentimiento de compra

Se deberá informar prominentemente lo atinente a los mecanismos de pago (por ej., no se deben emplear hipervínculos (*links*) o páginas de información separadas).

Los mecanismos de pago preconfigurados (*default settings*) no deben permitir que los débitos se realicen sin el consentimiento expreso del consumidor.

4. Indicación del correo electrónico del proveedor

Se debe hacer saber al consumidor a quién debe contactar en caso de consultas o reclamos. Para ello se debe informar el correo electrónico del proveedor. Esta información debe ser fácilmente accesible, clara y exhaustiva. También debe ser oportuna, esto es, debe ser comunicada antes de que el usuario comience a jugar, o a descargar el juego o a previamente a realizar una adquisición.

VII. Perspectiva del derecho argentino

Nuestro país no brinda una regulación específicamente diseñada en relación al sistema *free-to-play*. Sin embargo, existen diversas normativas que pueden resultar aplicables, a saber:

1) La ley 17.011 (recepcionada en la Argentina), aprobatoria del Convenio de París para la Protección de la Propiedad Industrial

El art. 10 bis, inc. 3, apartado 3ero. de la citada ley menciona que se considera competencia desleal a las "*indicaciones o alegaciones cuyo uso, en el ejercicio del comercio, sea susceptible de inducir al público a error sobre la naturaleza, el modo de fabricación, las características, la aptitud en el empleo o la cantidad de las mercancías*".

2) Ley 24.240 de Defensa del Consumidor

El art. 4 dispone: *"El proveedor está obligado a suministrar al consumidor en forma cierta, clara y detallada todo lo relacionado con las características esenciales de los bienes y servicios que provee, y las condiciones de su comercialización. La información debe ser siempre gratuita para el consumidor y proporcionada en soporte físico, con claridad necesaria que permita su comprensión. Solo se podrá suplantar la comunicación en soporte físico si el consumidor o usuario optase de forma expresa por utilizar cualquier otro medio alternativo de comunicación que el proveedor ponga a disposición"*.

3) Ley 26.061 de Protección Integral de Niños, Niñas y Adolescentes

En esta norma encontramos diversos aspectos, tales como son el principio de protección integral (art. 1), el reconocimiento del interés superior del niño, entendiéndose por tal la máxima satisfacción, integral y simultánea de sus derechos (art. 3), el derecho de los menores de edad a no ser sometidos a ninguna forma de explotación económica (art. 9) y el principio de efectividad de los derechos (art. 29).

4) Ley 26.522 regulatoria de los Servicios de Comunicación Audiovisual

Preliminarmente, cabe considerar si los videojuegos están incluidos o no dentro del concepto de servicio de comunicación audiovisual.

Al respecto, cabe referir que las Ciencias de la Comunicación han considerado a los videojuegos como un medio de comunicación de valores socialmente dominantes y como una herramienta didáctica para enseñar todo tipo de conceptos y materias educativas[25]. También se ha sostenido que inducen a los sujetos al consumo o no de determinados productos y al desarrollo de pautas de conducta[26]. En el mismo sentido, se ha argumentado que constituyen una forma narrativa no lineal y un producto cultural[27].

Cabe interpretar que este mecanismo comunicacional encaja dentro de los parámetros de la ley, a tenor de la nota al art. 1, donde se aclara que *"la ley atiende la previsión legal de los servicios de comunicación audiovisual como una realidad más abarcativa que la restringida emergente del concepto de radiodifusión"*.

Siendo así, se torna aplicable el art. 70, que dispone que dispone la veda de contenidos que promuevan o inciten comportamientos perjudiciales para la integridad de niños, niñas y adolescentes.

Asimismo, el art. 81, inc. h, expresa que "*la publicidad destinada a niñas y niños no debe incitar a la compra de productos explotando su inexperiencia y credulidad*".

Tampoco los avisos publicitarios podrán inducir a comportamientos perjudiciales para la salud física o moral de los menores de edad (art. 81, inc. i).

5) El Código Civil y Comercial de la Nación (CCyCN)

En primer lugar, debe destacarse que el deber de obrar de *buena fe* (art. 9), al cual debe sujetarse el *ejercicio de los derechos*, junto con la observancia de la *moral y las buenas costumbres* (art. 10) configuran *principios generales* que la propia normativa CCyCN recepta como tales.

Asimismo, la existencia de *erogaciones sorpresivas* podría resultar en una infracción al art. 987, inc. c), que veda las cláusulas contractuales que, por su *contenido, redacción* o *presentación*, no son razonablemente previsibles.

El art. 1100, por su parte, reitera principios obrantes en el art. 4 de la ley 24.240, y añade que se debe informar toda circunstancia relevante para el contrato.

En tanto, el art. 1101 prohíbe toda publicidad que "*contenga indicaciones falsas o de tal naturaleza que induzcan o puedan inducir a error al consumidor, cuando recaigan sobre elementos esenciales del producto o servicio*" (inc. a) o que induzca al consumidor a comportarse de forma perjudicial o peligrosa para su salud o seguridad (inc. c).

Por su parte, el art. 1107 dispone, en relación a los contratos celebrados a distancia mediante técnicas de comunicación electrónica, que el proveedor debe suministrar al consumidor "*los datos necesarios para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos*".

6) Decreto 274/2019 de Lealtad Comercial

El art. 10 de la ley considera como acto de *engaño* a los que inducen al error sobre la *existencia* o *naturaleza*, *características principales*, *aptitud* para el uso, *calidad*, *cantidad*, *precio*, *condiciones de venta* o *compra*, *disponibilidad*, resultados que pueden esperarse de su utilización y, en general, sobre los atributos, beneficios o condiciones que correspondan a los bienes y servicios.

A su vez, el art. 11 prohíbe la publicidad o propaganda que mediante inexactitudes u ocultamientos pueda inducir a error, engaño o confusión respecto de las características o propiedades, naturaleza, calidad, cantidad, uso, precio, condiciones de comercialización del producto o servicios.

Asimismo, el art. 26, inc. j, señala que la autoridad de aplicación tiene la potestad de "*Verificar el cumplimiento de la obligación de exhibición o publicidad de precios*".

VIII. A modo de conclusión

Como se ha visto, el derecho argentino impone un *deber de obrar* de *buena fe* (en la doble faz de protección, en torno a la creencia y la probidad), de *informar*, la veda de los actos que lleven al *engaño*, *error* y *confusión*, y la prohibición de la publicidad que tienda a sacar provecho de la vulnerabilidad de los menores de edad.

Asimismo, de acuerdo con nuestro derecho, la tutela de los menores de edad debe ser *eficaz*, *integral* y *prioritaria*.

Siendo así, es de entender que los *principios elaborados* por la OFT y la Red de Cooperación para la Protección de los Consumidores no son ajenos ni opuestos a las normas generales vigentes en nuestro país. Por el contrario, cabe considerar que tales desarrollos son consecuencias que se hallan *implícitas* en las leyes argentinas mencionadas.

Finalmente, cabe tener presente lo que fuera expresado por la Cámara Nacional en lo Comercial en el célebre precedente "Kosten". Allí se dijo que "*el derecho comparado puede servir para fundar decisiones justas, basadas en criterios que han recibido aceptación en países con un desarrollo jurídico similar al nuestro*"[28].

De tal manera, entendemos que el modelo *free-to-play* no presenta para el derecho argentino una situación de *vacío legal*, sino que, por el contrario, la normativa nacional ofrece herramientas robustas a la problemática que presenta ese esquema de negocios.

IX. Bibliografía

Flunger Robert - Mladenow Andreas - Strauss Christine, "The Free-to-play Business Model", en Indrawan-Santiago, M. - Salvadori I.L. - Steinbauer M., Khalil I. - Anderst-Kotsis G. (eds.), "The 19th International Conference on Information Integration and Web-based Applications & Services (iiWAS) ACM Conference Proceedings Series", 2018.

Koksal, Ilker, "Video gaming industry & its revenue shift", Forbes, 08/11/2019, rec. en 29/03/2021 en https://www.forbes.com/sites/ilkerkoksal/2019/11/08/video-gaming-industry--its-revenue-shift/?sh=8ac049e663e5.

Anderton, Kevin, "The ongoing controversy of microtransactions in gaming (infographic)", Forbes, 07/03/2018, en https://www.forbes.com/sites/kevinanderton/2018/03/07/the-on-going-controversy-of-microtransactions-in-gaming-infographic/?sh=15eb678d1d9c.

King, Daniel L. - Delfabbro, Paul H. - Gainsbury, Sally M. - Dreier, Michael - Greer, Nancy - Billieux, Joël, "Unfair Play? Video games as explotative monetized services: An examination from a consumer protection perspective", Computers in Human Behavior 101, 2019.

Federal Trade Commission, "FTC Video Game Loot Box Workshop. Staff Perspective", agosto 2020, en 21/05/2022 en https://www.ftc.gov/system/files/documents/reports/staff-perspective-paper-loot-box-workshop/loot_box_workshop_staff_perspective.pdf.

Ellison, Erik, "The high cost of free-to-play games: Consumer protection in the new digital playground", SMU Law Review, Volumen 7, segundo ejemplar, artículo 7, 2017.

Brugat, Marc, "Los videojuegos Free-to-play generan casi el 80% de los ingresos", https://www.lavanguardia.com/videojuegos/20210107/6172128/videojuegos-free-

(25) Morales, Enrique, "El uso de los videojuegos como recurso de aprendizaje en educación primaria y Teoría de la Comunicación", Diálogos de la Comunicación, Nro 80, 2010, rec. en 21/04/2022 en https://dialnet.unirioja.es/servlet/articulo?codigo=3719704.

(26) Marin Díaz Córdoba, Mariana, "Los videojuegos como medio de comunicación didáctica en el seno familiar", Comunicar, 23, 2004, rec. en 21/04/2022 en https://helvia.uco.es/bitstream/handle/10396/14306/marin14.pdf?sequence=1&isAllowed=y.

(27) Gómez García, Salvador, "Videojuegos: el desafío de un nuevo medio a la Comunicación Social", Historia y Comunicación Social, 2007, 12, 71-82, rec. en 21/04/2022 en file:///C:/Users/Usuario/Downloads/19942-Texto%20del%20art%C3%ADculo-19982-1-10-20110603%20(3).PDF.

(28) CNCom. Sala D, 22/03/2018 "Kosten, Esteban c/ Mercado Libre S.R.L. s/ Ordinario", rec. en 01/06/2022 en http://www.aidaargentina.com/jurisprudencia/kosten-esteban-c-mercado-libre-s-r-l-s-ordinario.

to-play-ingresos-warzone-call-of-duty-superdata.html, La Vanguardia, 07/01/2021.

García, José, "'Free to play', 'pay to win', 'pay to fast' en https://www.xataka.com/videojuegos/free-to-play-pay-to-win-pay-to-fast-demas-jerga-gamer-que-significan-estos-terminos-explicado-ejemplos.

Guskin Emily, "Teenagers are fueling a competitive gaming tidal wave", Washington Post, 09/03/2018, en https://www.washingtonpost.com/news/sports/wp/2018/03/09/teenagers-are-fueling-an-e-gaming-tidal-wave (22/4/2022).

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf (16/3/2022).

Morales, Enrique, "El uso de los videojuegos como recurso de aprendizaje en educación primaria y Teoría de la Comunicación", Diálogos de la Comunicación, Nro 80, 2010, en https://dialnet.unirioja.es/servlet/articulo?codigo=3719704 (21/04/2022).

Marin Díaz Córdoba, Mariana, "Los videojuegos como medio de comunicación didáctica en el seno familiar", Comunicar, 23, 2004, en 21/04/2022 en https://helvia.uco.es/bitstream/handle/10396/14306/marin14.pdf?sequence=1&isAllowed=y.

Gómez García, Salvador, "Videojuegos: el desafío de un nuevo medio a la Comunicación Social", Historia y Comunicación Social, 2007, 12, 71-82, en 21/04/2022 en file:///C:/Users/Usuario/Downloads/19942-Texto%20del%20art%C3%ADculo-19982-1-10-20110603%20(3).PDF.

CNCom. Sala D, 22/03/2018, "Kosten, Esteban c/ Mercado Libre S.R.L. s/ Ordinario", rec. en 01/06/2022 en http://www.aidaargentina.com/jurisprudencia/kosten-esteban-c-mercado-libre-s-r-l-s-ordinario.

VOCES: INFORMÁTICA - TECNOLOGÍA - PROPIEDAD INTELECTUAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - CÓDIGO CIVIL Y COMERCIAL - DERECHO COMERCIAL - DAÑO - DERECHO DE AUTOR - TRATADOS Y CONVENIOS - RESPONSABILIDAD CIVIL - ORDEN PÚBLICO - INTELIGENCIA ARTIFICIAL - PERSONAS JURÍDICAS - PRINCIPIOS GENERALES DEL DERECHO - INTERNET - PODER JUDICIAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - CONTRATOS - OBLIGACIONES - ECONOMÍA

Prevención 4.0: una aproximación jurídica. Análisis de soluciones digitales para la prevención de contingencias laborales(*)

por José L. Bettolli(**) y Leonardo L. Pucheta(***)

I. Tecnología y derecho: una relación paradigmática

El avance de la tecnología y su penetración en prácticamente todos los ámbitos de *desarrollo* e *interacción humanos* interpelan a los operadores jurídicos. Es innegable que el derecho se encuentra cruzado en la actualidad por una cantidad de innovaciones tecnológicas que no resultan indiferentes en términos *ético-jurídicos*, pues poseen efectos concretos y son susceptibles de generar beneficios y riesgos ciertos para la persona humana, tanto a título individual como colectivo.

Frente al vertiginoso desarrollo de las tecnologías de la información y la comunicación (TIC), potenciadas por las denominadas tecnologías *emergentes* y *convergentes*, tales como *big data*, la *robótica* y la *inteligencia artificial*, el derecho se encuentra profundamente exigido y movilizado para dar respuestas a problemáticas actuales(1).

En este contexto, se torna necesaria la *evaluación* del objeto de regulación, los efectos que produce y la existencia de bienes jurídicos a tutelar. Luego, dependiendo de la síntesis correspondiente y la ponderación axiológica asociada, el ordenamiento jurídico positivo habrá de asumir una actitud determinada, vale decir, de pasiva legitimación o de activa regulación. La *legitimación pasiva* de las potencialidades tecnológicas disponibles en la actualidad o las previsiblemente disponibles en el corto plazo implica su admisibilidad y tolerancia y la ausencia de una prescripción jurídica. La *regulación activa*, por su parte, supone la promoción o la desestimación de aquellas, según sean valoradas de forma positiva o negativa, respectivamente. Para integrarse al ordenamiento eficazmente, semejante valoración debe ser expresada formalmente en una *norma jurídica*.

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; *Discriminación 4.0: un desafío por abordar desde el derecho del trabajo*, por Iván Gabriel Lupinacci, Revista de Derecho del Trabajo y Seguridad Social, Número 5 - mayo 2022. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) El presente trabajo se inserta en el proyecto denominado "Prevención 4.0", en cuyo marco se desarrolló el *Libro blanco de la tecnología digital en la prevención del riesgo laboral* (en prensa); también del Programa IUS de Investigación Jurídica Aplicada que comanda el profesor doctor Jorge Nicolás Lafferriere, específicamente en Proyecto IUS titulado: "El daño resarcible frente al emergente alta tecnología - Desafíos e interpretación jurídica del daño indemnizable frente al daño 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.

(**) Abogado. Gerente de la Gerencia de Prevención en la Superintendencia de Riesgos del Trabajo.

(***) Abogado. Jefe del Departamento de Programas Preventivos en la Superintendencia de Riesgos del Trabajo.

(1) Julia Inés Imperiale, "El Derecho en la nueva era tecnológica". Disponible en https://repositorio.uca.edu.ar/bitstream/123456789/9679/1/derecho-nueva-era-tecnologica.pdf [Último acceso: 7 de febrero de 2022].

Lo dicho pone de manifiesto que, *grosso modo*, las normas que componen el ordenamiento jurídico positivo expresan una valoración sobre la *conducta humana*. Determinadas conductas son ponderadas positivamente y, por tanto, promovidas por vía reglamentaria. Otras pueden resultar jurídicamente indiferentes y por lo tanto son permitidas y enmarcadas en las *liberalidades* que se deducen del principio de reserva consagrado en el artículo 19 de nuestra Constitución Nacional. Pero, además, existen conductas que son valoradas *negativamente* y por lo tanto son desalentadas e incluso –dependiendo del grado de reproche que ameriten– penadas criminalmente.

El *descubrimiento* del valor o disvalor de la realidad expresado a través de las normas jurídicas se manifiesta situacionalmente, vale decir, en contextos culturales concretos y de modo circunstancial, lo que implica que, más allá del escrutinio de los individuos, el tratamiento normativo de las conductas humanas resulta de la conciencia colectiva de acuerdo con los *procedimientos legislativos* establecidos.

La relación entre los desarrollos tecnológicos y el derecho no es novedosa. De hecho, de unas décadas a esta parte asistimos al ensayo de novedosos marcos teóricos y normas jurídicas para hacer frente a los desafíos de la era de la informática, especialmente a partir de la *aparición de internet* y la *digitalización* de procesos.

En la actualidad, no obstante, advertimos en esta relación notas paradigmáticas, pues es indudable la *centralidad* que las invenciones tecnológicas poseen en cada persona humana desde el inicio de su existencia y durante el desarrollo de toda su experiencia vital, con efectos individuales y comunitarios identificables.

El impacto global de las nuevas tecnologías, por su parte, permite sostener la necesidad de plantear respuestas de alcance planetario, cuestión que se encuentra emparentada con la pretensión de *universalidad* de las *reglamentaciones* instadas para resolver las tensiones de la comunidad humana en la era tecnológica[2].

La *vinculación* actual entre *derecho y tecnología* conlleva, entonces, dos de los elementos que permiten describir nuestra era:

a) la insoslayable influencia de la tecnología en las relaciones sociales, en las relaciones entre lo humano y lo extrahumano y entre los mundos orgánico e inorgánico;

b) y el alcance global de la referida influencia.

Es, por tanto, necesario que el derecho ofrezca pautas apropiadas para el desarrollo humano en el contexto descripto.

II. Determinación del contenido de la reglamentación

Para el desarrollo de análisis y marcos conceptuales idóneos para la adaptación de los ordenamientos a las exigencias de una sociedad en constante *transformación*[3] deben considerarse todas las aristas comprometidas. Ahora bien, no corresponde a una valoración estrictamente jurídica la consideración del impacto de la implementación de desarrollos tecnológicos en la reducción de costos, en el aumento de rentabilidad o la optimización de los procesos involucrados, sino el *descubrimiento* de su idoneidad para satisfacer las demandas concretas de justicia distributiva y conmutativa.

Para proceder a tal valoración, el operador jurídico no debe limitarse a contrastar las alternativas técnicas en cuestión con la normativa vigente. Si bien lo dicho es parte constitutiva de la labor del agente, ceñir el estudio de la cuestión a la faceta *ius positivista* podría limitar el alcance de la ponderación *ético-jurídica* emprendida.

Así las cosas, en orden a determinar el contenido de la reglamentación, es necesario:

- descubrir los bienes jurídicos dignos de protección, y
- echar mano de los principios jurídicos, herramientas hermenéuticas y tuitivas que permiten dotar de coherencia y razonabilidad a las regulaciones promovidas.

Superar la rigidez de las lecturas *exegéticas* y considerar una aproximación dinámica consistente con la velocidad de los cambios y los progresos *tecnocientíficos*, como se verá, no debe redundar en la actitud de legitimación pasiva antes citada, sino en la puesta en crisis de las reglas y solemnidades que podríamos denominar "clásicas" con el objeto de describir el *deber ser* que las motivó oportunamente, su vigencia y razonabilidad en el contexto actual. ¿Por qué era importante la firma? ¿Sigue siendo relevante? ¿Las formalidades de la firma hológrafa oponen mayores garantías frente a las alternativas de las firmas electrónica o digital? ¿Cuál de los medios disponibles ofrece mejores perspectivas para garantizar los derechos e intereses de los sujetos parte?

III. Consideraciones sobre aplicaciones concretas

Nos interesa *particularmente* una serie de aplicaciones concretas de la tecnología disponible, tendientes a prevenir contingencias de origen laboral que impliquen una merma de la capacidad laborativa de los trabajadores. Se trata, en definitiva, de implementar tecnología priorizando la protección de la vida y la salud de los trabajadores por encima de cualquier otro valor involucrado, de modo consistente con la consideración de cada persona humana como un fin en sí mismo y nunca como un medio ordenado a otro fin. Sin embargo, la implementación de medidas preventivas no debe obstar a la protección de otros intereses subjetivos tales como la protección de *datos personales sensibles*, de contar con el consentimiento de las personas involucradas en los términos del artículo 59 del Código Civil y Comercial de la Nación (CCyCN) o de garantizar la *privacidad* y *confidencialidad*, entre otros.

Es así que al momento de *regular* las *nuevas tecnologías*, en el ámbito de la prevención de accidentes de trabajo o enfermedades profesionales, deben considerarse todos los bienes en juego conforme un orden de *prelación específico*. No se trata de llevar adelante un análisis conceptual en abstracto, sino de la evaluación de los intereses comprometidos en relación con las herramientas disponibles en ámbitos específicos.

Puede resultar sencillo conceder que en la consigna de la prevención de daños derivados del trabajo la *protección de la vida y la salud* ocupa un lugar central, de modo que toda medida adoptada en ese sentido debe ordenarse a proteger la *integridad psicofísica* de cada uno de los individuos que conforman la fuerza de trabajo, en consonancia con las previsiones de la Constitución Nacional, los instrumentos convencionales de rango constitucional y el complejo entramado legal del sistema de riesgos del trabajo[4].

Pero, además, la relación de trabajo es ciertamente uno de los ámbitos de interacción social más importantes, comprometiendo el manejo de *información personal* y de *datos sensibles* asociados a la salud de los trabajadores, a sus hábitos o afiliación sindical, por ejemplo. En línea con la protección de la salud y los datos sensibles asociados ha de reconocerse la relevancia de los exámenes médicos en salud, herramientas fundamentales desde la perspectiva preventiva y reparadora, los que deben llevarse a cabo conforme las reglas imperantes en materia de *autonomía de la voluntad* y *consentimiento informado* para actos médicos (art. 59, CCyCN y Ley 26.529).

En el mismo contexto, el manejo de información reservada o de interés comercial para el empleador exige la adecuada preservación de la *confidencialidad* y de bienes derivados tales como el *secreto comercial*.

Todo lo dicho se enmarca, desde ya, en los derechos consagrados en los artículos 14 y 14 bis de la Constitución Nacional, específicamente a trabajar y ejercer toda industria lícita, a ejercer el comercio, a usar y disponer de la propiedad y al aseguramiento de *condiciones dignas* para el trabajador.

IV. Principios jurídicos comprometidos

El contraste de las regulaciones instadas en el marco de la prevención 4.0 con los principios generales del derecho luce fundamental para garantizar su pertinencia. Estos serán origen y fundamento de tales regulaciones y eventualmente contribuirán a resolver dudas en torno al modo

(2) Francisco, *Humana Communitas*. Carta del Santo Padre Francisco al presidente de la Pontificia Academia para la Vida con ocasión del XXV aniversario de su institución. 11 de febrero de 2019. Disponible en https://www.vatican.va/content/francesco/es/letters/2019/documents/papa-francesco_20190106_lettera-accademia-vita.html [Último acceso: 7 de febrero de 2022].

(3) Antonio-Enrique Pérez Luño, "El derecho ante las nuevas tecnologías". Publicado en *El Notario del s. XXI*, ENSXXI N° 41, enero-febrero 2012. Disponible en https://www.elnotario.es/index.php/hemeroteca/revista-41/548-el-derecho-ante-las-nuevas-tecnologias-0-8050094412686392 [Último acceso: 7 de febrero de 2022].

(4) José L. Bettolli y Leonardo L. Pucheta, "La reparación de los siniestros laborales. Consideraciones en torno a la valoración del daño en las Comisiones Médicas". Publicado en SAIJ, 2021. Cita digital: Id SAIJ: DACF210168. Disponible en http://www.saij.gob.ar/DACF210168 [Último acceso: 8 de febrero de 2022].

en que deben ser aplicadas e interpretadas, pues, tal como enseña Ratti, los principios operan como "fuente de inspiración (*ex ante*) y criterio de validez (*ex post*) de todo el ordenamiento jurídico"[5].

Los principios jurídicos satisfacen de esta forma "la triple función de servir como criterio de interpretación de las normas escritas, de colmar las lagunas o vacíos normativos, y de constituir el medio más idóneo para asegurar la unidad dentro de la pluralidad de preceptos que se aplican (…)"[6].

Desde ya, la alusión a los principios para la determinación del contenido de las regulaciones necesarias para la implementación de tecnologías 4.0 no implica desatender otras fuentes del derecho, sino –de hecho– implicarlas a todas en una evaluación robusta que resulte consistente con los bienes particulares y colectivos en juego.

Es así que luce conveniente señalar, en primer lugar, que en el centro de la vida social y jurídica se encuentra la *persona humana*, por lo que el respeto de su *dignidad* constituye uno de los principios centrales de todo el ordenamiento jurídico.

Sin adentrarnos en la compleja problemática del fundamento y contenido del término "dignidad humana"[7], bastará a los efectos del presente acordar respecto del carácter instrumental del derecho, un medio dispuesto para el ser humano. Luce razonable reconocer un valor particular y distintivo en la persona humana que permite diferenciarlo de las cosas y, por tanto que en línea con la máxima *hominum causa omne ius constitutum est*[8], es sensato considerarlo como un fin en sí mismo y como epicentro del ordenamiento jurídico. En el mismo sentido, el principio *pro homine* informa todo el derecho de los derechos humanos[9] y constituye una pauta de interpretación constitucional y convencional insoslayable.

Luego, en la problemática de la *prevención de riesgos* derivados del trabajo, por su parte, advertimos la concurrencia de una variedad de ramas del derecho que se estructuran en torno a principios derivados.

Desde la perspectiva del *derecho del trabajo* debe estarse al *principio protectorio*[10], del cual se deduce el *in dubio pro operario* como desmembración del citado principio *pro homine,* la aplicación de la norma más favorable, la primacía de la condición más beneficiosa, el carácter irrenunciable de los derechos laborales, la no discriminación y la igualdad de trato.

Del *derecho de la salud*, íntimamente ligado a la dignidad humana[11], por su parte, se desprenden los principios de defensa de la *vida* física, *autonomía* y *consentimiento, integridad* psicofísica, *confidencialidad, privacidad, intimidad* y *acceso a la información*.

La prevención de riesgos del trabajo prorrumpe en el ordenamiento jurídico argentino como objetivo primordial del sistema de riesgos del trabajo, auténtico subsistema de la *Seguridad Social,* razón por la cual deben considerarse también principios propios de tal especialidad. Además de expresar la nota de sociabilidad inherente a la naturaleza humana, el complejo plexo normativo de la seguridad social se encuentra cruzado por los principios de *accesibilidad, universalidad* y *gratuidad* en términos prestacionales.

Como subsistema y rama formal de reflexión y ejercicio profesional, el derecho de *riesgos del trabajo* posee principios específicos que también son insoslayables para la evaluación de tecnologías, tales como los principios de *prevención* y *reparación*. Según el primero, las herramientas tecnológicas planteadas deben contribuir a evitar contingencias y, eventualmente, a revertir las secuelas derivadas de aquellas y a la recuperación de las capacidades psicofísicas que se hubieran visto disminuidas.

A su vez, en tanto el Estado nacional y las autoridades locales están implicados, tanto en su faceta legislativa como en la dimensión operativa y de control, deben tomarse en cuenta principios de derecho público, específicamente los propios del *derecho administrativo*. Es así como el principio rector de *interés general*, el principio de *legalidad*, de *proporcionalidad* y de *razonabilidad* juegan un rol fundamental. Ello permitirá el equilibrio entre las ventajas y las cargas de las tecnologías en cuestión, la adecuación entre el medio tecnológico empleado y la finalidad perseguida.

Lo dicho supone, en síntesis, que las tecnologías propuestas deben ser consistentes con los principios reseñados y los intereses asociados.

V. Faceta regulatoria

A partir de lo dicho y considerando las herramientas tecnológicas instadas, se torna necesario avanzar en la propuesta de reglamentaciones concretas. La implementación de innovaciones tecnológicas en los procesos productivos y en la prestación de servicios para la prevención de afecciones a la salud de los trabajadores, desde ya, debe ser consistente con la tradición jurídica vernácula y con la distribución de cargas obligacionales dispuestas en el sistema jurídico argentino, de modo que uno de los aspectos centrales a dilucidar es la pertinencia de crear nuevas obligaciones, de modificar las existentes o de habilitar nuevas formas de cumplimiento.

VI. ¿Cómo regular las tecnologías 4.0?

Los rápidos y profundos cambios sociales motivados por la evolución tecnológica constante ponen de relieve la dificultad de abordarlos legislativamente. Lo dicho se evidencia de la mano de la fragmentación del principio clásico de legalidad, vinculado al "legicentrismo" o "positivismo legalista", característico del escenario jurídico contemporáneo, signado por la constitucionalización y convencionalización de los ordenamientos jurídicos nacionales. La ley ha dejado de ser el centro del sistema jurídico.

La decadencia del legicentrismo y la necesidad de un correlato con la justicia material demandan la integración de los principios generales del derecho, los que se expanden y desarrollan en forma extraordinaria, prevaleciendo sobre las leyes positivas[12].

La opción por explicitar las exigencias de los principios *generales* y *específicos* correspondientes para la aplicación de desarrollos tecnológicos ofrece ventajas reglamentarias concretas, pero debe ser debidamente condicionada. La posibilidad de superar la rigidez de disposiciones *petras* o de complejo e incierto proceso de reforma luce ciertamente compatible con la rápida *transformación tecnológica* y no debe confundirse con normas laxas. Lo que se propone es poner de relieve los principios rectores como fuente y pauta de interpretación de la normativa, pero bajo ningún concepto establecer referencias abstractas con poco o nulo poder prescriptivo.

Otra ventaja de regular por principios es acortar la distancia entre reglamentaciones de alcance territorial amplio y las normas y convicciones locales. Para ello, puede resultar pertinente la incorporación de mecanismos de solución de controversias cuando los principios establecidos pudieran entrar en colisión. Aún más eficiente, aunque no por ello desprovisto de dificultades en términos de afiliación *ius* filosófica, es la jerarquización de los principios aludidos.

VII. Prescripción activa e innovación tecnológica

Hasta este punto se sostuvo:

- que es necesario un derecho para la prevención 4.0;
- que la ponderación ético-jurídica correspondiente debe expresar una actitud reglamentaria activa, conforme el rol prescriptivo del derecho;
- que el contenido de la reglamentación debe ser congruente con los principios generales y específicos aplicables;

(5) Florencia Ratti-Mendaña, "Los principios jurídicos: Revisión histórica y concepción actual desde la perspectiva neoconstitucionalista". *Prudentia Iuris*, N° 79, 2015, págs. 159-184.

(6) Miguel Lico, "Breve estudio de los principios generales del Derecho y de los principios generales del Derecho aplicables y surgidos del Derecho Administrativo". Disponible en https://www.buenosaires.gob.ar/procuracion-general/breve-estudio-de-los-principios-generales-del-derecho-y-de-los-principios#:~:text=Los%20principios%20generales%20del%20Derecho%2C%20son%20el%20origen%20o%20el,naturaleza%20misma%20de%20las%20cosas%20 [Ultimo acceso: 7 de febrero de 2022].

(7) Eduardo Martín Quintana, "Dignidad y deberes humanos". *Prudentia Iuris*, N° 83, junio 2017, pp. 73-94.

(8) Digesto, L. 2, "De statu hominu". 1,5.

(9) "Portal de Belén - Asociación Civil sin Fines de Lucro c/ Ministerio de Salud y Acción Social de la Nación s/ amparo".

(10) Viviana Mariel Dobarro, "El Derecho del Trabajo: Principios generales e institutos fundamentales". Disponible en http://derecho1.sociales.uba.ar/wp-content/uploads/sites/119/2015/04/El-Derecho-del-Trabajo-Principios-generales-e-instituciones-fundamentales3.pdf [Último acceso: 9 de febrero de 2022].

(11) Pedro Tadei (Dir.), *Reflexiones sobre el sistema de riesgos del trabajo. Compendio sistematizado de colaboraciones autorales sobre sus aspectos más significativos*. Ciudad de Buenos Aires, Superintendencia de Riesgos del Trabajo, 2019.

(12) Juan Carlos Cassange, *Los grandes principios del derecho público*, La Ley, Ciudad de Buenos Aires, 2015, p. 157.

- que todo lo dicho debe propender a brindar mayor protección a la salud y la vida de los trabajadores.

El establecimiento de *principios rectores* podrá contribuir al establecimiento de dinámicas de innovación tecnológica seguras, nutriendo y dando consistencia global al cuerpo normativo resultante.

El rol estatal sería ordenador y no limitante de la iniciativa privada, la negociación colectiva o el diálogo técnico con órganos públicos y privados especializados. La función de la normativa instada no sería simplemente permitir o inhibir conductas, sino habilitar y potenciar la innovación y la iniciativa privada en tanto contribuyan al bien común. Se aspira a formulaciones normativas y una hermenéutica que centren su mirada en el bien humano[13], no solo individual, sino también en su faceta comunitaria.

Desde la función pública el dictado de actos administrativos podría replicar una lógica potestativa, habilitando a la *libre implementación* de tecnologías preventivas de acuerdo a los estándares y principios consagrados[14], tomando en cuenta instrumentos de derecho comparado, así como de experiencias y estándares internacionales.

No debe desatenderse tampoco la faceta de control dispuesta en cabeza de las autoridades públicas nacionales y provinciales, por lo que las obligaciones que puedan cumplirse mediante herramientas tecnológicas deberán ser susceptibles de fiscalización efectiva.

VIII. Nuevas tecnologías, sociedad y derechos fundamentales

La *digitalización* y *procesamiento de bases de datos*, las soluciones virtuales tales como el almacenamiento en la nube, la automatización robótica de procesos o la aplicación de inteligencia artificial son todas realidades que impactan en la vida cotidiana de la población y exigen respuestas de parte del derecho. Así como ofrecen oportunidades para mejorar la calidad de vida y para la *innovación*, el *crecimiento económico* y la *sostenibilidad*, presentan simultáneamente nuevos desafíos para el tejido socioeconómico, la seguridad y la estabilidad[15].

Es así que la realidad tecnológica actual pone en crisis instrumentos y nociones legales clásicas y fuerza a la consideración de nuevas expresiones de derechos fundamentales, así como novedosas y sutiles formas de vulneración[16].

La formulación de un derecho para las nuevas tecnologías supone un posicionamiento concreto en términos ético-jurídicos y conlleva presupuestos específicos de corte *ius* filosófico, al turno que supone la superación de las premisas no cognitivistas subyacentes en la ausencia de reglamentación de prácticas o realidades con impacto en la persona humana.

La explosión de desarrollos *tecnológicos, informáticos, telemáticos, de automatización* y *digitalización de procesos* debe ser encausada jurídicamente en orden a preservar el orden público y facilitar el equilibrio entre los intereses económicos y los derechos individuales y de incidencia colectiva. Su implementación debe evidenciarse en un todo consistente con las exigencias ético-jurídicas correspondientes, las que sucintamente procuró presentarse precedentemente y, en definitiva, reflejar una contribución concreta a la promoción del bien humano.

(13) Juan Carlos Cassange. *Op. cit.*, p. 178 y ss.

(14) Similar a tradición regulatoria de órganos especializados en la problemática biotecnológica, tales como UNESCO. Véase, por ejemplo, la "Declaración Internacional sobre los datos genéticos humanos" (1997), la "Declaración Universal sobre el genoma humano y los derechos humanos" (1997) y la "Declaración Universal sobre Bioética y Derechos Humanos" (2005).

(15) Comisión Europea, *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*, del 26 de enero de 2022. Disponible en https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration [Último acceso: 9 de febrero de 2022].

(16) Gobierno de España, Plan de Recuperación, Transformación y Resiliencia. *Carta Española de Derechos Digitales*. Disponible en https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf [Último acceso: 9 de febrero de 2022].

IX. Bibliografía

BETTOLLI, José L. y PUCHETA, Leonardo L. (2021). "La reparación de los siniestros laborales. Consideraciones en torno a la valoración del daño en las Comisiones Médicas". Sistema Argentino de Información Jurídica. Disponible en http://www.saij.gob.ar/DACF210168.

CASSANGE, Juan Carlos (2015). "Los grandes principios del derecho público", La Ley, Ciudad de Buenos Aires.

COMISIÓN EUROPEA (2022). "Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital". Disponible en https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration.

DOBARRO, Viviana Mariel (2015). "El Derecho del Trabajo: Principios generales e institutos fundamentales". Disponible en http://derecho1.sociales.uba.ar/wp-content/uploads/sites/119/2015/04/El-Derecho-del-Trabajo-Principios-generales-e-instituciones-fundamentales3.pdf.

FRANCISCO, *Humana Communitas*. Carta del Santo Padre Francisco al presidente de la Pontificia Academia para la Vida con ocasión del XXV aniversario de su institución. 11 de febrero de 2019. Disponible en https://www.vatican.va/content/francesco/es/letters/2019/documents/papa-francesco_20190106_lettera-accademia-vita.html.

GOBIERNO DE ESPAÑA (2022). Plan de Recuperación, Transformación y Resiliencia. *Carta Española de Derechos Digitales*. Disponible en https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf.

IMPERIALE, Julia Inés (2019). "El Derecho en la nueva era tecnológica". Disponible en https://repositorio.uca.edu.ar/bitstream/123456789/9679/1/derecho-nueva-era-tecnologica.pdf.

LICO, Miguel (2020). "Breve estudio de los principios generales del Derecho y de los principios generales del Derecho aplicables y surgidos del Derecho Administrativo". Disponible en https://www.buenosaires.gob.ar/procuracion-general/breve-estudio-de-los-principios-generales-del-derecho-y-de-los-principios#:~:text=Los%20principios%20generales%20del%20Derecho%2C%20son%20el%20origen%20o%20el,naturaleza%20misma%20de%20las%20cosas%20.

PÉREZ LUÑO, Antonio-Enrique (2012). "El derecho ante las nuevas tecnologías". Publicado en *El Notario del s. XXI*, ENSXXI Nº 41. Disponible en https://www.elnotario.es/index.php/hemeroteca/revista-41/548-el-derecho-ante-las-nuevas-tecnologias-0-8050094412686392.

QUINTANA, Eduardo Martín (2017). "Dignidad y deberes humanos". *Prudentia Iuris*, Nº 83, junio 2017.

RATTI-MENDAÑA, Florencia (2015). "Los principios jurídicos: Revisión histórica y concepción actual desde la perspectiva neoconstitucionalista". *Prudentia Iuris*, Nº 79, 2015.

TADDEI, Pedro (Dir.) (2019). "Reflexiones sobre el sistema de riesgos del trabajo. Compendio sistematizado de colaboraciones autorales sobre sus aspectos más significativos". Ciudad de Buenos Aires, Superintendencia de Riesgos del Trabajo.

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

Nuevo paradigma en criterios de oportunidad aplicados a ciberdelitos y su reparación del daño

Aproximaciones a la problemática en Bolivia(*)

por Fabián Espinoza Valencia(**)

I. Introducción. Principios límite del *ius puniendi*

La facultad *sancionadora* del Estado, conocida como *ius puniendi*, suele ser excesiva y, desde políticas criminales *perfectibles*, incurre en el aforismo: la ley, en ciberdelincuencia, cuando llega, llega tarde y llega mal. Esto debido a la ya conocida aceleración de los paradigmas delictivos que se presentan en el ciberespacio. Como no podía ser de otra manera, la doctrina y jurisprudencia han desarrollado principios límite de ese *ius puniendi*, entre los que se pueden destacar:

- *Principio de utilidad*: en el que se debe aplicar esta facultad sancionadora desde un criterio de necesariedad, considerando que se puede generar un mensaje contraproducente en la sociedad al instaurar una medida exageradamente rigurosa, y que, en cualquier caso, únicamente era necesario imponer una falta moderada para evitar la concurrencia de actos delictivos.

- *Principio de intervención mínima*: compuesta por dos subprincipios: la *subsidiariedad* y la *fragmentariedad*. El primero se desglosa en tres parámetros subsecuentes: primero, la utilización de medios desprovistos de una sanción; segundo, la utilización de sanciones no penales, y tercero, la utilización de sanciones penales. En el segundo, desde una noción de peligrosidad, el derecho penal únicamente intervendrá y sancionará la vulneración más peligrosa de los bienes jurídicos protegidos.

- *Principio de exclusividad:* la tutela de la protección a un bien jurídico protegido deviene de su acepción político-criminal.

- *Principio de humanización de penas:* como reivindicación de la humanización del rigor de las penas del sistema inquisitivo priorizando siempre los derechos humanos.

II. Sistema garantista para el descongestionamiento de la administración de justicia

En el derecho penal, desde los –cuestionados[1]– criterios jurídicos indeterminados como:

- interés público;
- interés social;
- resocialización;
- reinserción;
- intervención mínima.

Se pretende implementar la mejor faceta del sistema *garantista* instaurado en los ordenamientos jurídicos penales iberoamericanos en la búsqueda de *descongestionar* la administración de justicia para, consecuentemente:

- resolver eficazmente el litigio;
- restaurar eficientemente los derechos de la víctima;
- mitigar la carga procesal;
- desarticular la burocracia administrativa judicial y
- reducir la potencial corrupción.

El Ministerio Público que defiende la legalidad y los intereses generales de la sociedad, ejerciendo la acción penal conforme a la normativa vigente, en este cometido, y por ello es quien tiene la *facultad* de abstenerse de promover el proceso judicial penal o de generar el sobreseimiento correspondiente.

III. La no discrecionalidad de la autoridad en la persecución penal

Dicha abstención de ninguna manera está regida por un criterio de *discrecionalidad*[2], sino que resulta como consecuencia directa del cumplimiento de parámetros establecidos por ley, con una doble finalidad:

- facilitar el descongestionamiento del aparato judicial,
- reparar (integralmente) el daño de la/s víctima/s.

Estos últimos apartados precitados son fundamentales para desarrollar la integralidad de la reparación del daño desde criterios jurisprudenciales desarrollados por la Corte Interamericana de Derechos Humanos (CIDH).

Es preciso señalar que, cuando se aborda el criterio de escasa relevancia social, una posible confusión se genera en torno al instituto jurídico de estado de necesidad que responde a otra arquitectura jurídica propia de la fase de imputabilidad del *iter criminis*.

IV. Criterios de oportunidad reglada

En la prosecución e investigación de ilícitos penales, los representantes de la Fiscalía, para optar por determinadas medidas procesales, deben tomar en cuenta:

- circunstancias que permitan comprobar la acusación,
- circunstancias que sirvan para eximir la responsabilidad del acusado, cuando así corresponda.

Surge, así, el instituto jurídico del criterio de oportunidad reglada como una potestad del Ministerio Público para prescindir de la facultad persecutora. La decisión está regida por los parámetros establecidos por la norma desarrollados más adelante.

V. Fenómenos de cibercrimen en los criterios de oportunidad reglada

Es complejo situar una acepción conceptual *unificada* del cibercrimen como fenómeno. Por ello Rodríguez Flo-

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *La víctima del delito informático*, por Hugo Alfredo Vaninetti, ED, 249-700; *Derecho penal internacional. Cooperación judicial internacional en materia penal*, por Juan Pablo Quaranta Costerg, EDPE, 05/2013-5; *Estafa o fraude informático: su tipificación en Argentina*, por Marcelo Alfredo Riquert, EDPE, 11/2014-5; *Los ataques informáticos como actos de agresión en el marco del derecho internacional público*, por Hugo Alfredo Vaninetti, ED, 262-718; *El miedo a Internet*, por Gregorio Badeni, ED, 265-616; *Ciberdelincuencia y abuso sexual de niños. Reflexiones a raíz de dos encuentros internacionales*, por Luis Gustavo Losada, ED, 265-665; *Panorama sobre aspectos de la responsabilidad civil relacionados con los denominados "ataques" a los sistemas informáticos*, por Guillermo Agustín Peyrano, ED, 266-954; *Ransomware: ¿Cómo puede tipificarse este ciberataque a la luz de la legislación penal vigente?*, por Bianca F. Emiliozzi, Derecho, Innovación & Desarrollo Sustentable, Número 4 - Diciembre 2021. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) El presente trabajo se inscribe en el Programa IUS de Investigación Jurídica Aplicada de la Pontificia Universidad Católica Argentina (UCA), que lidera el profesor doctor Jorge Nicolás Lafferriere, específicamente en el marco del Proyecto IUS denominado: "El daño resarcible frente al emergente alta tecnología - Desafíos e interpretación jurídica del daño indemnizable frente al avance tecnológico, la innovación permanente y el desarrollo sustentable", que comandan los Dres. Emiliano Carlos Lamanna Guiñazú y Matilde Pérez.

(**) Abogado (Universidad Católica Boliviana). Máster en derecho digital y ciberseguridad (Universidad de Barcelona). Diplomado en Derecho Procesal Civil y Educación Superior (UMSA). Asesor legislativo del Senado. Docente de Derecho Informático (UCB, UNIFRANZ y EMI). Miembro asociado Internet Society ISOC - Bolivia. Miembro del Consejo de TIC del Estado. Becario en el Simposio de Ciberseguridad de la OEA e INCIBE. Miembro de LACRALO-ICANN e Instituto de Derecho e Inteligencia Artificial, Brasil y asociado de la Federación Iberoamericana de Derecho Informático (FIADI). CEO de ciberjusticia.com.bo. Doctorando en la Pontificia Universidad Católica Argentina (UCA). Contacto personal: fespinoza@ucb.edu.bo.

(1) Cuestionados porque dan lugar a una múltiple interpretación que se contrapone al principio de objetividad.

(2) La discrecionalidad es la facultad que el ordenamiento jurídico otorga a un juez o a un funcionario para que decida según los principios o estándares que considere justificadamente de aplicación ante la indeterminación o el carácter abierto de la norma jurídica a aplicar (Joan MESQUIDA SAMPOL, Universidad de las Illes Balears, España, 2013).

res (2013) señala que el término "cibercrimen" *carecería* de una definición universalmente *homogénea* y aceptada por los especialistas en el área, existiendo acuerdo entre los investigadores en que sería una actividad ilegal realizada mediante el computador. Sin embargo, continúa el autor, habría desacuerdo sobre el lugar en que se ejecuta tal actividad, y tales diferencias se evidenciarían en las definiciones del señalado delito.

Chung lo define como actividades ilegales realizadas a través de computadores que a menudo tienen lugar en las redes electrónicas globales[3].

Power lo define como la *intromisión* sin autorización de un computador[4].

Chawki indica que el computador tiene varios roles en el cibercrimen, pues sirve de objeto, sujeto, herramienta y símbolo. A su vez, sostiene que se diferencia en cuatro formas de los llamados *crímenes territoriales*: permiten un fácil aprendizaje de cómo realizarlos, requieren pocos recursos en comparación con el daño potencial que pueden ocasionar, pueden ser cometidos en una jurisdicción sin necesidad de estar físicamente presentes y a menudo no son claramente identificados como ilegales[5].

Por su parte, Kleve, De Mulder y Van Noortwijk, citados por Rodríguez Flores, señalan la importancia de investigar el *cibercrimen*, por la necesidad de conocer cómo opera, para *diseñar* las investigaciones criminales, por la percepción de que las leyes convencionales no se aplican a este tipo delitos, ya sea por no estar explícitas o por la forma en que se interpreten, y por la insuficiencia de un manejo seguro de la infraestructura que ofrece internet. Enfatizan que este tipo de delitos dependen del conocimiento, en lo que sucede dentro de un *sistema automatizado* y cómo se *estructura*, beneficiándose además de un vacío en la legislación, dada la posibilidad de que la autoridad del Estado pueda estar indeterminada en dicho espacio[6].

Luego, Salom, Chawki, Speer, refiriéndose a los desafíos de la regulación del cibercrimen y a los sujetos amenazados por este, mencionan distintos tópicos, utilizando el término *delito informático*[7], pero refiriéndose principalmente a la *ciberseguridad* en el manejo de datos[8].

También hay quienes hacen sinónimos ambos términos, al señalar que se entiende por *ciberdelito* o *cibercrimen* cualquier infracción punible, ya sea delito o falta, en la que se involucra un equipo informático o internet y en la que el *ordenador, teléfono, televisión, reproductor* de audio o video o *dispositivo* electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito.

En el mismo sentido, homologando, se dice que *delito informático*, *delito cibernético* o *ciberdelito* es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de internet (13º Congreso sobre Prevención del Delito y Justicia Penal, 2005)[9].

De la misma manera hay quien señala genéricamente que la diferencia entre el *delito informático* y el *ciberdelito* es que el primero se vale de elementos informáticos para su perpetración, mientras que el segundo se refiere a una posterior generación delictiva vinculada a las tecnologías de la información y comunicaciones (TIC) en la que interviene la comunicación telemática abierta, cerrada o de uso restringido[10].

Rayón y Gómez sintetizan a diversos autores señalando que los *ciberataques* son una categoría de ilícito más amplia que los *delitos informáticos*, pues los *ciberataques* incluirían conductas criminales que no constituirían delitos, pero que sí serían parte de la criminalidad informática.

De las distintas definiciones recopiladas por Rayón y Gómez[11], se puede ver que numerosos autores e instituciones[12] se refieren y definen distintos conceptos, tales como *delincuencia informática*, *abuso informático*, *criminalidad informática*, *criminalidad mediante computadoras*, *delitos informáticos*, etc., bajo determinados enfoques doctrinales, refiriéndose, más que a una forma específica de delito, a una pluralidad de modalidades delictivas vinculadas de algún modo con los computadores, designando una multiplicidad de conductas ilícitas y no una sola de carácter general, y parece hablarse de *delito informático* cuando nos estemos refiriendo a una de estas modalidades en particular[13].

Es así que se concibe este nuevo fenómeno propio de la ciencia jurídica con acepciones encontradas entre dos escuelas doctrinarias opuestas (confirmatoria y negatoria), que han surgido en el ámbito del cibercrimen, concretando que para la escuela confirmatoria los sistemas de procesamiento, tratamiento y comunicación electrónica de información adquieren relevancia jurídico-penal desde una doble perspectiva: primero, como posible objeto de conducta ilícita (el soporte físico del sistema informático y/o los componentes lógicos) y, segundo, como instrumento que facilita, asegura o agrava los efectos tradicionales[14]. Mientras que la escuela negatoria, bajo el aforismo bíblico *Nihil novum sub sole* ("No hay nada nuevo bajo el sol"), destaca que son los mismos delitos cometidos de diferente manera, con tres características propias de las tecnologías de la información y comunicación: a) inmediatez, b) masividad y c) anonimato, consideradas como la *materia prima*[15].

VI. El comportamiento de los parámetros de criterios de oportunidad reglada en ciberdelitos

Desde la doctrina clásica del sistema garantista penal, están plasmados los ya conocidos criterios de oportunidad reglada. El *quid* radica en realizar un desarrollo analítico neológico-doctrinal del comportamiento de cada parámetro de los criterios de la oportunidad reglada aplicados a ciberdelitos.

Para ello, es necesario establecer, para fines sintéticos, el delito estandarizado por la doctrina contemporánea: el *fraude informático*, que por lo general está vinculado a bienes jurídicos protegidos de orden patrimonial. En la legislación internacional el 96 % de los países de Sudamérica tienen tipificado el ilícito referido al *fraude informático,* con diferente *nomen iuris*, por ello es preciso identificar la política criminal plasmada en el tipo penal de cada legislación en Latinoamérica.

VI.1. Delito de manipulación informática en la legislación comparada

País	Tipo penal
Argentina	**(FRAUDE INFORMÁTICO).** "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o a la trasmisión de datos"[16].

(3) Chung, Wingyan; Chenb, Hsinchun; Changc, Weiping and Chouc, Shihchieh. (2004). "Fighting cybercrime".

(4) Power, R. (2002). "CSI/FBI computer crime and security survey". *Computer Security Issues & Trends* 8 (1) (2002) 1-22.

(5) Chawki M. (2005). "A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy". DROIT-TIC, 11 april 2005.

(6) Kleve, Pieter; De Mulder, Richard; Van Noortwijk, Kees. (2011). "The definition of ICT Crime". *Computer Law & Security Review* 27 (2011) 162-167.

(7) Salom C., Juan (2005). "La investigación del Delito Informático en la Guardia Civil". Colección "Estudios de Derecho Judicial" - CGPJ, 71-2005. Ídem 6. Speer, David L. (2000). "Redefining borders: The challenges of cybercrime". *Crime, Law & Social Change* 34: 259-273, 2000.

(8) Rodríguez Flores, María Eugenia, "América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?", ed. Departamento de Economía de la Universidad de Chile, septiembre, 2013.

(9) Congresos de las Naciones Unidas sobre prevención del delito y justicia penal, DOHA 2015, 1955-2015.

(10) Romeo Casabona, Carlos (2006). "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", en *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Editorial Comares. Granada.

(11) Rayón Ballesteros, María Concepción; Gómez Hernández, José Antonio, "Cibercrimen: particularidades en su investigación y enjuiciamiento", Anuario Jurídico y Económico Escurialense, XLVII (2014) 209-234 / ISSN: 1133-3677, 2014.

(12) Gómez Perals, Ruiz Vadillo, recomendaciones de la OCDE, Consejo de Europa, Ruiz Vadillo, Comité de Ministros del Consejo de Europa, Baón Ramírez, Tiedemann, Sarzana, Callegari, Rodríguez, Téllez Valdés, y otros.

(13) Cavada Herrera, Juan Pablo citando a Rayón y Gómez, 2014: 209-234 en N° SUP:126200 de la Biblioteca del Congreso Nacional de Chile / BCN, 2020.

(14) En revista electrónica de ciencia penal y criminología. RECPC. 01-14, 1999 citado en Sáez Capel, José, "El llamado delito informático no existe", Rayo del Sur, Sucre, 2014.

(15) "Suplemento especial de cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet", Erreius, Buenos Aires, 2018.

(16) La ley 26.388 (sancionada el 4/6/2008) que incorpora al Código Penal argentino un conjunto de ilícitos que se consideran *delitos informáticos*, entre ellos el delito de fraude informático.

Bahamas	Sección 3. (1) Sujeto a la subsección (2), cualquier persona que, sin autorización, a sabiendas haga que una computadora realice cualquier función con el fin de asegurar el acceso a cualquier programa o datos guardados en cualquier computadora será culpable de un delito y estará sujeto en sentencia sumaria a una multa que no exceda los cinco mil dólares o a una pena de prisión por un término que no exceda los seis meses o tanto a la multa como a la prisión y, en el caso de una segunda o subsecuente condena, a una multa que no exceda los diez mil dólares o a prisión por un término que no exceda un año o tanto a dicha multa como a prisión. (2) Si se causa algún daño como resultado de un delito en virtud de esta sección, una persona condenada por el delito estará sujeta a una multa que no exceda los veinte mil dólares o a una pena de prisión por un período que no exceda los tres años o ambas multas y encarcelamiento. (3) A los efectos de esta sección, es irrelevante que el acto en cuestión no esté dirigido a: (a) cualquier programa o datos en particular; (b) un programa o datos de cualquier tipo; (c) un programa o datos almacenados en cualquier computadora en particular. Sección 4. (1) Cualquier persona que haga que una computadora realice cualquier función con el fin de asegurar el acceso a cualquier programa o datos guardados en cualquier computadora con la intención de cometer un delito (ya sea por sí mismo o por cualquier otra persona) para el cual esté aplicable será culpable de un delito. (2) Esta sección se aplicará a un delito que involucre propiedad, fraude, deshonestidad o que cause daños corporales y que sea punible en caso de condena con prisión por un período de no menos de dos años. (3) Cualquier persona culpable de un delito bajo esta sección estará sujeta a una condena sumaria, a una multa que no exceda los diez mil dólares de una pena de prisión por un término que no exceda los tres años o tanto a la multa como a la prisión. (4) Una persona puede ser culpable de un delito bajo esta sección, aunque los hechos sean tales que la comisión de otro delito sea imposible. (5) A los efectos de esta sección, es irrelevante si: (a) el acceso mencionado en la subsección (1) está autorizado o no autorizado; (b) el delito al que se aplica esta sección se comete al mismo tiempo que se asegura el acceso o en cualquier otro momento. Sección 6. (1) Sujeto a la subsección (2), cualquier persona que a sabiendas: (a) asegure el acceso sin autorización a cualquier computadora con el fin de obtener, directa o indirectamente, cualquier servicio informático; (b) intercepte o haga que se intercepte sin autorización, directa o indirectamente, cualquier función de una computadora por medio de un dispositivo electromagnético, acústico, mecánico o de otro tipo; o (c) use o haga que se use, directa o indirectamente, la computadora o cualquier otro dispositivo con el propósito de cometer un delito bajo el párrafo (a) o (b), será culpable de un delito y estará sujeto en sentencia sumaria a una multa que no exceda los diez mil dólares o a una pena de prisión por un término que no exceda los tres años o tanto a la multa como a la prisión y, en el caso de una segunda o posterior condena, a una multa que no exceda de veinte mil dólares o a prisión por un término que no exceda de tres años o tanto a dicha multa como a prisión. (2) Si se causa algún daño como resultado de un delito en virtud de esta sección, una persona condenada por el delito estará sujeta a una multa que no exceda los cincuenta mil dólares o a una pena de prisión por un término que no exceda los cinco años o a ambas multas y encarcelamiento. (3) A los efectos de esta sección, es irrelevante que el acceso o la interceptación no autorizados no estén dirigidos a: (a) cualquier programa o datos en particular; (b) un programa o datos de cualquier tipo; (c) un programa o datos almacenados en cualquier computadora en particular.
Barbados	**9.** Una persona que, a sabiendas, utiliza una computadora para realizar cualquier función con el fin de garantizar el acceso a cualquier programa o datos almacenados en esa computadora o en cualquier otra computadora con la intención de cometer un delito relacionado con la propiedad, el fraude o la deshonestidad es culpable de un delito y está sujeto a una multa de $ 50.000 o la prisión por un período de 5 años o ambos, en caso de condena por acusación.
Bolivia	**(MANIPULACIÓN INFORMÁTICA).** El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días[17].

(17) Contenido en el Código Penal, artículo 363 bis.

Brasil	**(FRAUDE ELECTRÓNICO)** Art. 171 - 2-A. La pena es de prisión, de 4 (cuatro) a 8 (ocho) años, y multa, si el fraude se comete con el uso de información proporcionada por la víctima o por un tercero inducido a error a través de redes sociales, contactos telefónicos o envío de correo electrónico fraudulento, o por cualquier otro medio fraudulento similar[18].
Chile	**Artículo 1°. -** El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo[19].
Colombia	**(ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO).** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Ecuador	**(ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS).** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad[20].
Guyana	**3.** (1) Salvo lo dispuesto en esta sección, una persona que intercepte intencionalmente una comunicación en el curso de su transmisión por medio de un sistema de telecomunicaciones comete un delito y está sujeta en sentencia sumaria a una multa que no exceda los cinco millones de dólares y a prisión por un término no mayor de tres años. (2) Una persona no comete un delito bajo esta sección si ~ (a) la comunicación es interceptada en cumplimiento de una orden emitida por un juez bajo la sección 6; (b) la comunicación no se intercepta en cumplimiento de una orden emitida por un juez en virtud de la sección (), sino por la autoridad de un oficial designado en el caso de una emergencia nacional o en respuesta a un caso en el que la aprobación de una orden es impracticable teniendo en cuenta la urgencia del caso. (3) El Tribunal por el cual una persona es condenada por un delito en virtud de esta sección puede ordenar que cualquier dispositivo utilizado para interceptar una comunicación en la comisión del delito sea decomisado y eliminado como el Tribunal considere adecuado. (4) A los efectos de la subsección (j), se considerará que una comunicación está en curso de transmisión por medio de un sistema de telecomunicaciones en cualquier momento en que se utilice el sistema por medio del cual se está transmitiendo o se ha transmitido la comunicación para almacenar la comunicación de una manera que permita al destinatario recopilarla o tener acceso a ella.
Paraguay	**Art. 175. (SABOTAJE DE SISTEMAS INFORMÁTICOS).** 1° El que obstaculizará un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante: 1. Un hecho punible según el Artículo 174, inciso 1°; o 2. la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable. Será castigado con pena privativa de libertad de hasta cinco años o con multa. 2° En estos casos será castigada también la tentativa[21].

(18) Incluido por Ley N° 14.155 de 2021.
(19) Ley 19.223
(20) Código Orgánico Integral Penal, Artículo 232.
(21) Ley N° 4.439 que modifica y amplía varios artículos de la Ley N° 1.160/97.

Perú	El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social[22].
San Vicente y las Granadinas	**72.** Una persona que de manera fraudulenta cause pérdida de propiedad a otra persona al: (a) cualquier entrada, acceso, alteración, eliminación o supresión de datos; (b) cualquier interferencia con el funcionamiento de un sistema de información; con la intención de obtener una ventaja para sí mismo o para otra persona, comete un delito y está sujeto a una multa que no exceda los diez mil dólares o a una pena de prisión que no exceda los cinco años o tanto a una multa como a una prisión.
Surinam	**Artículo 286** del Código Penal (Fraude informático).
Trinidad y Tobago	**4.** (1) Una persona que, a sabiendas, hace que una computadora realice cualquier función con el fin de garantizar el acceso a cualquier programa o datos almacenados en esa computadora o en cualquier otra computadora con la intención de cometer un delito: (a) que involucre propiedad, fraude, deshonestidad o que cause daño corporal; y (b) que es punible en caso de condena con prisión de más de un año, comete un delito y está sujeto en sentencia sumaria a una multa de quince mil dólares y a prisión por dos años. (2) A los efectos de esta sección, es irrelevante si: (a) el acceso mencionado en la subsección (1) está autorizado o no autorizado; (b) el delito al que se aplica esta sección es (i) cometida al mismo tiempo que se asegura el acceso o en cualquier otro momento; y (ii) punibles de forma sumaria o acusatoria.
Uruguay	**ARTÍCULO 8°. (FRAUDE INFORMÁTICO).** El que de forma deliberada e ilegítima, por medio de tecnología informática, telemática y/o electrónica, introdujere, alterare total o parcialmente, borrare total o parcialmente, suprimiere total o parcialmente datos (informáticos, relativos al tráfico y/o a los abonados) o interfiriere total o parcialmente en el normal funcionamiento de uno o varios sistemas informáticos, con independencia de que los datos sean legibles e inteligibles directa o indirectamente, generando directa o indirectamente perjuicios y/o daños patrimoniales o de cualquier otra naturaleza, será castigado con la pena de seis meses de prisión a seis años de penitenciaría. Se considerará como circunstancia agravante especial de este delito, que el mismo se cometa para obtener de forma ilegítima un beneficio económico para sí y/o para un tercero[23].
Venezuela	**ARTÍCULO 14. (FRAUDE).** Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias[24].

Elaboración propia con fuentes de normativa pública oficial.

Individualizada la tipología penal, desde la teoría del delito, los puntos de cohesión identificados son:

- delitos de sujeto activo impersonal;
- delitos de orden patrimonial;
- el bien jurídico protegido (directo o indirecto) es el sistema informático y los datos (personales).

Corresponde en consecuencia, realizar el análisis doctrinal del comportamiento de cada criterio de oportunidad reglada en ciberdelitos:

a) Escasa relevancia social por la afectación mínima del bien jurídico protegido

En la comisión de ilícitos penales relativos al ciberespacio, se genera una noción de incertidumbre por las siguientes razones:

a.1. En la criminalidad informática es complejo *individualizar* el bien jurídico lesionado; existe una corriente doctrinaria que sostiene que la *información* debiese considerarse un bien jurídico protegido autónomo (la Corte Suprema de Colombia tiene una línea jurisprudencial en este sentido). Sin embargo, contiene dificultades de orden configurativo en tanto la tipología penal. Otra corriente más conservadora se adscribe a sostener que únicamente existe una *intensificación*[25] de la lesión a los bienes jurídicos protegidos prestablecidos por la escuela clásica.

a.2. "El principio de lesividad, exige que se lesione o ponga en peligro el bien jurídico, para que pueda ser sancionada la conducta prevista como delito. Si no hay una ofensa ocasionada, mal puede verificarse la persecución y posterior juzgamiento de un individuo" (González Herrera, 2006). Considerando que existe una doble percepción jurídico-penal en relación al sistema informático como medio para la comisión de delitos o como fin, criterios por los que el ordenamiento jurídico iberoamericano no es uniforme en tanto a las figuras de la tentativa o peligrosidad.

Asimismo, el sistema garantista ha resuelto, entre otras políticas, en la etapa investigativa preliminar, que la acción sea privada (promovida por la parte) para delitos de bagatela. La normativa iberoamericana tiene prácticamente unificada la postura que contempla este régimen (de acción privada) a los delitos contra el honor (difamaciones, injurias, calumnias, etc.). No obstante, cuando se cometen estos delitos en el ámbito cibernético la *afectación* no es mínima ni tampoco necesariamente de escasa relevancia social, particularmente por la difusión viral y por esa *intensificación* precitada.

b) Cuando el imputado haya sufrido, a consecuencia del hecho, un daño físico o moral más grave que la pena a imponerse

Conocida como *pena natural*. El punto de partida necesario es comprender que derechos humanos y garantías constitucionales, en esta denominada –en palabras de Bauman– cultura líquida que profesa la *sociedad de la información*[26] contemporánea se ha topado con una problemática jurídica, y con ella, neologismos tales como la identidad o reputación digital que cada vez más se apodera del universo, conforme al Informe Global Statshot de usos digitales, en 2022 el 60 %[27] de los usuarios utilizan redes sociales en el mundo. Viéndose esta identidad sobreexpuesta, a partir de la estructura doctrinal y jurisprudencial alemana "que utiliza la teoría de las esferas (*Sphären*) para reconstruir dogmáticamente el derecho a la intimidad (esfera individual, esfera privada y esfera íntima)"[28]. Conexas a máximas jurídicas con tinte axiológico, como lo son:

- fama,
- intimidad,
- privacidad,
- dignidad,
- honra,
- honor,
- imagen.

Asimilando que en la delincuencia cibernética ha surgido el fenómeno social de la *condena previa,* sumamente relevante por la animadversión hacia la presunción de inocencia, superando el aforismo de la *pena natural* que sostiene el presente criterio de oportunidad reglada. Esta gravedad radica en el hecho de que genera un doble juicio y un escarnio público que produce una nueva variante de punición que se asemeja a la *muerte civil*[29], "en lo fo-

(22) Ley N° 30.096 de delitos informáticos.

(23) Proyecto de ley de ciberdelincuencia y delitos informáticos, Carpeta N° 972/2016.

(24) Ley especial contra los delitos informáticos, Gaceta N° 37.313.

(25) Este fenómeno jurídico responde a los principios de ubicuidad y multiterritorialidad propios del derecho informático, por la masiva difusión simultánea de una acción u omisión lesiva en y/o desde el ciberespacio.

(26) A partir de los años sesenta, aparece una nueva sociedad caracterizada por el incremento de la información, como una definición del mundo moderno creándose un nuevo paradigma para interpretar el desarrollo social sobre la base del uso y empleo de tecnologías de información. El concepto *sociedad de la información* lleva muchas suposiciones acerca de lo que está cambiando, y cómo este cambio es efectivo. (Estudillo García, Joel, "Surgimiento de la Sociedad de la Información", *Biblioteca Universitaria*, vol. 4, núm. 2, julio-diciembre, 2001, pp. 77-86. Universidad Nacional Autónoma de México Distrito Federal, México).

(27) Aprox. 5.000 millones de internautas (Informe Global Statshot de usos digitales, 2021).

(28) Zúñiga U., Francisco. "El Derecho a la Intimidad y sus paradigmas". *Ius et Praxis*, vol. 3, núm. 1, 1997, Universidad de Talca, Talca, Chile, p. 19.

(29) Su origen se desarrolla en un arco cronológico que tiene su piedra angular en la cuarta de las Leyes de Toro de 1505. (Vallejo, Jesús, "Vida Castellana de la muerte civil", Universidad de Sevilla, HID 31, 2004).

rense, es la mutación de Estado, por la cual la persona en quien acontece, se contempla en derecho, para en orden a efectos legales, como si no fuera"[30].

La incesante trifulca entre la libertad de expresión y el acceso a la información se torna sistémica, desde un paradigma reformulado del planteado por Jean-Paul Sartre al decir que "mi libertad se termina donde empieza la de los demás", en el que podría considerarse que el acusado, en la mayoría de los casos, sí ha sufrido un daño moral[31] más grave, comprendiendo este último "tanto los sufrimientos y las aflicciones causados a la víctima directa y a sus allegados, el menoscabo de valores muy significativos para las personas, así como las alteraciones, de carácter no pecuniario, en las condiciones de existencia de la víctima o su familia"[32].

Nótese como noción necesaria que, desde la doctrina del derecho informático, se habla también de un *daño informático* en el que, desde la teoría de la imputabilidad objetiva civil, se considera al *software* una *cosa peligrosa*[33].

c) Cuando la pena que se espera por el delito de cuya persecución se prescinde carece de importancia en consideración a una pena ya impuesta por otro delito

Esa situación, basada en una relación de *costo-beneficio*, en el caso de ciberdelitos, suele surgir por la ínfima sanción que se establece, ya sea por la falta de privación de libertad en algunos casos, o en otros con cifras muy reducidas. Por ejemplo, en Bolivia, la legislación penal únicamente contempla dos delitos informáticos tipificados[34]:

- Art. 363 bis. Manipulación informática, que sanciona al autor con reclusión de uno a cinco años y con multa de sesenta a doscientos días.
- Art. 363 ter. Alteración, acceso y uso indebido de datos informáticos, que sanciona al autor con prestación de trabajo hasta un año o multa hasta doscientos días.

Nótese que, en el primer caso, *mayoritariamente* no se impone la pena máxima, por lo que, por indulto u otro mecanismo y otros criterios procedimentales de la ejecución de penas, la idoneidad de la política criminal no es la adecuada. En el segundo caso, se puede evidenciar que la sanción no implica privación de libertad, y la pena máxima se reduce a la prestación de trabajo por 1 año o (no *y)* multa de hasta 200 días. Pudiéndose inferir que este último caso, paradójicamente, *motiva* a delinquir, puesto que, con la plusvalía que ha cobrado la información en esta era, es conveniente cometer el ilícito para obtener un beneficio y sopesar la sanción impuesta.

Es por ello que, en este criterio, por lo general, los ciberdelitos están vinculados a otros delitos de orden patrimonial y/o en contra del honor u otros que vulneran libertades y bienes jurídicos protegidos vinculados a derechos humanos, que implican una sanción más significativa. Esto de cierta forma menoscaba la teleología de los delitos informáticos porque les otorgan una cualidad accesoria.

d) Cuando sea previsible el perdón judicial

Conforme al principio de uniformidad, reserva de ley y extraterritorialidad[35], este criterio responde a la arquitectura sistémica propia de cada ordenamiento jurídico de derecho interno, que corresponde a parámetros particulares que no atañen al presente desarrollo. Contando como único parámetro general que la pena impuesta no supere los dos a tres años, sin existir consideraciones específicas que impliquen un comportamiento distinto del presente criterio de oportunidad en caso de tratarse de ciberdelitos.

e) Cuando la pena a imponerse carezca de importancia en consideración a las de otros delitos o a la que se impondría en un proceso tramitado en el extranjero y sea procedente la extradición solicitada

Este precepto establece la posibilidad de que el acusado hubiera sido sancionado con anterioridad por otros delitos o que exista una extradición donde el acusado igualmente termine con una sanción. En el contexto de la ciberdelincuencia, el instituto de la extradición está directamente vinculado con mecanismos especiales de cooperación internacional, por la relevancia e impacto socioeconómico cultural[36] que implica la comisión transfronteriza de delitos informáticos.

Un principio rector es el de la doble incriminación, que en su dimensión efectiva se explica a partir de que el hecho por el que se solicita la extradición esté tipificado como delito, tanto en la legislación del Estado requerido como en la del Estado requirente, en el momento de su comisión, como en el de solicitud o de entrega; de esta manera, si el hecho no es delito en el Estado requirente, no se le podrá entregar para juzgar o para que cumpla una pena, si no lo es en el Estado requerido, no obstaculiza la convivencia del mismo.

Entendido de esta forma el principio de *doble incriminación*, es útil para delimitar si las conductas son susceptibles de extradición, en la medida en que se puedan identificar en un tipo penal, tanto en la legislación del Estado requerido, como en la del requirente; además que esté incluida entre aquellas que puedan motivar el procedimiento extradicional; en este sentido, Jiménez de Asúa declaró el principio de legalidad, *nulla traditio sine lege*[37].

Dicho principio cobra otra dimensión en el ámbito de la delincuencia informática por los factores de ubicuidad y simultaneidad de la comisión de un ilícito en diversas jurisdicciones. Esta disyuntiva es abordada por el Convenio de Ciberdelincuencia de Budapest de 2001, que entre las temáticas que contiene incluye la facilitación de los medios de extradición para la persecución penal de delitos cibernéticos perpetrados en el territorio de los países miembros[38].

(30) Cavada Herrera, Juan Pablo citando a Rayón y Gómez, 2014: 209-234 en N° SUP:126200 de la Biblioteca del Congreso Nacional de Chile / BCN, 2020.

(31) Daño moral y psicológico: cómo una categoría más genérica, incluye perjuicios en la honra, el sufrimiento y el dolor derivados de la violación. Es el resultado de la humillación a que se somete la víctima, del desconocimiento de su dignidad humana, del sufrimiento y dolor que se le causa como consecuencia de una violación de sus derechos humanos (Cfr. Faundez Ledesma, Héctor. *El Sistema Interamericano de protección de los Derechos Humanos*, Edit. IIDH, 2000., pp. 516 y 833). El daño psicológico se configura por la alteración o modificación patológica del aparato psíquico como consecuencia de un trauma que desborda toda posibilidad de elaboración verbal o simbólica (Ghersi, Carlos A. *Los nuevos daños, soluciones modernas de reparación*, 2ª ed, Buenos Aires, Hammurabi, 2000, p. 68).

(32) Corte IDH, Caso de los "Niños de la Calle" (Villagrán Morales y otros) vs. Guatemala, Reparaciones y Costas. Sentencia de 26 de mayo de 2001, Serie C No. *77*, párr. 84; Corte IDH. Caso Chitay Nech y otros vs. Guatemala, Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 25 de mayo de 2010, Serie C No. 212, párr. 275.

(33) Altmark, Daniel R., Molina Quiroga Eduardo, *Tratado de derecho informático*, ed. La Ley, Buenos Aires, Argentina, 2012.

(34) Modificado por la Ley Nacional N° 1.768 del Estado Plurinacional de Bolivia.

(35) Principio propio de la rama del derecho informático.

(36) El Foro Económico Mundial, en su Informe de Riesgos Globales 2019, posiciona el fraude de datos y los ataques cibernéticos entre los primeros cinco riesgos globales (https://es.weforum.org/reports/the-global-risks-report-2019).

(37) Jiménez De Asúa, L. *Tratado de Derecho Penal; op. cit.,* p. 941.

(38) El Convenio de Ciberdelincuencia Budapest 2001 es un tratado internacional vinculante en materia penal, que busca el establecimiento de herramientas legales para la tipificación de delitos informáticos de forma común en los países parte, para que estos puedan ser perseguidos a través de la cooperación internacional. En el artículo 24 contempla la extradición con el siguiente texto: 1. a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que estas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año. b. Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición aplicable a dos o más Estados, comprendido en la Convención Europea de Extradición (STE n° 24), o de un acuerdo basado en la legislación uniforme o recíproca, aplicarán la pena mínima prevista en esos tratados o acuerdos. 2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición. Los Estados se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir. 3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo. 4. Los Estados que no condicionen la extradición a la existencia de un tratado podrán llevar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo. 5. La extradición quedará sometida a las condiciones establecidas en el derecho interno del Estado requerido o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que el país requerido puede denegar la extradición. 6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, este deberá someter el asunto –la demanda del Estado requirente– a sus autoridades competentes a fin de que estas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que

VII. Integralidad en la reparación de daños en ciberdelitos

Habiéndose planteado la *doble finalidad* de la aplicación de los criterios de oportunidad reglada, entre ellas la reparación integral del daño, que necesariamente debe ser previo e integral, ¿a qué hace referencia esta *integralidad*?

La jurisprudencia ha vinculado la integralidad con el estándar de protección más alto de derechos humanos conforme al siguiente criterio: "La vulneración de los derechos concede a las víctimas el derecho a la indemnización, reparación y resarcimiento de daños y perjuicios en forma oportuna"[39]. Desde su doble dimensión: obligación de Estado y derecho fundamental de la víctima[40].

Con excepción del criterio de oportunidad enunciado en el literal c), es una condición *sine qua non* que el acusado haya reparado *previamente* el daño a la víctima.

Las medidas de reparación deben ser aplicadas en estricto cumplimiento a la Convención Americana sobre Derechos Humanos, en el marco del control de convencionalidad, lo que significa que la reparación debe ser comprendida dentro de los parámetros establecidos por la Corte Interamericana de Derechos Humanos (Corte IDH) que, conforme a los principios de favorabilidad y progresividad, contiene el estándar más alto de protección al derecho de reparación integral, que implica:

a) La restitución, que debería devolver a la víctima a una situación idéntica a la que se encontraba antes de sufrir alguna vulneración a sus derechos.

Esta ficción jurídica adopta una *particular* complejidad ante un perjuicio ocasionado en internet, por el efecto viral que intensifica la lesión al bien jurídico protegido. Más aún en el contexto en el que se plasma una *huella digital* irreversible, que invocando el derecho al acceso a la información es prácticamente[41] imposible eliminar el registro de algún suceso suscitado en la red. Motivo por el cual la víctima encuentra menoscabado su derecho de autodeterminación informativa[42] de manera irreversible.

b) La indemnización, que es una de las más comunes utilizadas por la Corte IDH, referida a una compensación económica tanto por los daños materiales como por los inmateriales que haya sufrido la víctima, como consecuencia de la vulneración de un derecho humano.

El presente parámetro no muestra ningún comportamiento atípico con respecto al cibercrimen, salvo hallar consideraciones particulares en los daños inmateriales ocasionados por el perjuicio *intensificado* ocasionado en el ciberespacio.

c) La rehabilitación. La Corte IDH señala a respecto que: "(…) es preciso disponer una medida de reparación que brinde una atención adecuada a los padecimientos físicos y psicológicos sufridos por las víctimas de las violaciones establecidas en la presente Sentencia (…)"; las medidas de reparación estarán destinadas a daños inmateriales, principalmente a los morales y físicos que sufrirá la víctima como consecuencia de las violaciones a sus derechos humanos y garantías constitucionales.

El presente parámetro no muestra ningún comportamiento atípico con respecto al cibercrimen.

d) La satisfacción, que tiende a generar en la víctima un sentimiento de reconocimiento positivo como consecuencia de los daños que pudiere haber sufrido por la violación de sus derechos humanos. Beristain señala: "Las medidas de satisfacción se refieren a la verificación de los hechos, conocimiento público de la verdad y actos de desagravio; las sanciones contra perpetradores; la conmemoración y tributo a las víctimas".

Una *optimización* de este criterio se puede *evidenciar* en la publicación o difusión de la sentencia. Por ejemplo, en la sentencia de reparaciones emitidas en los casos Barrios Altos, Cantorales Benavides y Durand y Ugarte de la CIDH ordenó por primera vez la publicación de su sentencia en un diario oficial del Estado, así como en otros medios de comunicación como parte del acuerdo celebrado entre las partes y que fuera homologado por la Corte IDH. A partir de ese momento, la publicación de su sentencia, no solo en medios impresos sino incluso a través de la radio y la internet, se ha constituido en una medida de satisfacción constante en las decisiones de la Corte.

e) La garantía de no repetición, que está dirigida a mitigar los daños colectivos.

Los daños de carácter *colectivo* y *social* atienden a vulneraciones derivadas de la violación que repercuten en un grupo de personas o población determinada; principalmente en su calidad del grupo, más allá de las afectaciones de carácter individual. Estos daños han sido reparados principalmente en casos de masacres o de derechos de pueblos indígenas y tribales, u otras colectividades, principalmente cuando se afecta el tejido social. En la mayoría de estos casos dicho daño ha sido resarcido a través de *medidas restitutorias* (derechos sobre territorio) e indemnizatorias. Asimismo, mediante *medidas de satisfacción* (creación de centros de educación, salud, caminos, recuperación de la cultura indígena). En el fenómeno de la criminalidad informática, es muy interesante identificar la similitud entre el derecho de autodeterminación informativa, desarrollado líneas *supra*, con el derecho de libre determinación de los pueblos o autodeterminación indígena, y que cobran relevancia en el sentido en el que los daños y perjuicios en la red, por su naturaleza interconectada, tienden a ser masivos y colectivos.

Sin encontrar ninguna garantía ni medida de contención viable de que no se pueda reproducir, en internet, algún contenido en detrimento a un bien jurídico protegido.

f) Otros criterios de la reparación integral del daño vinculados al cibercrimen.

Restitución de bienes y valores. Con el mismo objetivo se ha ordenado la restitución de bienes y/o valores como se ha visto en el caso "Tibi vs. Ecuador" (2004), en el que se ordenó la restitución de los bienes y valores que le fueron incautados al Sr. Tibi por la policía al momento de su detención (piedras preciosas y un vehículo) que no le fueron devueltos o, en caso de no ser posible, el valor de estos.

Por su parte, en el caso "Parlamara Iribarne vs. Chile"[43] (2005), se ordenó al Estado restituir todo el material que le fue privado a la víctima como los ejemplares de su libro Ética y servicios de inteligencia y el material relacionado que le fueron incautados en su domicilio y una imprenta.

Recuperación de la identidad. La Corte IDH ha ordenado también que el Estado adopte todas las medidas adecuadas y necesarias para la restitución de la identidad de la víctima que fueron sustraídas por autoridades, incluyendo el nombre y apellido que sus padres biológicos le dieron, así como demás datos personales, lo cual debe abarcar la corrección de todos los registros estatales en los cuales aparezca con el apellido. Adoptando una *optimización* idónea a los derechos propios de la autodeterminación informativa, que se desglosan en derechos de acceso, rectificación, cancelación, revocación y oposición referentes a proteger los datos personales en internet.

VIII. Conclusiones

Las políticas criminales en el fenómeno del cibercrimen son *escasas* y *precarias*, y se hacen manifiestas al momento de *compatibilizar* los institutos jurídicos tradicionales a la comisión de delitos informáticos que responden a una arquitectura jurídica diferente. Desde el sistema garantista, que plantea los criterios de oportunidad reglada como una concesión que realiza el Estado para *prescindir* de la persecución de los delitos de bagatela, se puede avizorar que cuando dichos criterios son aplicados a ciberdelitos y surge una problemática *multidimensional*

---

para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado.

(39) Sentencia constitucional N° 019/2018 del Tribunal Constitucional Plurinacional de Bolivia.

(40) Jiménez De Asúa, L. *Tratado de Derecho Penal; op. cit.,* pp. 941.

(41) Existen técnicas y herramientas que procuran eliminar los rastros de datos en internet vinculados a una persona y/o institución.

(42) "El derecho a la autodeterminación informativa, o también conocida como la libertad informática, consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos, (…) busca garantizar la facultad de todo individuo de poder preservarla (la intimidad) ejerciendo un control en el registro, uso y relevancia de los datos que le conciernen". (Orrego, César Augusto, "Una aproximación al contenido constitucional del derecho de autodeterminación informativa en el ordenamiento jurídico peruano", *Anuario de derecho constitucional Latinoamericano*, ISSN 2346-0849, Bogotá, Colombia, 2013).

(43) Corte Interamericana de Derechos Humanos, caso "Palamara Iribarne vs. Chile", sentencia del 22 de noviembre de 2005 (Fondo Reparaciones y Costas), (https://www.corteidh.or.cr/docs/casos/articulos/seriec_135_esp.pdf).

que genera cambios de paradigma al momento de aplicar los preceptos determinados.

a) Escasa relevancia social por la afectación mínima del bien jurídico protegido. En la criminalidad informática es complejo individualizar el bien jurídico lesionado por existir escuelas doctrinarias opuestas. Estando ante una *intensificación* de la lesión a bienes jurídicos protegidos tradicionales. El principio de lesividad aplicado al cibercrimen no termina de precisar la figura de tentativa o peligrosidad por factores como el anonimato y las técnicas computacionales que evitan la identificación del ciberdelicuente y muestran que los delitos informáticos raramente serán de escasa relevancia social.

b) Cuando el imputado haya sufrido, a consecuencia del hecho, un daño físico o moral más grave que la pena a imponerse. En la delincuencia informática la *autodeterminación informativa* se encuentra sobrexpuesta a un daño moral por un fenómeno sociocibernético de la *condena previa* generando un doble juicio y un escarnio público que produce una *nueva* variante de punición que se asemeja a la *muerte civil*. Con una serie de daños conexos, entre los que se apunta el daño informático, como tipo penal autónomo.

c) Cuando la pena que se espera por el delito de cuya persecución se prescinde carece de importancia en consideración a una pena ya impuesta por otro delito. Prácticamente, se sugiere (paradójicamente) al cibercriminal que delinca, puesto que, con la *plusvalía* que ha cobrado la información en esta era, es conveniente cometer el ilícito para obtener un beneficio y sopesar la sanción impuesta, afectando la teleología de los delitos informáticos porque les otorgan una cualidad accesoria.

d) Cuando la pena a imponerse carezca de importancia en consideración a las de otros delitos o a la que se impondría en un proceso tramitado en el extranjero y sea procedente la extradición solicitada. En el contexto de la ciberdelincuencia, el instituto de la extradición está directamente vinculados con mecanismos especiales de *cooperación* internacional por la relevancia e impacto socioeconómico cultural contemplado en el convenio de ciberdelincuencia, que implica la comisión transfronteriza de delitos informáticos, desde el principio de doble incriminación y los principios del derecho informático de ubicuidad y simultaneidad.

Para que los criterios de oportunidad procedan, es necesario que se haya concretado la reparación integral del daño a la víctima. Esta *integralidad* consiste en medidas comprendidas dentro de los parámetros establecidos por la Corte Interamericana de Derechos Humanos (Corte IDH) que, conforme a los principios de favorabilidad y progresividad, contiene el estándar más alto de protección al derecho de reparación integral que implica:

a) Restitución, que en la delincuencia informática surge la *huella digital* de la que emerge el derecho de autodeterminación informativa que es prácticamente irreversible por el efecto masivo, reproducible y simultáneo de difusión.

b) Indemnización.

c) Rehabilitación, figura en la que se pueden hallar consideraciones particulares en los daños inmateriales ocasionados por el perjuicio *intensificado* ocasionado en el ciberespacio.

d) Satisfacción. Desde el precepto de que la publicación de la sentencia en sí misma ya constituye una medida de satisfacción, las tecnologías de información y comunicación han permitido que dicha difusión no sea solo en medios impresos sino incluso a través de la radio y la internet, por lo que se ha constituido en una medida de satisfacción constante en las decisiones de la Corte IDH.

e) No repetición, quedando con una medida inaplicable, al menos en el ámbito técnico-informático por la naturaleza descentralizada de la *red de redes,* en la que, a partir del derecho de acceso a la información, es complejo generar una *irreproducibilidad* de algún contenido en internet, con excepciones muy marcadas como el caso de China o Rusia.

f) Otros criterios de la reparación integral del daño vinculados al cibercrimen.

Como parte de la investigación, además de las medidas prestablecidas por la línea jurisprudencial de la Corte Interamericana de Derechos Humanos, se han divisado otras medidas relevantes para la *criminalidad* informática como son la *restitución de bienes y valores* y la *recuperación de la identidad*, altamente relevantes en la economía digital y en el sensible régimen de protección de datos personales.

Reitero mi agradecimiento más profundo a la editorial jurídica argentina El Derecho de la querida Pontificia Universidad Católica Argentina (UCA) por la posibilidad de acercar una visión de la realidad jurídica de mi país a tan prestigiosa publicación jurídica. Salutaciones afectuosas.

IX. Bibliografía

Altmark, Daniel R., Molina Quiroga Eduardo, *Tratado de derecho informático*, ISBN: 9789870323211, ed. La Ley, Buenos Aires, Argentina, 2012.

Cavada Herrera, Juan Pablo citando a Rayón y Gómez, 2014: 209-234 en Nº SUP:126200 de la Biblioteca del Congreso Nacional de Chile / BCN, 2020.

Chawki Mohamed, "A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy". DROIT-TIC, 2005.

Chung, Wingyan; Chenb, Hsinchun; Changc, Weiping and Chouc, Shihchieh. (2004). "Fighting cybercrime".

Corte IDH, Caso de los "Niños de la Calle" (Villagrán Morales y otros) vs. Guatemala, Reparaciones y Costas. Sentencia de 26 de mayo de 2001, Serie C No. 77; Corte IDH. Caso Chitay Nech y otros vs. Guatemala, Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 25 de mayo de 2010, Serie C No. 212.

Convenio de Ciberdelincuencia, Budapest, Consejo de Europa, 2001 (https://www.oas.org/juridico/english/cyb_pry_convenio.pdf).

Faúndez Ledesma, Héctor. *El Sistema Interamericano de protección de los Derechos Humanos*, Edit. IIDH, 2000.

Ghersi, Carlos A., *Los nuevos daños, soluciones modernas de reparación*, 2ª ed., Buenos Aires, Hammurabi, 2000.

González Herrera, Alberto H., "Problemática del bien jurídico en los nuevos delitos informáticos y telemáticos", Id SAIJ: DACC060073, 2006 (www.saij.jus.gov.ar).

Informe Global Statshot de usos digitales, 2021 (https://wearesocial.com/es/blog/2021/01/digital-report-2021-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/).

Informe de Riesgos Globales 2019, Foro Económico Mundial (https://es.weforum.org/reports/the-global-risks-report-2019).

Jiménez De Asúa, L. *Tratado de Derecho Penal*, Tomo II, Filosofía y Ley Penal, ed. Losada S.A., Buenos Aires, 1950.

"La reparación integral en la jurisprudencia de la Corte Interamericana de Derechos Humanos: estándares aplicables al nuevo paradigma mexicano", Instituto de investigaciones jurídicas, suprema corte de justicia de la nación, fundación Konrad Adenauer, 2013 (https://www.corteidh.or.cr/tablas/r33008.pdf).

Joel Estudillo García, Estudillo García, Joel, "Surgimiento de la sociedad de la información", *Biblioteca Universitaria*, vol. 4, núm. 2, julio-diciembre, Universidad Nacional Autónoma de México Distrito Federal, México, 2001.

Joan Mesquida Sampol, Universidad de las Illes Balears, España, 2013.

Órrego, César Augusto, "Una aproximación al contenido constitucional del derecho de autodeterminación informativa en el ordenamiento jurídico peruano", *Anuario de derecho constitucional Latinoamericano*, ISSN 2346-0849, Bogotá, Colombia, 2013. (https://www.corteidh.or.cr/tablas/r32202.pdf)

Power, Richard, "CSI/FBI computer crime and security survey". *Computer Security Issues & Trends* 8 (1) (2002) 1-22, 2002.

Revista electrónica de ciencia penal y criminología. RECPC. 01-14, 1999 citado en Sáez Capel, José, "El llamado delito informático no existe", Rayo del Sur, Sucre, 2014.

Rico Carrillo, Mariliana, "El impacto de Internet y las redes sociales en el derecho a la libertad de expresión", *Revista de Filosofía Jurídica, Social y Política*. Instituto de Filosofía del Derecho Dr. J.M. Delgado Ocando, Universidad del Zulia FRONESIS. ISSN 1315-6268 - Dep. legal pp 199402ZU33 Vol. 19, No. 3, Universidad Católica del Táchira Táchira-Venezuela, 2012. (https://www.corteidh.or.cr/tablas/r32923.pdf)

Romeo Casabona, Carlos María, *Nuevos Instrumentos Jurídicos en la Lucha contra la Delincuencia Económica y Tecnológica*, ed. Casa del Libro, España, 2006.

"Mecanismos formales de cooperación internacional", UNODC, 2017 (https://www.unodc.org/e4j/es/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html).

Sentencia Constitucional Nº 019/2018 del Tribunal Constitucional Plurinacional de Bolivia.

"Suplemento especial de cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet", Erreius, Buenos Aires, 2018.

Vallejo, Jesús, "Vida Castellana de la muerte civil", Universidad de Sevilla, HID 31, 2004.

Zúñiga U., Francisco, "El Derecho a la Intimidad y sus Paradigmas", Ius et Praxis, vol. 3, núm. 1, Universidad de Talca Talca, Chile, 1997.

VOCES: INFORMÁTICA - INTERNET - DERECHO PENAL - DERECHO INTERNACIONAL - ORGANISMOS INTERNACIONALES - DERECHO PENAL INTERNACIONAL - TECNOLOGÍA - DERECHO PENAL ESPECIAL - DAÑOS Y PERJUICIOS - INTELIGENCIA ARTIFICIAL - PRUEBA - DELITOS INFORMÁTICOS - CIBERSEGURIDAD - IMPUTABILIDAD PENAL