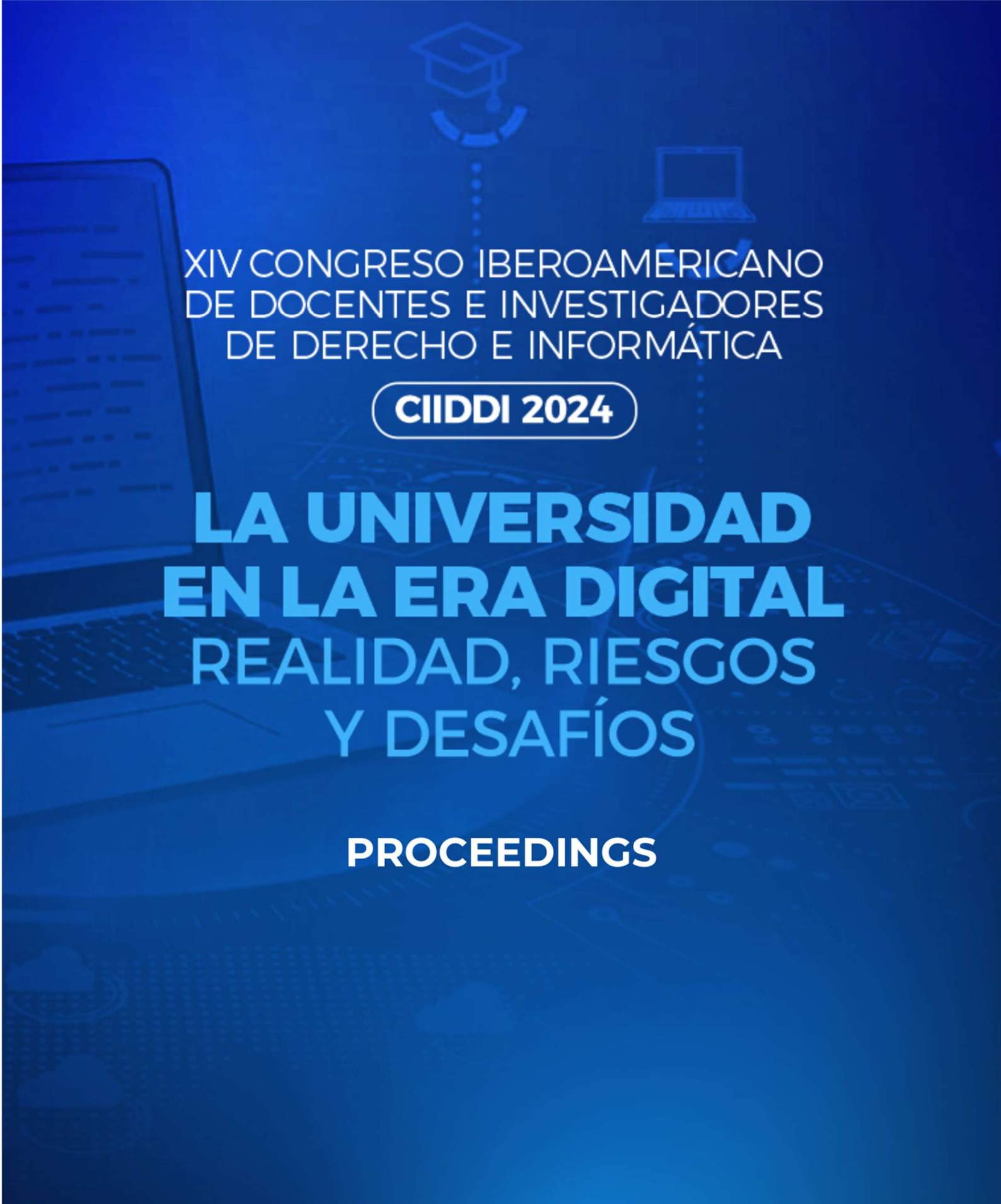




XIV CONGRESO IBEROAMERICANO  
DE DOCENTES E INVESTIGADORES  
DE DERECHO E INFORMÁTICA

**CIDDI 2024**

# **LA UNIVERSIDAD EN LA ERA DIGITAL REALIDAD, RIESGOS Y DESAFÍOS**

**PROCEEDINGS**

Universidad FASTA

Proceedings del XIV Congreso Iberoamericano de Docentes e Investigadores de Informática y Derecho : CIIDDI 2024 : la universidad en la era digital : realidad, riesgos y desafíos / 1a ed - Mar del Plata : Universidad FASTA, 2024.

Libro digital, PDF

Archivo Digital: descarga y online

ISBN 978-631-90546-5-1

1. Derecho. 2. Seguridad Informática. 3. Derecho Informático. I. Título.  
CDD 340.07

XIV CONGRESO IBEROAMERICANO  
DE DOCENTES E INVESTIGADORES  
DE INFORMÁTICA Y DERECHO

**CIIDDI 2024**

**LA UNIVERSIDAD EN  
LA ERA DIGITAL**  
REALIDAD, RIESGOS Y  
DESAFÍOS

**PROCEEDINGS**



UNIVERSIDAD  
CHAMPAGNAT



Sponsors:





## Comités:

### **COMITÉ EJECUTIVO**

#### **Presidente del congreso:**

Mario Adaro

#### **Vicepresidente del congreso:**

Fernanda Giaccaglia

#### **Secretaria del congreso:**

Antonela D'Onofrio

### **COMITÉ ORGANIZADOR**

María Eugenia Arenz

Mariana Brachetta

Enzo Completa

Antonela D'Onofrio

Ana Di Iorio

María Fernanda Giaccaglia

María Paula Giaccaglia

Roberto Giordano Lerena

Paula Muscia

María Martínez Palacios

Virginia Sebastian

### **COMITÉ ACADÉMICO**

María Eugenia Arenz

Cielo Artigas

Vanesa Blache

Mariana Brachetta

Tania Bueno

Carla Carrillo

Carlos Catania

Ana Karin Chávez Valdivia

Cristiano Colombo

Enzo Completa

Bruno Constanzo

Hugo Curti

Antonela D'Onofrio

Enrique Del Carril

Ana Di Iorio

Luis Fontana

Zoraida García Castillo

Ana Garis

María Fernanda Giaccaglia

María Paula Giaccaglia

Roberto Giordano Lerena

Horacio Granero

Sabrina Lamperti

Rosane Leal da Silva

Clara Bibiana Luz

Aline Macohin

Manuel Masseno

Aida Noblia

Beatriz Parra de Gallo

Ariel Podesta

Aires Rover

Fernanda Rosales

Coorganizado por la Universidad FASTA, la Red CIIDDI y la Universidad Champagnat de Mendoza, siendo esta última la anfitriona, los días 2 y 3 de mayo de 2024 se llevó a cabo el **XIV Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática (CIIDDI 2024)**.

Bajo el lema *“La universidad en la era digital: realidad, riesgos y desafíos”*, y con formato híbrido, el CIIDDI 2024 reunió a renombrados profesionales, tanto nacionales como internacionales, en el campo de la informática y el derecho, erigiéndose como un espacio de intercambio y reflexión sobre los nuevos paradigmas que enfrenta la educación superior en la actualidad digitalizada.

Durante dos intensas y provechosas jornadas, el congreso abordó una amplia gama de temas, desde el impacto de la inteligencia artificial en la enseñanza y el aprendizaje, hasta la regulación legal de la tecnología educativa y la protección de datos en entornos académicos digitales.

El CIIDDI 2024 no solo fue un espacio de reflexión, sino también de acción, con **presentaciones de trabajos** sobre temas como la convivencia digital en el ámbito educativo, la protección digital de niños y adolescentes, y los desafíos en la educación de las facultades de Derecho en la era digital.

El éxito del CIIDDI 2024 marcó un hito en la colaboración entre la Universidad Champagnat y UFASTA, reafirmando su compromiso con la excelencia académica y la innovación en el campo de la informática y el derecho.

**¡Agradecemos a todos los que fueron parte del CIIDDI 2024 y que nos acompañaron, tanto presencial, como virtualmente!**

## **GRABACIONES DE LAS JORNADAS**

Para acceder, ingresar los siguientes enlaces en el navegador:

- Jueves 2 de mayo de 2024: **[bit.ly/CIIDDI1](https://bit.ly/CIIDDI1)**
- Viernes 3 de mayo de 2024: **[bit.ly/CIIDDI2](https://bit.ly/CIIDDI2)**

# INDICE DE TRABAJOS

|                                                                                                                                                        |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| @Supremadefallo: la investigación académica como ecosistema digital                                                                                    | <b>7</b>   |
| Ciberviolencia                                                                                                                                         | <b>22</b>  |
| Componentes y Valoración Docente a las Credenciales Digitales con Blockchain                                                                           | <b>33</b>  |
| Confesiones, sexting, insultos y amenazas: ciberviolencia en la educación                                                                              | <b>44</b>  |
| Convivencia Digital en el Ámbito Educativo: Prevención y Acción ante las Ciber Violencias                                                              | <b>54</b>  |
| Derechos Humanos, Inteligencia Artificial, Ética y Constitucionalismo Digital                                                                          | <b>59</b>  |
| Desafíos del Derecho educativo en la posmodernidad                                                                                                     | <b>68</b>  |
| Desafíos en la educación de las facultades de Derecho desde los paradigmas de educación y la disrupción tecnológica                                    | <b>74</b>  |
| Engenharia da Paz na Era da Quarta Revolução Industrial: Moldando uma Nova Mentalidade no Ensino da Engenharia                                         | <b>83</b>  |
| Fortalecimiento de la Seguridad y Protección de Datos Personales en Chile: Desafíos y Perspectivas hacia el Futuro                                     | <b>93</b>  |
| Incorporación de la Inteligencia Artificial en el aula: Cómo comenzar a involucrar las nuevas tecnologías en la enseñanza del Derecho y la Ingeniería  | <b>104</b> |
| Innovación en la enseñanza del Derecho del Consumidor: Integrando la IA para un aprendizaje significativo                                              | <b>109</b> |
| Inteligência Artificial e Propostas Regulatórias Brasileiras: uma análise acerca da explicabilidade                                                    | <b>124</b> |
| Las competencias digitales en la formación del abogado y la práctica del Derecho                                                                       | <b>134</b> |
| Modelo Híbrido de dos niveles para la detección de anomalías con técnicas de Machine Learning en redes IoT                                             | <b>145</b> |
| ¿Podemos considerar persona a la IA?                                                                                                                   | <b>157</b> |
| Privacidad de datos en aplicaciones de sistemas IOT para Smart Cities: una revisión sistemática                                                        | <b>165</b> |
| Protección Digital de Niños, Niñas y Adolescentes - Caso de Estudio en Escuelas de Salta (Argentina)                                                   | <b>180</b> |
| Readecuación del Perfil Docente/Investigador en la Facultad Regional Delta                                                                             | <b>189</b> |
| Recomendaciones para una infraestructura legal y normativa adecuada en organizaciones de I+D y Gestión de la Propiedad Intelectual en disciplinas STEM | <b>193</b> |
| Tecnología H5P y aprendizaje autodirigido                                                                                                              | <b>203</b> |

# @Supremadefallo: la investigación académica como ecosistema digital

Enrique H. del Carril (UFASTA, UCA)

**Abstract**—La irrupción de las redes sociales, más allá de su existencia novedosa como objetos digitales, configuró un cambio cultural en el modo de acercarse al conocimiento. Estas nuevas condiciones imponen la necesidad de repensar los modos de expresión de la investigación académica. A partir de estos principios, en el presente se expone el “ecosistema digital” construido para un estudio sistemático de la evolución de la jurisprudencia de la Corte Suprema de Justicia de la Nación (CSJN) y la Suprema Corte Suprema de los Estados Unidos de América (SCOTUS). Este ecosistema tiene varios objetivos que se despliegan por capas de “profundidad”, que van desde proveer información actualizada de las sentencias de estos tribunales y su uso para la docencia, hasta la generación de artículos para su publicación en revistas con referato.

**Index:** investigación académica – transferencia de conocimiento – docencia universitaria – redes sociales – ecosistema digital.

## I. INTRODUCCIÓN

LA investigación académica en el Derecho no ha variado sustancialmente desde al menos un siglo. El “producto” en la investigación académica del Derecho (y, en general, de todas las humanidades) consta, casi exclusivamente, en la publicación de textos a partir de análisis normativos, jurisprudenciales o de fuentes académicas anteriores.

En consecuencia, la metodología de investigación jurídica se circunscribe a la búsqueda, clasificación y análisis de estas fuentes. De allí que sus métodos no se han modificado sustancialmente, más allá de la incorporación del uso de bases de datos electrónicas y repositorios académicos en línea (además de una sensible reducción de la publicación en papel en favor de los soportes digitales).

En consecuencia, fuera de estas innovaciones el objetivo de la investigación académica continúa idéntico: la publicación de libros y de artículos publicables en revistas indexadas y/o con referato.

Si bien es importante mantener los objetivos de toda investigación académica puesto que contribuyen al desarrollo de la ciencia del Derecho, lo cierto es que el modo en que ésta se lleva a cabo en la actualidad se muestra anacrónica y, además, no produce efectos visibles en el mundo de los operadores del Derecho ni en la docencia universitaria, con la velocidad que imponen los tiempos actuales.

Es una percepción extendida que la investigación académica del Derecho es un universo que se aprecia como absolutamente extraña para aquel que se dedica a la práctica jurídica y judicial. Es que la transferencia de estos conocimientos más allá del universo académico es prácticamente nula o, al menos, muy gradual: señala un autor que la tasa de consulta de tesis de posgrado es prácticamente inexistente, aún dentro de la propia comunidad académica (Darnton, 2014).

Lo mismo ocurre con la docencia universitaria: la especificidad y complejidad de los temas que aborda el investigador jurídico hace difícil su transferencia a los estudiantes; al menos a los que cursan carreras de grado.

Por otro lado, es fácilmente observable que la cultura digital viene imponiendo una lógica diametralmente opuesta.

El universo de lo digital en todas sus formas pero, en particular, en la configuración que ha tomado a partir del auge de las redes sociales aspira a otros modos de adquisición y “consumo” de la información. Los formatos escritos se van reduciendo en cantidad y extensión, a la vez que priman otros modos de comunicación más breves y versátiles. El ritmo al que corren las noticias y los conocimientos en las redes sociales exige la transferencia rápida de información y, además, en formatos que la muestren de manera sencilla, breve y, preferentemente, sobre soportes gráficos o visuales.

Es preciso, en consecuencia, idear nuevas estrategias que, a tono con la cultura digital en la que estamos inmersos, permitan una transferencia más inmediata de los conocimientos adquiridos fruto de la investigación académica.

Dos son los problemas que muestra la investigación académica en este nuevo contexto: el tiempo que insume para socializar el fruto del trabajo académico y la complejidad en que está presentada la información fruto de las investigaciones jurídicas.

El factor tiempo es crítico puesto que la dinámica digital actual exige que la transferencia de los conocimientos del ámbito académico a la sociedad (en el caso, a los operadores del derecho) estén disponibles a la brevedad, aun cuando las conclusiones o la información sea parcial. Lo mismo ocurre con la complejidad y extensión de los trabajos académicos: es preciso encontrar modos de comunicación que, si bien no pierdan la profundidad de análisis que es parte de la naturaleza de la investigación académica, permitan producir “entregables” aptos para el uso de otros actores del mundo del derecho que no

tienen ni el tiempo (como los abogados que ejercen la profesión), ni la preparación suficiente (como los estudiantes universitarios), para aprovechar los productos de la investigación en Derecho.

En el presente trabajo se presentará una propuesta que pretende combinar ambas expectativas del trabajo académico: la profundidad de análisis, por un lado, y la transferencia rápida de conocimientos a la comunidad jurídica, por el otro.

La propuesta que aquí se expondrá no es un mero ejercicio teórico, sino que se encuentra actualmente en servicio.

En los puntos que siguen se expondrá, en primer lugar, los presupuestos y la estrategia comunicacional sobre la base de los cuales se construyó este producto digital para luego, en segundo lugar, hacer una descripción completa de las estrategias aplicadas y los productos digitales utilizados.

## II. PRESUPUESTOS Y ESTRATEGIA DIGITAL

EL objetivo primario que se tuvo en cuenta al idear este servicio digital fue promover y hacer conocida la jurisprudencia de la Corte Suprema de Justicia de la Nación y de la Suprema Corte de los Estados Unidos de América.

Luego, como se explicará más adelante, se unieron a éste, otros objetivos secundarios que, a la vez, sirven para promocionar aquel fin central.

La estrategia comunicacional está pensada a partir de la combinación de la lógica de las redes sociales y de las publicaciones académicas, con el objetivo de ofrecer diferentes productos que den cuenta de distintos niveles de profundidad de análisis de la jurisprudencia de la Corte Suprema de Justicia de la Nación y la Suprema Corte de los Estados Unidos de América.

El objetivo, por último, está también enfocado a ofrecer material útil para los distintos operadores del derecho (abogados, estudiantes, profesores).

Al estar integrado por distintos canales de comunicación, cuando se haga referencia a esta el paquete digital se lo denominará “Ecosistema@supremadefallo” para una mejor comprensión, a pesar de que sus distintos elementos llevan nombres diferentes y, en caso de la escritura académica, el nombre de su autor.

### A. Elementos del producto comunicacional

El Ecosistema@supremadefallo está integrado por una cuenta de Instagram, una de TikTok, un canal en YouTube, una cuenta de X (ex Twitter), un newsletter en LinkedIn, una columna mensual en una publicación jurídica y artículos varios en revistas con y sin referato.

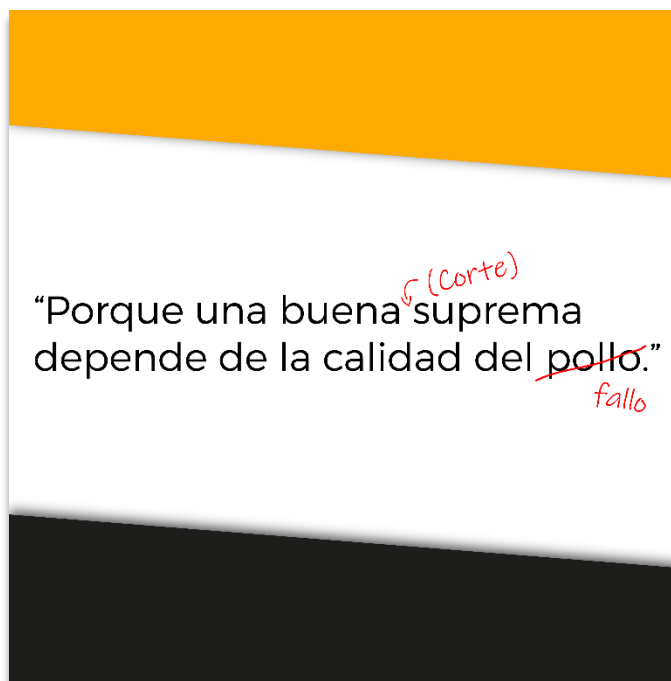
La idea principal es que todos estos elementos tengan correlación entre sí y se retroalimenten para que formen una red por la cual la información circule y se replique y, a la vez gane en profundidad de análisis.

Las ideas secundarias son que este ecosistema sea de utilidad para que sus “usuarios” (seguidores, lectores, etc.) puedan acceder casi en tiempo real a la información que en ella se vuelca y, por último, su objetivo está también enfocado a la

docencia: un canal que sea útil a los estudiantes de derecho para actualizarse en los temas de estudio en la materia de Derecho Constitucional.

### B. El nombre

El nombre “Suprema de Fallo” surgió a partir de un ejercicio de juegos de palabras que quedó compendiado en esta plantilla que se utiliza como carátula de los principales productos digitales.

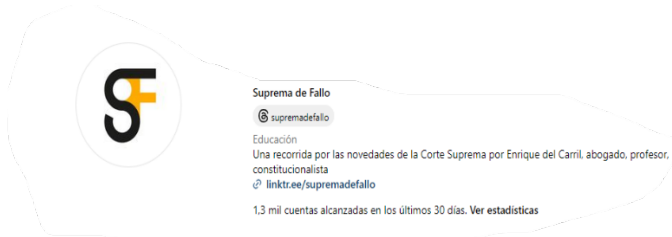


A partir de esta idea, y para lograr un elemento identitario de todos los productos del Ecosistema@supremadefallo, se generó el logo que se muestra a continuación, que identifica los perfiles de los productos digitales y, además, se usa como marca de agua



Así, en función de esta idea primigenia, los distintos elementos fueron tomando nombres que relacionan la idea culinaria de “suprema” con la jurídica de los fallos de la Corte Suprema de Justicia de la Nación.

Así, el Instagram lleva el nombre @supremadefallo



Al igual que la cuenta de TikTok,



el canal de YouTube



y la cuenta de X (ex Twitter)



Por su parte, si bien los otros productos llevan nombres distintos, mantienen la identidad a partir del logo y juegan con esa idea culinaria.

Así, el newsletter de LinkedIn, que se llama “Corte de la Semana”

## Corte de la semana (del 27 de noviembre al 3 de diciembre)



Enrique del Carril

Profesor Derechos Humanos en Universidad FASTA  
Profesor Derecho Constitucional UCA Creador de IG @supremadefallo

26 artículos

Y la columna mensual en el periódico jurídico cuyo nombre es “Suprema Corte a la carta”

### SUPREMA CORTE A LA CARTA

Octubre: sobre límites nacionales, provinciales y familiares, por Enrique H. del Carril • Cita Digital: ED-VLXXXVII-499

El foco central del ecosistema se encuentra en la cuenta de Instagram, donde se vuelcan las principales novedades sobre la Corte Suprema de Justicia de la Nación. Las demás reproducen su contenido (como X y LinkedIn), profundizan esta información (como el TikTok y el YouTube) o se vuelcan a contenidos académicos más tradicionales (la columna mensual y los papers académicos).

Toda esta información sigue un cronograma específico cuyo objetivo es producir contenido todos los días de la semana.

En lo que sigue, se describirá cada uno de los canales del ecosistema, con el contenido que se produce en ellos.

### C. Instagram @supremadefallo

Como es sabido, Instagram ofrece a sus usuarios tres canales: el “feed”, los “reels” y las “historias”.

El feed es el más estático de los tres y, a pesar de que admite otros formatos, en general se utiliza para mostrar imágenes o textos que se muestran todos juntos desde el perfil.

Los reels, en cambio, son similares al feed pero dinámicos. En general son videos que no exceden los sesenta segundos y, al igual que el anterior, se muestran juntos en el perfil específico.

Por último, las historias admiten múltiples formatos, pero son más efímeras, duran visibles 24 horas.

#### C.1 Feed

La Corte Suprema de Justicia de la Nación produce semanalmente, en promedio, entre trescientas (300) y cuatrocientas (400) sentencias. Los ministros firman una vez por semana en el denominado “acuerdo” que se reúne los martes o jueves.

La gran mayoría de estas sentencias tiene una importancia menor, ya sea porque son cuestiones de competencia que la Corte debe resolver, o decide que los temas traídos a su conocimiento constituyen “cuestiones federales insustanciales” y, por ello, las rechaza por aplicación del artículo 280 del Código Procesal Civil y Comercial de la Nación.

Son menos las sentencias “de fondo” en cada acuerdo que introducen temas de interés.

Todas las semanas, una vez que el Acuerdo se hace público en la página oficial de la Corte Suprema, se revisan todas las sentencias y se eligen entre tres y seis para informarlas en el feed.

Para presentar estas se optó por una estética que simulara un archivo, para que fueran fácilmente visualizables por los usuarios; ésta es una imagen de la visión general del feed:



Como se advertirá, los archivos del feed tienen distintos colores. Estos colores identifican siete categorías temáticas, con el objetivo de que sean más fáciles de identificar por parte del usuario.

Para diagramar estas categorías, se optó por un número reducido que, en cada una, englobe muchos subtemas y se le asignó un color específico a cada una. Estas categorías son:

1. Derechos individuales (verde claro)
2. Ambiental (verde oscuro)
3. Debido proceso (violeta)
4. Trabajo y Seguridad Social (marrón)
5. Federalismo (rojo)
6. Propiedad (naranja)
7. Electoral y democracia (celeste)

Como se habrá advertido, estas categorías no responden estrictamente a clasificaciones jurídicas tradicionales o, al menos, no parecerían abarcar todos los temas que toca la Corte

Suprema.

Es que se ha buscado generar una suerte de “índice” más bien indicativo, para facilitar la búsqueda a los usuarios que no estén familiarizados con el modo en que la doctrina y la propia Corte Suprema divide los temas; por ejemplo, “Federalismo” incluye los temas específicos de la discusión sobre las facultades de las provincias, aquellos casos en los que una provincia es demandada o demandante en instancia originaria ante la Corte y las cuestiones de competencia entre la justicia provincial y la federal.

A partir de esto, cada uno de los fallos se presenta en el *feed*, con tres pantallas consecutivas, con su color correspondiente.

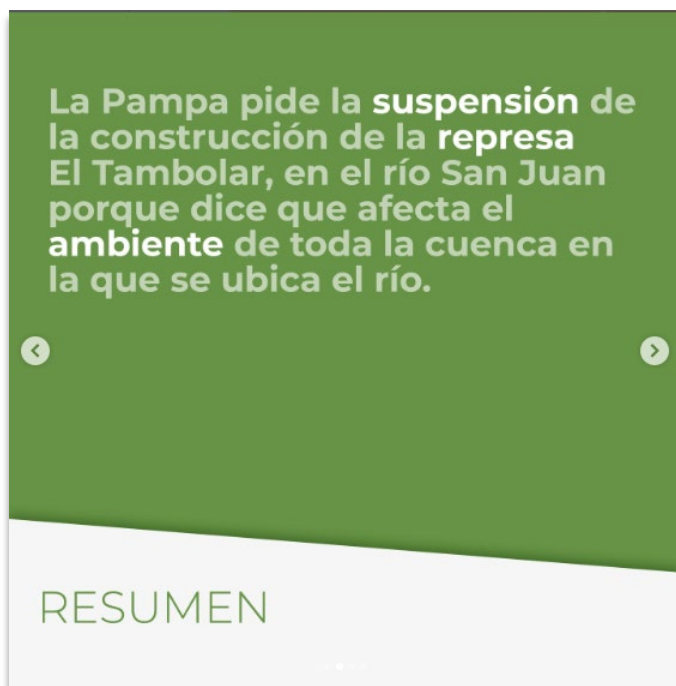
En la primera, se informa la fecha del acuerdo, el nombre del caso y la categoría en la que está incluida, tal como puede verse en la siguiente imagen:



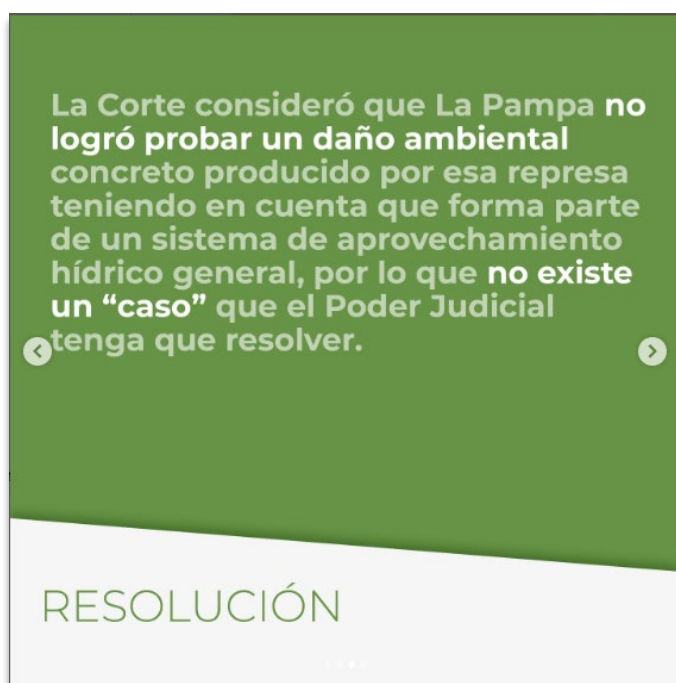
El nombre del caso es una simplificación que ayuda a que el usuario pueda recordarlo (por ejemplo, el caso que se exhibe en la imagen de arriba se denomina, en realidad, “CSJ 2005/2018: La Pampa, Provincia de c/San Juan, Provincia de y otro (Estado Nacional) s/amparo ambiental”).

En la segunda pantalla, bajo el título “Resumen”, manteniendo el color identificador y la misma estética, se explica en lenguaje claro y en un texto breve los hechos en litigio. En el caso de la carátula anterior, el texto es el siguiente:





En la siguiente, con el título “Resolución” y siguiendo los mismos lineamientos (igual estética y color, textos cortos y en lenguaje claro), se explica la decisión que tomó la Corte, conforme puede verse en la siguiente imagen:



Como puede verse en las dos pantallas anteriores se evita utilizar lenguaje excesivamente técnico (aunque esto implique, en algunas ocasiones, perder algo de precisión jurídica) y se resaltan algunas palabras clave que permitan entender la cuestión sin necesidad de leer todo el texto.

Para compensar estas imprecisiones y apuntando a una parte del público con mayores conocimientos de los temas, en la

última pantalla, bajo el título “Cita clave”, se transcribe la parte pertinente de la sentencia, que explica la decisión de la Corte, tal como se muestra en la siguiente imagen:



En ésta, si bien se intenta que la cita sea textual, por una cuestión de espacio se suprimen las referencias normativas usuales en las sentencias, así como también giros lingüísticos innecesarios o superfluos, típicos de la escritura jurídica.

El objetivo principal del feed es que los usuarios puedan acceder a esta información de manera rápida y que sea fácilmente ubicable. Por eso estos gráficos se suben, como máximo, 24 horas después del acuerdo.

Adicionalmente, cuando algún usuario quiera más detalle, se le ofrece enviarle la sentencia por el canal que él elija:

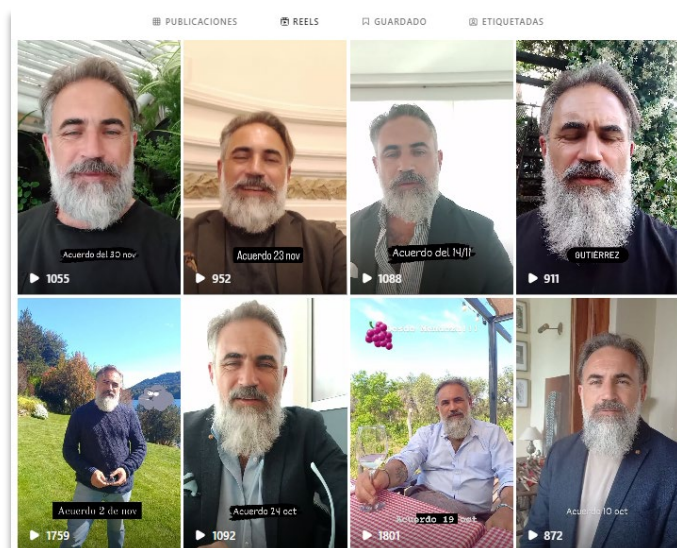


### C.2 Reel

El reel es el canal por el cual se transmiten las noticias casi en tiempo real.



En general (salvo que aparezcan cuestiones que tengan interés público, el cual genera un *reel* autónomo), se sube uno por semana en el que se detallan los fallos elegidos con una breve explicación del tema que abordan. Su extensión no excede los treinta segundos y su producción es lo más ágil y espontánea posible, sin mucha elaboración posterior a la filmación. Se filma con un celular y, casi siempre, en modo selfie:

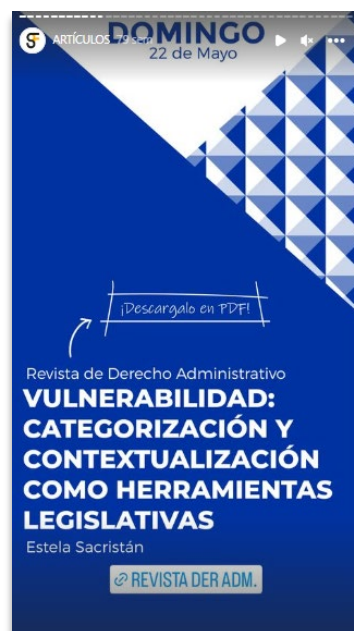


En la actualidad, Instagram está priorizando los reels (probablemente para competir con TikTok), por lo que tienen altos grados de visualización en tiempos breves.

### C.3 Historias

Las *Historias* están enfocadas en aportar novedades o noticias. Además de este uso principal, dos de las secciones complementarias del Instagram están diseñadas para este formato.

En primer lugar, una sección denominada “El artículo de la semana”. Se publica los domingos por la tarde y tiene por objetivo recomendar un artículo sobre temas relacionados con el Derecho Constitucional, cuando el autor o la revista tienen perfil de Instagram, se los arroba para aumentar la visibilidad y, como ocurre usualmente, permitirle al autor del artículo replicarlo en su perfil:



El otro contenido que se entrega semanalmente (los lunes) se denomina “Sabías que...”.

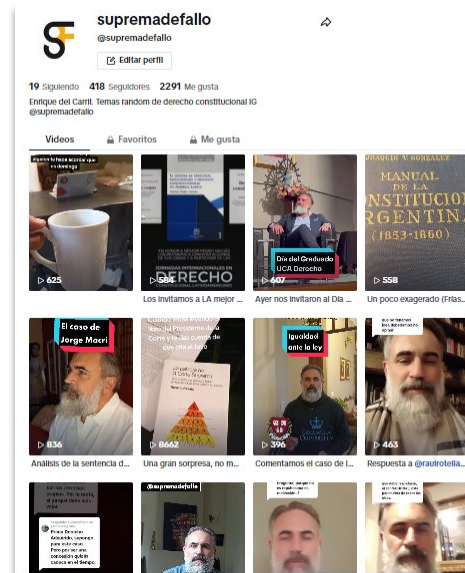
En él se fue relatando la historia de la Corte Suprema. En sus primeras entregas se centró sobre los edificios que ocupó y luego en cada uno de sus ministros por orden cronológico.

Esta sección tiene, a su vez, cuatro subsecciones para ordenar la información: “biografía”, “actuación pública”, “su tiempo en la Corte” y “datos curiosos”.

A continuación, dos ejemplos de la sección:



La estética del formato se fue modificando, haciendo juego con el tiempo cronológico de los ministros



#### D. TikTok @supremadefallo

La lógica de TikTok es sustancialmente diferente a la de Instagram. Si bien esta última, con la incorporación de los reel buscó emularla, lo cierto es que, más allá de esta similitud, las prácticas sociales construidas en torno al TikTok tienen una identidad propia.

En primer lugar, la identificación de un perfil “exitoso” en TikTok está enfocada más al número de visualizaciones que al de seguidores. En segundo lugar, el verdadero motor de esta red social se encuentra en los “trends” (tópicos que adquieren notoriedad), los “desafíos” (videos o coreografías que se repiten y reversionan) y, en particular, de los audios y canciones “virales” (fragmentos que se utilizan como trasfondo en los videos).

La propuesta de TikTok es la producción de videos, que generalmente no superan uno o dos minutos como máximo, para explicar un tema, relatar alguna curiosidad o informar.

A partir de esto, para este formato se optó por una propuesta distinta del Ecosistema@supremadefallo.

En este espacio se hace un video con un relato breve de alguna sentencia de la Corte Suprema que sea trascendente o en las que se introducen cuestiones novedosas.

El formato, en video, luego de relatar los hechos del caso y las líneas principales de los argumentos de la Corte, deja una o dos preguntas disparadoras.

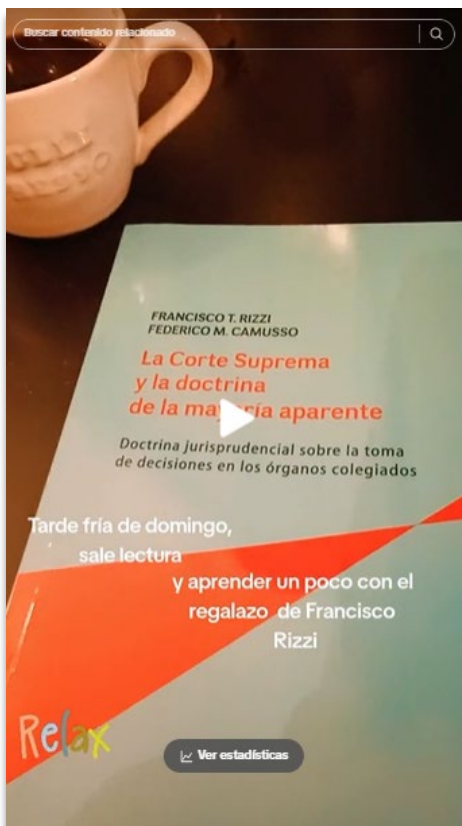
El problema de esta decisión sobre el contenido es que no siempre la Corte dicta sentencias que cumplan con estas condiciones; además, como el perfil está enfocado a un público general, se busca evitar temas excesivamente técnicos (tributarios o cuestiones de competencia, por ejemplo). En consecuencia, para mantener activo el perfil se decidió ampliar la temática. Así, se incorporaron también sentencias de la Corte Suprema de los Estados Unidos.



y se completó con noticias varias sobre actividades académicas:



y otros contenidos más casuales, aunque relacionados con el mundo de lo académico y del derecho constitucional en particular:



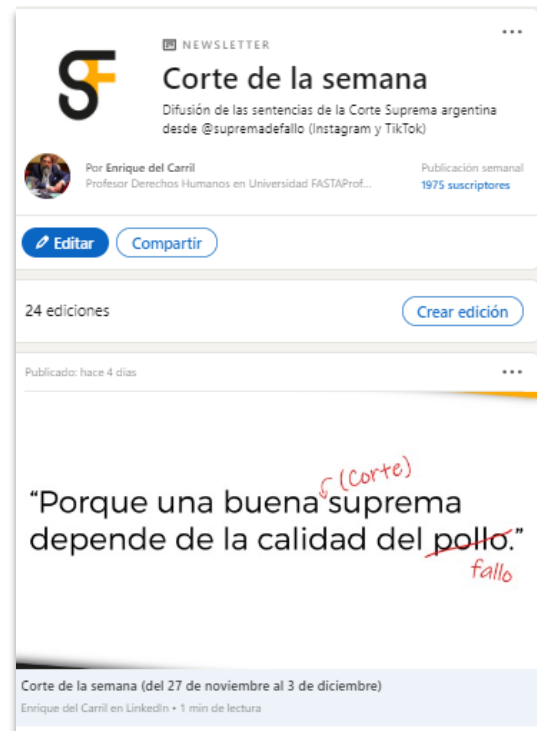
por objetivo completar al Instagram con un análisis más detallado de las sentencias de la Corte Suprema de Justicia de la Nación y, además, agrega otros contenidos útiles para quienes estén interesados en el Derecho Constitucional.

### E. Newsletter de LinkedIn: “Corte de la semana”

Como complemento del Instagram y para generar un esquema de interconexión entre todas las redes sociales, se utilizó el “newsletter” que propone la red social LinkedIn.

Este producto permite generar un informe periódico (en este caso es semanal) con un formato predefinido al que los usuarios de LinkedIn pueden suscribirse para recibirlo en su correo electrónico. Además, cada entrega se publica en el perfil de LinkedIn del usuario.

Para el nombre, siguiendo con referencias culinarias del mismo estilo que el Instagram, se optó por “Corte de la semana” y, además, el newsletter usa el logo y la carátula del Instagram como puede verse aquí



Cada edición del newsletter tiene tres secciones:

1. Acuerdo: en el que se describe en un texto corto el contenido de las sentencias del acuerdo de esa semana;

De esta manera, el TikTok, en su contenido “central” tiene



## Corte de la semana (del 19 al 26 de noviembre)



Enrique del Carril  
Profesor Derechos Humanos en Universidad FASTA/Profesor Derecho Constitucional UCA Creador de IG @supremadefallo

26 artículos

24 de noviembre de 2023

[Abrir lector interactivo](#)

Bienvenidos al newsletter de @supremadefallo en el que les acercamos las novedades de la Corte Suprema de Justicia de la Nación.

Si recibiste esto de un amigo/o podés suscribirte para recibirlo en tu correo todas las semanas en este link:

[Suscribite en LinkedIn](#)

### Acuerdo del 23 de noviembre

#### 1. La Pampa c/San Juan

Inexistencia de "caso" en un amparo ambiental entre provincias por la construcción de una represa.

2. "Mientras tanto en...": en la que se informa sobre las novedades de las otras redes sociales

### Mientras tanto, en LinkedIn...

Nueva edición de la columna "Suprema Corte a la carta" en el suplemento de derecho constitucional de El Derecho



Enrique del Carril en LinkedIn: Corte a la carta octubre

Y llegó "Octubre" sobre límites nacionales, provinciales y familiares", la publicación de este mes de mi columna "Suprema Corte a la carta" en el Editorial ED.

### Mientras tanto, en Youtube

Comentamos una muy interesante sentencia de la Corte en la que revoca una condena por homicidio a una mujer en atención a su situación de vulnerabilidad



y; 3. "Noticias de la Corte": en la que se publican noticias de los medios de comunicación relacionadas a la Corte Suprema y/o de casos que están por elevarse a la Corte.

### Noticias sobre la Corte

Los jueces de la Corte se reunieron con Mariano Cúneo Libarona, ministro de Justicia de Javier Milei (Infobae)



Los jueces de la Corte se reunieron con Mariano Cúneo Libarona, ministro de Justicia...

Fue un encuentro protocolar, informaron fuentes judiciales. Horas más tarde, el futuro funcionario realizó declaraciones con elogios hacia los jueces que integran el máximo tribunal.

[Infobae](#)

### Prisión perpetua para policía (Cadena 3 Patagonia)



Prisión perpetua para policía que mató a un hombre en Río Negro - Radio 3 Cadena...

La Corte Suprema de Justicia de la Nación (CSJN) dispuso la condena de prisión perpetua a un efectivo de la Policía de Río Negro que mató a un hombre al que sorprendió cuando...

[Radio 3 Cadena 3 Patagonia](#)

### La Corte Suprema rechazó el planteo de Pérez Corradi (Infobae)



La Corte Suprema rechazó el planteo de Pérez Corradi y su ex mujer en una causa ligada a l...

El imputado fue juzgado por aplicar, mediante operaciones en su caja de ahorros, valores provenientes de la sociedad Oroganiza San Javier para encubrir el origen ilícito de los dineros y de esta...

[Infobae](#)

### Juan Pablo "Pata" Medina: Casación rechazó que llegue a la Corte el sobreseimiento (Infobae)



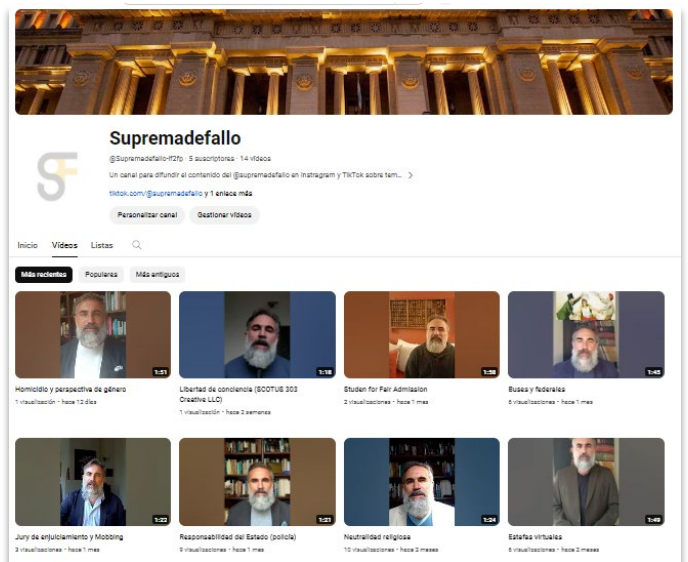
Juan Pablo "Pata" Medina: Casación rechazó que llegue a la Corte el sobreseimiento por...

La Fiscalía apeló la denotación del dudoso caso pero la Cámara entendió que no había motivos para que intervenga el máximo tribunal.

[Infobae](#)

### F. YouTube @supremadefallo

El canal de YouTube sirve, principalmente, como complemento del TikTok. En él se suben los videos que previamente se publicaron en esa red social.



Sin embargo, YouTube es una red cuyos usuarios utilizan para encontrar información más compleja por lo que estos

“soportan” videos de mayor duración.

En consecuencia, se utiliza también con este objetivo; un buen ejemplo de esto es el video animado en el cual se explica el fallo de la Corte “MaCaMe” (cannabis medicinal).



### G. Producción académica

Todo lo que se acaba de describir tiene dos objetivos: el primero -desde la perspectiva de la investigación académica- es mantenerse actualizado sobre las novedades tanto de la Corte Suprema de Justicia de la Nación como de la Suprema Corte de los Estados Unidos de América.

El segundo objetivo podría identificarse dentro del concepto de “transferencia académica”, es decir, aquella finalidad -que se encuentra en la naturaleza misma de la Universidad- de trasladar el fruto de las investigaciones a la comunidad.

El cambio de paradigma que está implicado en el Ecosistema@supremadefallo es que esa transferencia de conocimientos es inmediata, en un lenguaje claro y breve, tal como exige la propia lógica de las redes sociales. Pero acorde con esta reversión de los procesos, la tríada investigación-producción académica- transferencia, se invierte en este orden: investigación - transferencia- producción académica.

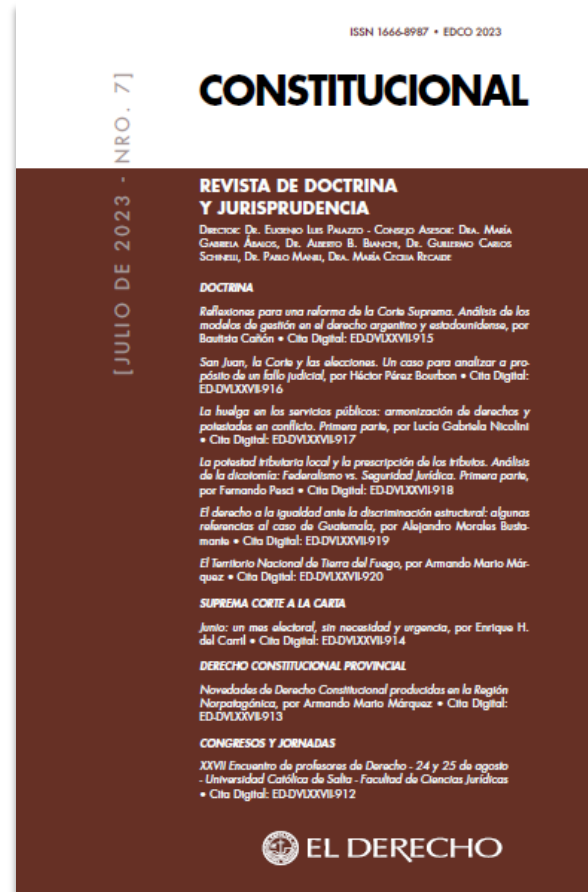
Más allá de esta socialización de y su puesta a disposición de la comunidad, esta información (es decir, la actualidad de ambas cortes supremas) se utiliza en la producción académica más tradicional.

En el caso del Ecosistema@supremadefallo se refleja en una serie de textos académicos que, también, tienen distintos grados de profundización. En este caso son tres: una columna mensual, artículos en revistas académicas sin referato y artículos con referato.

Estos productos que forman parte de la producción académica tradicional llevan el nombre del autor (y no el del ecosistema), aún cuando -como se verá- en algunas ocasiones se permitió relacionarlos a ambos.

### G.1 Columna semanal: Suprema Corte a la carta

A raíz de una propuesta de la prestigiosa revista jurídica El Derecho se comenzó a publicar una columna mensual con el nombre “Suprema Corte a la carta” para mantener informado a un público más especializado respecto de las novedades que, resumidas, se publican en las redes sociales.



La columna es, hoy, una parte integrante fija del suplemento El Derecho Constitucional

#### SUPREMA CORTE A LA CARTA

*Junio: un mes electoral, sin necesidad y urgencia*, por Enrique H. del Carril • Cita Digital: ED-DVLXXVII-914

En ella se busca mantener un estilo informal (en especial en los títulos), aunque algo más elevado, más cercano al que utilizan los medios de comunicación gráfica.

**SUPREMA CORTE A LA CARTA**

**Junio: un mes electoral, sin necesidad y urgencia**

por ENRIQUE H. DEL CARRIL<sup>(\*)</sup>



**Sumario:** OTRA VEZ REELECCIONES. — EL TAMAÑO DE LOS DNJ. — CÓRDOBA ¿SÍ O NO? — IMPUESTO A LAS GANANCIAS. — VIVIR EN ESPAÑA. — OCUPACIONES VARIAS. — ¿QUIÉN PRUEBA QUE Y CUÁNDO? — COMPETENCIA Y CONCLUSIÓN.

Comenzó junio, como se preveía, con una sentencia “de fondo” orden”. La Administración Nacional de la Seguridad Social (ANSES) apeló y la Cámara Federal de Apelaciones de Comodoro Rivadavia confirmó la sentencia de primera instancia, pero condenó en costas a la parte vencida.

En lo que hace a las costas, declaró la inconstitucionalidad del decreto 157/2018, que derogaba el artículo 36 de la ley 27423 que imponía que en estos procesos las costas debía asumirlas este organismo; este decreto es, como se imaginarán, un decreto de necesidad y urgencia. Esto (entre otros agravios) motivó el recurso extraordinario de la ANSES.

e invita a visitar las redes de @supremadefallo

(\*) Para estar al día sobre las novedades de la Corte Suprema, podés seguirnos en el Instagram y en el TikTok @supremadefallo.

El objetivo de la columna es relatar y explicar en un lenguaje más técnico (acorde con los potenciales lectores, es decir, quienes están suscriptos a la revista El Derecho), las principales sentencias de la Corte Suprema de Justicia de la Nación emitidas en el mes anterior.

A los efectos de su adecuada identificación dentro del Ecosistema@supremadefallo, las principales limitaciones son estéticas: no puede mantener la identidad de colores, marcos, logos y sublogos por políticas de la editorial.

## G.2 Artículos varios

En el último escalón de “profundidad” de este ecosistema, están los artículos y papers académicos, ya sea publicados en revistas con o sin referato. Estos se refieren a temas específicos y/o a sentencias trascendentes de ambas cortes supremas y se publican a título personal, puesto que las normas académicas no permiten otra opción.

Estos son algunos ejemplos publicados en revistas sin referato:

### La primera sentencia de nuestra Corte Suprema y sus protagonistas

por ENRIQUE DEL CARRIL<sup>(\*)</sup>

**Sumario:** 1. INTRODUCCIÓN. — 2. EL CASO. 2.1. LAS PARTES. 2.2. EL CASO. 2.2.1. Hechos y antecedentes. 2.2.2. La sentencia de la Corte Suprema. — 3. LA CORTE. — 4. CONCLUSIÓN.

**1. Introducción**

El 15 de octubre de 1863, la flamante Corte Suprema de Justicia de la Nación dictó su primera sentencia<sup>(1)</sup>. Sus integrantes fueron designados un año antes<sup>(2)</sup> pero, paradójicamente, sus primeras acciones no fueron jurisdiccionales sino legislativas. Sus miembros se abocaron a redactar las leyes que serían la columna vertebral del naciente Poder Judicial Federal: las leyes 48, 49 y 50, que delimitaban la competencia de los tribunales y de la propia Corte, y su primera acordada, en la que organiza internamente al Tribunal<sup>(3)</sup>.

Es probable que esta demora en dictar su primera sentencia se haya debido, sencillamente, a que el tribunal no tenía casos por resolver<sup>(4)</sup>; en la también naciente República Argentina, la conciencia de que existía una Corte Suprema que, como cabeza de uno de los poderes del Estado, estaba allí, presente y con el único objetivo de defender los edificios en la Barraca “Victoria” entre Miguel Otero y José Nadal.

La identidad de las partes que llegaron a la Corte se hace vaga en el tiempo y no puede, por lo pronto, confirmarse con precisión. Sin embargo, algunas referencias a estos nombres existen en los pocos registros que pude consultar, de allí que, en lo que sigue, propongo tan solo un ejercicio tentativo, casi adivinatorio de quienes fueran los protagonistas del litigio.

**2.1. Las partes**

Don Miguel Otero estaba metido en más de un problema judicial. Era una costumbre para esos años (quizás como una estrategia publicitaria encubierta o, si lo vemos con su mejor luz, como un modo de apelar a la comunidad), publicar en los periódicos o como libelos autónomos, los escritos judiciales que presentaban los abogados en los pleitos que llevaban.

En un interesante trabajo histórico sobre la publicación de estos alegatos en la prensa de aquella época<sup>(5)</sup>, se listan en un apéndice publicaciones que el autor identifica como “piezas forenses publicadas en Buenos Aires”. Pues bien, para el año 1857 figura en ese listado este pleito en particular bajo el título “Cuestión de derecho en un arbitramento

### “Netchoice vs. Paxton” (o los desafíos de internet y la libertad de expresión)

por ENRIQUE H. DEL CARRIL<sup>(\*)</sup>

**Sumario:** INTRODUCCIÓN. — EL CASO. — EL TRASFONDO DE LA SENTENCIA. — MAYORÍAS Y MINORÍAS. — CONCLUSIÓN.

**Introducción**

Si los hechos que ocasionaron los casos “Calvete” (1864)<sup>(1)</sup> y “Sojo” (1887)<sup>(2)</sup> hubieran ocurrido hoy, estaríamos en el medio de un escándalo institucional. Que el Congreso arreste o inicie acciones penales contra periodistas por criticar a los legisladores, tal vez, era una opción constitucionalmente admisible en el siglo XIX, pero en la actualidad no lo es.

El propósito de este trabajo es reflexionar sobre un caso (o a partir de él) que ocupó recientemente la atención de esa Corte<sup>(3)</sup>.

**El caso**

En “Netchoice vs. Paxton”<sup>(4)</sup>, se discute la constitucionalidad de una ley del estado de Texas; esta, conocida como la ley HB20, prohíbe que las plataformas de redes sociales con al menos cincuenta millones de usuarios activos bloqueen, eliminen o “desmoneticen”<sup>(5)</sup> el contenido de perfiles de usuarios, sobre la base del contenido de sus opiniones. Para justificar esta limitación, el gobierno local

y éste de una revista con referato

**EL DERECHO A LA EXTIMIDAD  
(LA PROTECCIÓN CONSTITUCIONAL  
EN ÉPOCA DE REDES SOCIALES)**

**THE RIGHT TO EXTIMACY (CONSTITUTIONAL  
PROTECTION IN THE AGE OF SOCIAL MEDIA)**

ENRIQUE H. DEL CARRIL<sup>1</sup>

Recibido: 28 de abril de 2021  
Aprobado: 14 de mayo de 2021

**RESUMEN**

La tesis que se sostiene en este trabajo es que el derecho a la privacidad es insuficiente para proteger la actividad de las personas en los entornos digitales de la Sociedad de la Información; en especial, en las redes sociales.

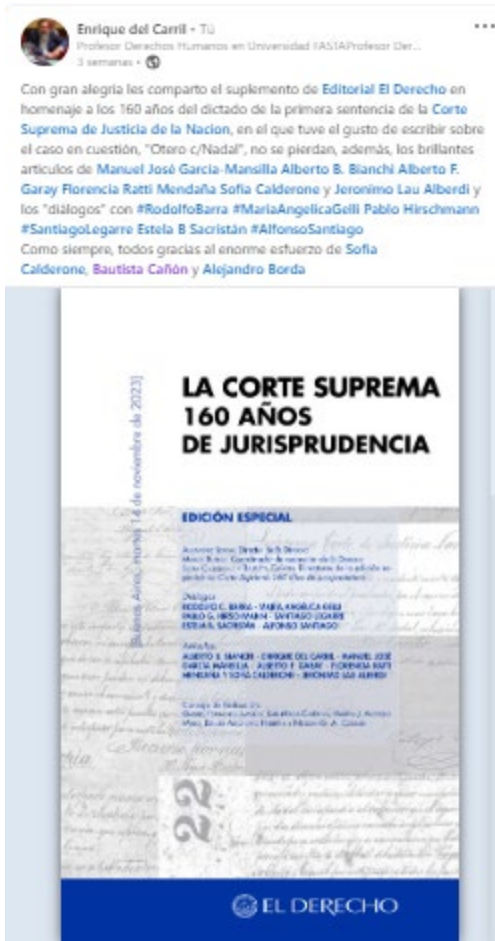
En estos entornos, tal como se desenvuelven en la actualidad, las personas publican información personal, privada e íntima con pleno conocimiento de las consecuencias posibles de sus actos: la viraliza-

1. Abogado (UCA), Magíster en Derecho y Magistratura Judicial (Austral), Profesor de Derecho Constitucional (UCA), Derechos y garantías (UCA), Argumentación jurídica (UCA, Austral) y Derechos Humanos (UFASIA). Correo electrónico: enrique-del@uca.edu.ar.

Como es evidente, también aquí los formatos y la identidad total con el Ecosistema@supremadefallo es inviable, puesto que estos elementos están regidos por las normas académicas o editoriales.

Éste, el último paso en la cadena del ecosistema es el nivel más profundo de análisis de la información (es decir, la jurisprudencia de ambas cortes), en el que los artículos se refieren a temas bien específico y técnicos.

Para cerrar el círculo del ecosistema, estos artículos (cuando las políticas editoriales de las revistas académicas lo permiten) se comparten en LinkedIn:



y en historias de Instagram

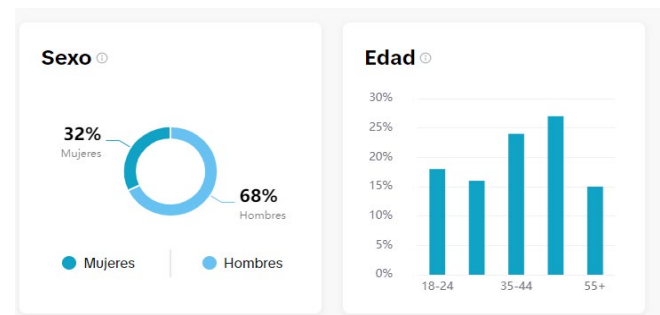
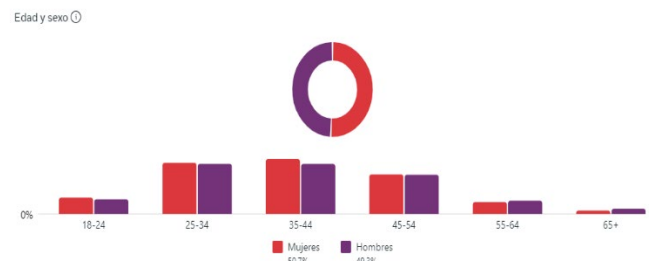


### III. ANÁLISIS DE REDES

ESTE ecosistema de información volcado en los diversos perfiles tiene, además, otra ventaja. A partir de las herramientas para creadores de contenido que suelen ofrecer las redes sociales es posible hacerse una idea del nivel de injerencia que tiene la información y la audiencia objetiva que está haciendo uso de ella para poder hacer las correcciones necesarias, si es preciso.

El nivel de información que ofrece cada una de las redes sociales puede variar un poco por lo que se dificulta hacer análisis globales del todo el ecosistema, pero igualmente es posible tomar de ellas información útil.

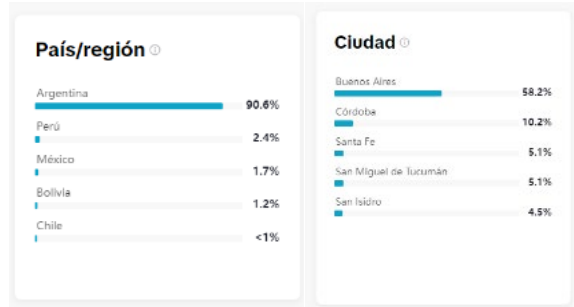
La primera conclusión es que la audiencia del Ecosistema@supremadefallo es relativamente joven, aunque no está compuesta -como se especuló como probable en los inicios- exclusivamente de estudiantes universitarios (es decir, menores de 25 años):



Como puede verse en estos gráficos (el primero corresponde a Instagram y el otro a TikTok, LinkedIn no aporta esta información) la audiencia está compuesta mayoritariamente por personas entre 35 y 44 años, con una distribución similar de hombre y mujeres en Instagram y algo más marcados los hombres en TikTok.

Otra información interesante es la ubicación geográfica de la audiencia





#### Información detallada principal

Ubicaciones

Buenos Aires y alrededores • 57,3 %

La Plata y alrededores • 2 %

Córdoba y alrededores, Argentina • 1,8 %

Madrid y alrededores • 1,4 %

Rosario y alrededores • 1,2 %

Como puede verse en ambas estadísticas (la primera corresponde a Instagram y la segunda a LinkedIn) la distribución territorial de la audiencia es similar, con una preponderancia absoluta de público ubicado en nuestro país. Un aspecto para mejorar es que hoy el público, centralmente, se ubica dentro del área metropolitana de Buenos Aires (AMBA), por lo que deberían pensarse estrategias para tener un alcance más federal.

Por último, LinkedIn ofrece información de la profesión y lugar de trabajo de los seguidores

#### Información detallada principal

Cargos

Abogado • 11,6 %

Profesor • 2,8 %

Maestro • 2,6 %

Abogado • 2,5 %

Secretario • 2,3 %

La presencia de público relacionado con el derecho y la educación es absoluta (la identificación de “secretario” es ambigua, pero se asume -en este contexto- que debe tratarse de funcionarios judiciales de ese rango).

Lo mismo ocurre cuando se desagrega por lugar de trabajo

Empresas

Ministerio Público Fiscal • 1,7 %

Poder Judicial de la Nación • 1,6 %

Universidad Austral, Argentina • 1,5 %

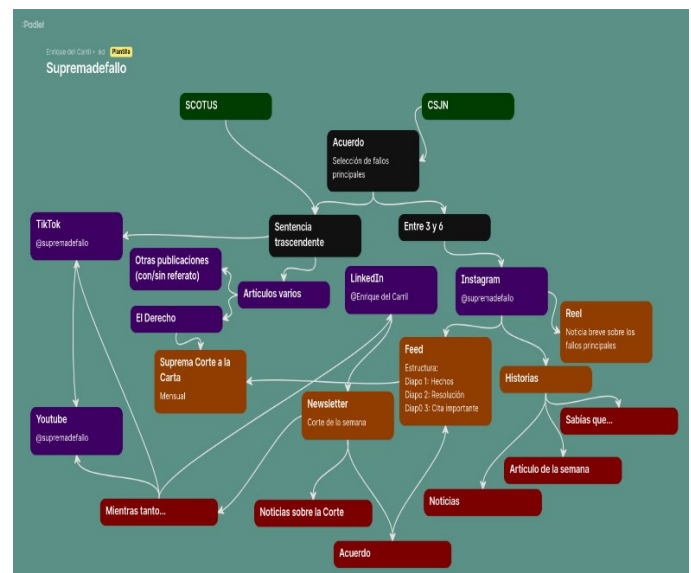
Gobierno de la Ciudad de Buenos Aires • 1,3 %

Universidad de Buenos Aires • 1,3 %

Como puede inferirse de esta información estadística, el ecosistema está correctamente dirigido al público objetivo para el cual se lo planificó (más allá de la necesidad de ampliar su base geográfica): abogados en el ejercicio práctico de la profesión y alumnos/profesores, es decir, individuos que se encuentran en el sector educativo universitario.

#### IV. CONCLUSIONES

EL esquema que se acaba de relatar forma una estructura de perfiles de redes sociales y productos académicos tradicionales, entre los cuales circula información que se retroalimenta y se ordena por capas de “profundidad”. Éste es un esquema de la interrelación:



Esta profundidad está dada por el nivel de análisis del “producto” que se presenta a partir de la información recopilada (es decir, la jurisprudencia de la Corte Suprema de Justicia de la Nación y la Suprema Corte de los Estados Unidos). Si ordenáramos esta información conforme estas capas el esquema resultaría así:



La investigación académica es un pilar fundamental en el desarrollo del conocimiento. Una descripción bastante acertada de ella la identifica como un proceso sistemático a través del cual se busca obtener datos, analizar información y, en especial, generar nuevos conocimientos con el objetivo de aportar a la comprensión de problemas en el área específica de la ciencia de la que se trate.

Como se señaló en la introducción, el modelo tradicional de comunicación científica centra la divulgación de resultados en medios como revistas, congresos, informes, conferencias, etc. Sin embargo, este sistema clásico que es el que subsiste en la actualidad y casi sin ninguna modificación desde hace al menos un siglo, olvida que a partir de la denominada “web 2.0” surgen nuevas posibilidades para mejorar la visibilidad de contenidos académicos en espacios de interacción de Internet (Corchuelo Rodríguez, 2018).

Y estas mejoras deben darse en uno de los puntos centrales de la era digital de las redes sociales: la presencia.

Es que, como se ha advertido, hoy en día es un deber y una necesidad del investigador “... estar presente en los medios y soportes en los que, en pleno siglo XXI, se está dando la comunicación y la conversación académicas y sociales” (Baraibar & Cohen, 2012).

La manera de relacionarse y, en especial, de transmisión de la información ha variado sustancialmente (Scolari, 2008), pero el punto de inflexión de esta modificación no es la aparición de la world wide web (que, en definitiva, no es más que un gran repositorio de información indexado), sino el surgimiento de los usos sociales (en definitiva, la cultura) generada a través del proceso comunicacional instaurado por las redes sociales, que va desde los cambios en las relaciones que se establecen entre los actores, la forma en que el sujeto se muestra y actúa con los otros y las nuevas formas de afiliación y vinculación social (Caceres Zapatero, Brandle Senan, & Ruiz San Roman, 2017).

Lo que se ha denominado en este documento como el Ecosistema@supremadefallo y que aquí se presenta tiene por fin hacer real y efectiva esa presencia, al combinar el momento de la recopilación y clasificación de la información necesaria para una investigación académica con la divulgación de esa misma información a los múltiples usuarios potenciales, que pueden necesitar esos datos para objetivos distintos al conocimiento académico.

Esto redundará no sólo en beneficio de la comunidad en general y, en este punto, cumple con la expectativa de

transferencia social que es uno de los pilares de la misión de la Universidad, sino que colabora a la promoción del investigador, el docente y la propia institución educativa (García-Peñalvo, 2018).

## V. REFERENCIAS

- Baraibar, Á., & Cohen, S. (2012). Nuevas tecnologías y redes sociales en la investigación en Humanidades. *La Perinola*, XVI, 155-164.
- Caceres Zapatero, M., Brandle Senan, G., & Ruiz San Roman, J. (2017). Sociabilidad virtual: la interacción social en el ecosistema digital. *Historia Y Comunicación Social* 22.1, 233-247.
- Corchuelo Rodríguez, C. A. (2018). Visibilidad científica y académica en la web 2.0: análisis de grupos de investigación de la Universidad de La Sabana. *Información, Cultura Y Sociedad* 38, 77-88.
- Darnton, R. (2014). *El coloquio de los lectores: ensayos sobre autores, manuscritos, editores y lectores*. México D.F: Fondo de Cultura Económica.
- García-Peñalvo, F. J. (2018). Identidad digital como investigadores. La evidencia y la transparencia de la producción científica. *Education In The Knowledge Society* 19.2, 7–28.
- Scolari, C. (2008). *Hipermediaciones. Elementos para una teoría de la comunicación digital interactiva*. Barcelona: Gedisa.

## VI. AUTOR



**E**nrique Horacio del Carril es abogado (UCA), Magíster en Derecho y Magistratura Judicial (Austral) donde se graduó con tesis sobresaliente y mejor promedio y Diplomado en Humanidades Digitales (UFASTA). Se ha especializado en Derecho Constitucional, Derechos Humanos, Filosofía del Derecho y Derecho y Tecnología.

Es profesor de grado y posgrado en la Universidad Austral, la Universidad Católica Argentina y la Universidad FASTA, y posgrado en la Universidad Austral, Universidad Nacional del Noroeste de Buenos Aires (UNNOBA), Universidad Nacional del Noreste (UNNE), Universidad de Ciencias Empresariales y Sociales (UCES), entre otras.

Ha dictado clases en los Poderes Judiciales de El Salvador, Colombia, Costa Rica, Salta, Tucumán, Jujuy, Chaco, Corrientes, Tierra del Fuego, Misiones, La Rioja, entre otros.

Integra el Comité de Redacción de los Cuadernos de Derecho Judicial de Editorial La Ley, es evaluador bajo el sistema de “doble ciego” en revistas académicas, evaluador de proyectos de investigación de la Facultad de Ingeniería de la Universidad FASTA y fue evaluador independiente de la revista Persona y Derecho, de la Universidad de Navarra, España.

Premiado en el año 2005 con el Premio La Ley al fortalecimiento del Poder Judicial y en el 2015 por el National Center for Missing & Exploited Children de los Estados Unidos de América por sus aportes a la lucha contra la pornografía infantil en internet.

Es Miembro Correspondiente del Centro de Estudios Jurídicos Notariales, Miembro Honorario del Comité Consultivo de la Escuela de Formación de Auxiliares Jurisdiccionales de la Corte Superior del Callao, República de Perú,

Miembro del Comité Nacional del Observatorio de Ciberdelitos y Evidencia Digital de la Universidad Austral y Miembro Titular de la Asociación Argentina de Derecho Constitucional.

En la actualidad es Secretario de Casos Originarios y Asuntos Constitucionales del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires y anteriormente fue Director del Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal de la CABA y Prosecretario Letrado de la Procuración Fiscal ante la Corte Suprema de Justicia de la Nación.

Contacto: edelcarril@ufasta.edu.ar; enriquedel@uca.edu.ar  
cel. +54 9 11 36 88 80 78

# Ciberviolencia

Sebastian Berrios, *Member, Pontificia Universidad Católica de Valparaíso*, Pamela Hermosilla, *Member, Pontificia Universidad Católica de Valparaíso*, Héctor Allende Cid, *Member, Pontificia Universidad Católica de Valparaíso*.

**Abstract—**This research delves into cyber violence within the school context, highlighting how increased access to technology has led to new forms of online violence. It explores various manifestations of this violence and its psychological, emotional, and physical impacts on victims, aggressors, and witnesses. Additionally, the study analyzes associated risk factors and highlights different legislations and school policies implemented worldwide to combat it. The research also examines the crucial roles of families and teachers in the lives of adolescents and emphasizes the importance of prevention initiatives such as school programs, communication campaigns, and workshops. Within this framework, digital education emerges as a key tool to prevent cyberbullying and promote a safe digital environment.

**Keywords—**Cyber violence, Cyberbullying, Cybercrimen.

## I. INTRODUCCIÓN

En los últimos años, el acceso exponencial a recursos tecnológicos ha sido fundamental para facilitar tareas cotidianas, pero también ha incrementado la vulnerabilidad a ataques en la red. Dentro de las topologías del cibercrimen, se identifican cuatro categorías principales: engaño/robo, pornografía, violencia e intrusión. La violencia, en particular, se define como la intervención intencionada y voluntaria para causar daño o influir negativamente en el comportamiento de individuos o grupos. Este tipo de violencia, especialmente en el contexto escolar, no es un fenómeno nuevo pero ha adquirido una nueva dimensión con la masificación de Internet, trasladándose al ámbito virtual. La ciberviolencia, entonces, emerge como una faceta contemporánea de la violencia, adaptándose y evolucionando en el entorno digital.

Se ha determinado ciberviolencia en las escuelas ha descubierto una realidad alarmante que ha cobrado mayor relevancia con el acceso generalizado a las tecnologías. Los efectos de la ciberviolencia son múltiples y significativos,

afectando no solo a las víctimas, sino también a los perpetradores y testigos en aspectos psicológicos, emocionales y físicos. Esto subraya la urgencia de comprender a fondo este fenómeno y de implementar intervenciones efectivas.

La identificación de factores de riesgo asociados tanto a las víctimas como a los agresores revela la complejidad de la ciberviolencia y la necesidad de atender sus causas subyacentes. A nivel global, la adopción de leyes y políticas escolares específicas demuestra un reconocimiento generalizado de la seriedad de la violencia en línea y la necesidad de adoptar medidas preventivas y correctivas. Además, el análisis del papel de las familias y los educadores resalta la importancia de su colaboración para una respuesta integral a este problema. Los esfuerzos preventivos, incluyendo programas escolares, campañas de comunicación y talleres, son esperanzadores y muestran que existen estrategias efectivas para combatir la ciberviolencia. Este estudio enfatiza que la educación digital es clave para prevenir el ciberacoso y otras formas de ciberviolencia. Este enfoque pedagógico ha demostrado ser una manera efectiva de empoderar a estudiantes, padres y educadores, fomentando la conciencia y promoviendo un comportamiento responsable en línea. En un mundo cada vez más digital, una respuesta efectiva a la ciberviolencia requiere el compromiso de toda la comunidad educativa y debe trascender las fronteras nacionales. La integración de todos estos elementos es fundamental para abordar y mitigar el impacto de la ciberviolencia en las escuelas.

## II. CIBERVIOLENCIA

La ciberviolencia engloba actividades en plataformas digitales con intención de causar daño

o sufrimiento. Se manifiesta a través de mensajería instantánea, redes sociales, foros, salas de chat, correo electrónico o comunidades de juegos, adoptando formas como ciberbullying, grooming, sexting, stalking, shaming, y doxing.[3]

El ciberbullying o ciberacoso es acoso e intimidación mediante tecnologías digitales. Los comportamientos que lo caracterizan incluyen:

El ciberacoso incluye diversas prácticas nocivas en entornos digitales: Flaming, que implica enviar mensajes violentos y ofensivos para provocar conflictos; Cyber-harassment, caracterizado por mensajes ofensivos y repetitivos que causan estrés emocional y psicológico; Cyber-stalking, donde el acoso y las amenazas en línea incluyen seguimiento y mensajes intrusivos para intimidar a la víctima; Denigration, que se basa en difundir mensajes falsos o despectivos afectando la reputación y las relaciones sociales de alguien; Impersonation, utilizando información personal de la víctima para suplantar su identidad en línea; Outing, que consiste en persuadir a la víctima para que comparta información personal y luego exponerla; Exclusion, excluyendo a individuos de grupos sociales o chats; y Happy-slapping, la publicación de videos donde se muestra a la víctima siendo agredida o humillada. Estas prácticas reflejan la severidad y variedad del ciberacoso en el ámbito digital.

El ciberacoso y el acoso escolar tradicional comparten varias semejanzas, a pesar de sus diferencias en el medio y la forma de ejecución. Algunas de estas semejanzas incluyen:

- **Intención de Dañar:** Tanto en el ciberacoso como en el acoso escolar tradicional, el agresor tiene la intención de causar daño, humillación o malestar a la víctima.
- **Repetitividad:** Ambos tipos de acoso suelen ser repetitivos. No se trata de un incidente aislado, sino de un patrón de comportamiento que se prolonga en el tiempo.
- **Desequilibrio de Poder:** En ambos casos, existe un desequilibrio de poder percibido. El agresor puede tener más poder debido a la fuerza física, estatus social, conocimiento tecnológico o anonimato.
- **Impacto en la Víctima:** Las víctimas de ambos

tipos de acoso pueden experimentar efectos similares, como ansiedad, depresión, baja autoestima, problemas escolares, e incluso pensamientos suicidas.

- **Dinámica Social:** Tanto el ciberacoso como el acoso escolar pueden involucrar dinámicas de grupo, donde otros pueden participar activamente o ser espectadores pasivos, contribuyendo así a la perpetuación del acoso.
- **Ocultamiento del Agresor:** En ambos casos, el agresor puede tratar de ocultar sus acciones o mantenerse anónimo, especialmente en el ciberacoso, donde el uso de perfiles falsos o anónimos es común.
- **Necesidad de Intervención:** La intervención de adultos, como padres, maestros y otros profesionales, es crucial en ambos tipos de acoso para detener el comportamiento y apoyar a la víctima.
- **Uso de la Tecnología:** Aunque el ciberacoso es específicamente tecnológico, el acoso escolar tradicional también puede emplear la tecnología, como en casos donde el acoso continúa o se extiende a través de dispositivos digitales.

Estas semejanzas subrayan la importancia de abordar ambos tipos de acoso de manera seria y proactiva, reconociendo sus impactos potencialmente dañinos y duraderos en los individuos afectados.[4]

El grooming alude a un adulto que engaña a un menor de edad, donde le ofreciendo o prometiendo cosas que no pueda o piensa cumplir, buscando manipular a la víctima con fines sexuales. [5] En concreto, consiste en un proceso en el que un adulto utiliza recursos tecnológicos para persuadir y victimizar sexualmente a un menor a través de la solicitud de material sexual de dicho menor. El adulto se aprovecha de la inmadurez psicológica y sexual de la víctima, vulnerando sus derechos al normal desarrollo sexual y, por consecuencia, compromete su bienestar mental.

El sexting, o sexteo en español, hace referencia a al envío y/o recibo de material audiovisual, de manera voluntaria, por medio de dispositivos móviles o cámara con determinado sentido sexual. Con el fin de entender mejor este concepto, es necesario tomar en consideración factores claves que permitan determinar la descripción de manera más precisa. En cuanto al origen del material, puede ser producida por la misma persona, producida por otra con el consentimiento, o robado. El contenido del material



implica la dificultad de categorizar la carga sexual en atrevida, erótica o pornográfica. También, si es posible identificar la persona del material y si se puede determinar la minoría o mayoría de edad de dicho individuo. [6]

El stalking es el acto de acosar, acechar, seguir ilegalmente y durante un determinado periodo de tiempo. [7] Se caracteriza por comportamientos deliberados, maliciosos y repetidos de seguir, hostigar y vigilar a otra persona sin autorización ni consentimiento. Dicho comportamiento pretende establecer comunicaciones con la víctima que no son deseadas, y se repiten con tanta frecuencia que la persona afectada teme por su seguridad, viéndose obligada a cambiar su rutina diaria.

El shaming implica avergonzar o humillar a una persona, por medio de una plataforma virtual, con la intención de que la víctima experimente sentimientos de culpa o vergüenza debido a su comportamiento o características personales. Una de las formas en que se manifiesta es el body-shaming, o humillación corporal, que hace alusión a cualquier acción o comentario que juzga y avergüenza a individuos por su apariencia física. [8]

El doxing se refiere a la práctica de buscar y publicar información privada o identificativa de una persona en internet, sin su consentimiento y con el objetivo de avergonzar o hacer daño a la persona afectada. [9]

### III. IMPACTOS PSICOLÓGICOS, EMOCIONALES Y FÍSICOS

Durante las etapas cruciales del desarrollo psicológico en la infancia y adolescencia, es esencial un ambiente sano tanto en el hogar como en la escuela, siendo este último un espacio clave para enseñar valores como el respeto, fundamentales para el buen vivir y la coexistencia social.

La presencia de violencia y ciberviolencia en el ámbito escolar es un problema psicosocial grave con consecuencias negativas.[10] Los impactos de la ciberviolencia en las víctimas se pueden dividir en corto y largo plazo.[11] A corto plazo, incluyen emociones como ira, tristeza, miedo, impotencia y llanto. A largo plazo, se observan efectos físicos y emocionales, como trastornos psicosomáticos, problemas de sueño, migraña, dolor abdominal, anorexia y náuseas, además de emociones negativas persistentes como ansiedad, soledad y depresión.[12]

Las repercusiones en el victimario de ciberviolencia incluyen falta de empatía,

dificultades con las reglas, conductas antisociales, adicción, delincuencia, abuso de poder y trastornos de personalidad.[13]

Los testigos, que observan la violencia y permanecen en silencio por miedo o indiferencia, también sufren consecuencias, tales como sentimientos de culpa, pérdida de empatía, interiorización de conductas antisociales, conflicto emocional y un déficit en su desarrollo moral y emocional. Estos efectos subrayan la importancia de abordar de manera integral el fenómeno de la ciberviolencia en los entornos juveniles.

### IV. FACTORES DE RIESGO

Investigaciones han identificado factores de riesgo que incrementan la probabilidad de que un adolescente sea víctima de bullying. Niños con pocos amigos son más susceptibles al rechazo o exclusión por sus compañeros, convirtiéndolos en blancos fáciles de acoso [14]. Adicionalmente, se ha encontrado que niños con trastornos psiquiátricos tienen un riesgo elevado de ser acosados.

En cuanto al comportamiento del agresor, los estudios han señalado también ciertos factores de riesgo. Un adolescente con altos niveles de ansiedad, dificultad para adaptarse a cambios, tendencia a la frustración y distracción puede exhibir falta de control e impulsividad. Estas características pueden predisponerlo a involucrarse en dinámicas de agresión, asumiendo cualquier rol dentro del espectro del bullying. [14]

### V. FACTORES DE RIESGO QUE AUMENTAN LA VICTIMIZACIÓN POR BULLYING

Los factores de riesgo que pueden aumentar la probabilidad de que un individuo se convierta en víctima de bullying son variados y multifacéticos. Incluyen aspectos individuales, sociales y ambientales:

- Características Personales: Niños y adolescentes con ciertas características personales pueden ser más propensos al bullying. Esto incluye aquellos con baja autoestima, timidez, o aquellos que presentan diferencias físicas, de comportamiento o de aprendizaje notables.

- Problemas Psicosociales: Individuos que

enfrentan problemas psicosociales, como trastornos de ansiedad, depresión, o problemas de conducta, pueden ser más vulnerables al acoso.

- **Dificultades Sociales:** Los niños y adolescentes con dificultades para socializar, como aquellos con pocos amigos o problemas para establecer relaciones, pueden ser blancos fáciles para los acosadores.

- **Percepción de Ser Diferente:** Ser percibido como diferente, ya sea por razones de raza, etnia, género, orientación sexual, religión o discapacidad, puede aumentar el riesgo de ser víctima de bullying.

- **Entorno Familiar y Dinámicas Hogareñas:** Un entorno familiar conflictivo, falta de supervisión parental, o la presencia de violencia en el hogar pueden aumentar la vulnerabilidad al bullying.

- **Entorno Escolar y Clima:** El clima escolar y la cultura de la escuela, incluyendo la actitud de los maestros y administradores hacia el bullying, pueden influir en la prevalencia del acoso. Escuelas con un ambiente hostil o competitivo pueden incrementar los riesgos.

- **Experiencias Previas de Victimización:** Los niños y adolescentes que han sido víctimas de bullying en el pasado son a menudo más susceptibles a ser acosados nuevamente.

- Estos factores pueden interactuar entre sí, creando un complejo panorama de riesgo que requiere enfoques integrales para la prevención y la intervención.[15]

Varios estudios también se han enfocado en el comportamiento del perpetrador de la violencia y, de hecho, se han definido factores de riesgo. Una adolescente con elevados niveles de ansiedad, dificultad para adaptarse a cambios, propensión a la frustración y distracción, podría mostrar falta de control y tendencias impulsivas. Esta combinación de características podría llevarlo a participar en dinámicas de agresión en cualquiera de los roles. [14]

Un estudio, ha identificado 8 problemas que se deben erradicar desde la familia y escuela para evitar la formación de un adolescente que inicie y dirige el acoso escolar. [16]

## VI. CARACTERÍSTICAS OBSERVADAS CON FRECUENCIA EN LOS ADOLESCENTES QUE INICIAN Y DIRIGEN EL ACOSO ESCOLAR

Los adolescentes que inician y dirigen el acoso escolar suelen presentar ciertas características y comportamientos comunes. Estas incluyen:

- **Agresividad y Comportamiento Dominante:** Suelen ser física o verbalmente agresivos y buscan establecer una posición de dominio o poder sobre sus compañeros.

- **Falta de Empatía y Sensibilidad:** A menudo muestran una falta de empatía y no se preocupan por los sentimientos o el bienestar de los demás.

- **Necesidad de Control y Poder:** Tienen un deseo de controlar o influir en los demás y pueden usar el acoso para afirmar su poder o estatus social.

- **Problemas Conductuales y Disciplinarios:** Es común que presenten otros problemas de comportamiento, como desafío a la autoridad, problemas en la escuela o comportamientos delictivos.

- **Influencia de las Relaciones Familiares:** Pueden provenir de hogares donde la disciplina es excesivamente severa, inconsistente, o donde se modelan comportamientos agresivos o abusivos.

- **Habilidades Sociales Pobres o Manipuladoras:** Aunque algunos pueden ser socialmente hábiles, suelen usar estas habilidades de manera manipuladora. Otros pueden tener dificultades en las relaciones sociales saludables.

- **Actitudes y Creencias que Justifican el Acoso:** Pueden tener creencias que justifican el acoso como un comportamiento aceptable o una forma 'normal' de interacción.

- **Baja Autoestima o Inseguridades:** En algunos casos, el acoso puede ser una forma de compensar la baja autoestima o las inseguridades personales.

- **Búsqueda de Atención y Reconocimiento:** Algunos acosadores buscan atención y reconocimiento de sus pares y ven el acoso como un medio para lograrlo.

- **Exposición a la Violencia y Agresión en los Medios:** La exposición regular a la violencia y agresión en los medios puede normalizar estos comportamientos en su percepción.

Estas características no se aplican a todos los acosadores y pueden variar según el individuo y el contexto. Sin embargo, son tendencias comunes observadas en estudios sobre acoso escolar.[15]

## VII. FACTORES DE RIESGO QUE PUEDEN INDUCIR A UN ADOLESCENTE A SER AGRESOR

Los factores de riesgo que pueden predisponer a un adolescente a convertirse en agresor en situaciones de bullying abarcan una gama amplia de elementos individuales, familiares y sociales:

- **Problemas de Conducta y Agresividad:** Los adolescentes que muestran patrones de conducta agresiva, impulsiva o desafiante tienen una mayor tendencia a involucrarse en comportamientos de acoso.
- **Influencias Familiares:** Un entorno familiar caracterizado por la falta de calidez o afecto, disciplina inconsistente o excesivamente severa, o la presencia de violencia y conflictos, puede influir en el desarrollo de comportamientos agresivos.
- **Falta de Empatía y Conciencia Social:** Los jóvenes con bajos niveles de empatía, dificultades en las habilidades sociales o un entendimiento limitado de los efectos de sus acciones en los demás son más propensos a participar en bullying.
- **Presión de Grupo y Búsqueda de Aceptación Social:** La necesidad de aceptación o estatus dentro de un grupo de pares puede llevar a algunos adolescentes a usar la agresión como una forma de establecer su dominio o popularidad.
- **Exposición a la Violencia en los Medios:** La exposición regular a la violencia en los medios de comunicación, como televisión, videojuegos o internet, puede desensibilizar a los adolescentes y hacer que perciban la agresión como un comportamiento normal o aceptable.
- **Historial de Victimización:** Los adolescentes que han sido víctimas de bullying u otras formas de abuso pueden adoptar

comportamientos agresivos como mecanismo de defensa o represalia.

- **Problemas Psicológicos o Emocionales:** Problemas como la ansiedad, depresión o baja autoestima pueden manifestarse en comportamientos agresivos hacia otros.
- **Contexto Escolar y Comunitario:** Un ambiente escolar o comunitario que tolera o no aborda adecuadamente el bullying puede fomentar la continuación de estos comportamientos.

Entender estos factores es crucial para el desarrollo de estrategias efectivas de prevención y tratamiento del comportamiento agresivo en adolescentes.

Otro factor de riesgo incidente en la formación del atacante está asociado a la formación de los padres. La depresión de los padres, es incidente en que dicho niño sea un futuro perpetrador de la violencia. La depresión materna está vinculada al acoso escolar, ya que las madres deprimidas y sus hijos tienden a ser más irritables, críticos y hostiles. Si el padre experimentó bullying durante su niñez, aumenta el riesgo de que sus hijo lo sufran también.

## VIII. LEGISLACIÓN Y POLÍTICAS ESCOLARES

Gobiernos y organizaciones internacionales están implementando políticas para combatir la ciberviolencia, especialmente en el ámbito escolar, enfocándose en la prevención y educación de niños y jóvenes. Este enfoque es crucial, ya que estas etapas son claves para detener la ciberviolencia a tiempo.

En España, el ciberacoso está regulado por el Código Penal en su artículo 172 ter, que sanciona el acoso persistente y reiterado sin autorización legítima, incluyendo vigilancia, contacto no deseado y uso indebido de datos personales, con penas de prisión o multa.[17][18]

En Estados Unidos, el US Code en su sección 18, sanciona el delito de stalking, castigando comportamientos que causen estrés o pongan en peligro la vida de una persona mediante servicios postales o interactivos en línea, con multas y hasta cinco años de prisión.[19]

En Chile, aunque el ciberbullying no está regulado como en otros países, la Ley N° 20.536 de violencia escolar y la Ley N° 21.153 modifican el Código Penal para tipificar el acoso sexual y el acoso

sexual en espacios públicos, incluyendo actos cometidos a través de medios tecnológicos. [17][20] Además, la Ley N° 21.369 aborda específicamente el acoso sexual en la educación superior, reconociendo su naturaleza virtual o telemática. [21]

Estas legislaciones reflejan un esfuerzo global por abordar la ciberviolencia, aunque aún queda trabajo por hacer para asegurar una protección completa en el espacio digital.

El proyecto de ley en Chile destinado a combatir la violencia digital tiene un enfoque integral, apuntando tanto a la violencia digital en general como a la dirigida específicamente hacia las mujeres. Su principal objetivo es establecer un marco legal claro que prohíba, tipifique y sancione diversas formas de violencia digital. Entre las conductas que busca penalizar se encuentran el acoso digital, la difusión no consentida de contenido íntimo, la suplantación de identidad, y la propagación de información falsa. Estas medidas son fundamentales para abordar la creciente preocupación sobre la seguridad y el bienestar de los individuos en el ámbito digital.

Además, el proyecto de ley no se limita a aspectos punitivos, sino que también contempla iniciativas proactivas. Propone la creación de programas de educación digital, los cuales son esenciales para prevenir la violencia digital educando a la población sobre el uso responsable de la tecnología y las consecuencias de las acciones en línea. Asimismo, el proyecto pone un énfasis especial en la reparación para las víctimas de violencia digital, buscando no solo sancionar a los agresores sino también ofrecer apoyo y recursos a quienes han sufrido daño.

Este enfoque dual, que combina medidas punitivas con programas educativos y de apoyo, refleja un entendimiento de que la lucha contra la violencia digital requiere tanto de prevención como de castigo, y un compromiso particular con la protección y empoderamiento de las mujeres, que a menudo son desproporcionadamente afectadas por este tipo de violencia.

## IX. ROLES

El entorno familiar juega un rol crucial en la satisfacción vital de los adolescentes, siendo la cohesión familiar un factor protector contra la ciberviolencia y, en contraste, los conflictos familiares un factor de riesgo para la victimización y perpetración del ciberacoso. [22] La pandemia de Covid-19 ha exacerbado el ciberacoso, afectando negativamente la satisfacción de vida de los

adolescentes, lo que subraya la importancia de fortalecer los vínculos familiares positivos para contrarrestar estos efectos adversos.

Por otro lado, los profesores enfrentan retos significativos en la gestión del ciberacoso. A menudo, tienden a sobrestimar la disposición de los estudiantes a reportar estos incidentes y pueden no tomar medidas efectivas para su prevención. [23] Esto resalta la urgencia de incluir estrategias de prevención de ciberacoso en la formación docente y la necesidad de actualizar sus conocimientos en tecnología. Una mejor comprensión y manejo de la violencia escolar en el ciberespacio es fundamental para crear un ambiente educativo más seguro y saludable.

## X. PREVENCIÓN

En 2017, Chile implementó un programa antiacoso originado en Finlandia en 2007, llamado KiVa, con el objetivo de prevenir e intervenir en casos de bullying en establecimientos educativos. KiVa se distingue por su enfoque en la prevención, intervención y supervisión periódica de los establecimientos educativos. El programa incluye medidas universales como talleres y juegos en línea para estudiantes, y acciones indicadas para casos específicos de bullying, involucrando entrevistas individuales con los afectados, incluyendo a la víctima, al agresor, cómplices y espectadores, a cargo de un equipo docente especializado. [24] Además, en 2015 se lanzó Brave Up en Chile con el fin de mejorar la comunicación entre instituciones educativas y familias mediante canales de comunicación virtuales confidenciales. Esta aplicación proporciona un diagnóstico de la realidad escolar y ofrece recomendaciones y herramientas para una mejor gestión. Incluye un espacio de comunicación confidencial para que los estudiantes afectados por la violencia escolar puedan comunicarse en tiempo real con el responsable de la convivencia escolar dentro de las instalaciones. La aplicación funciona mediante notificaciones, contenidos informativos y un botón de denuncia para informes anónimos o no anónimos sobre problemas en la comunidad escolar.

Adicionalmente, se han desarrollado campañas comunicacionales y talleres enfocados en prevenir la violencia cibernética. Estos talleres buscan fomentar una ciudadanía digital responsable y son parte de un esfuerzo educativo más amplio para

sensibilizar sobre el uso de redes sociales e internet, tanto para estudiantes como para familias y profesores. Estas iniciativas reflejan un compromiso integral con la prevención y el manejo de la violencia escolar y cibernética en Chile.[24]

Además de los programas KiVa y Brave Up, Chile ha implementado campañas comunicacionales y talleres enfocados en prevenir la violencia cibernética. Algunos de estos son:

- **#NoMásCiberBullying:** Esta campaña combate el acoso virtual. Inició con cuatro ciclos de diálogo destinados a concienciar sobre el ciberacoso que afecta a jóvenes y familias. Expertos de diferentes áreas abordaron temas relevantes, como la influencia de la dopamina en los jóvenes, la importancia de la identidad virtual, las huellas digitales, la convivencia escolar digital, el papel de los testigos y maneras efectivas de mejorar la comunicación en entornos virtuales entre familias y sus hijos.[24]
- **#ElijoSerTestigo:** Es una campaña contra el bullying y ciberbullying que alienta a los testigos de estos abusos a denunciarlos. Reconoce que los testigos juegan un papel crucial en detener el abuso, ya que su actitud puede frenar o fomentar el acoso. Originada en la Fundación Ad Council de Estados Unidos, esta iniciativa llegó a Chile en 2018, impulsada por Ripley y la Fundación Volando en V, y ha sido adoptada por aproximadamente 100 instituciones educativas municipales y más de 20 colegios privados en diversos municipios.[24]

Estas campañas y talleres demuestran un compromiso activo con la educación y sensibilización sobre la violencia cibernética, buscando no solo informar, sino también empoderar a estudiantes, familias y educadores para que se conviertan en agentes activos en la prevención y respuesta al ciberacoso en Chile. Proteger tus datos personales y prevenir el ciberbullying son pasos esenciales para mantener una experiencia segura en línea. Aquí te presentamos algunos consejos útiles:

- **Concientización:** Es fundamental aprender a reconocer el ciberbullying y sus formas, informarse sobre cómo manejarlo y cómo ayudar a quienes lo sufren.
- **Configuración de Privacidad:** Limita la cantidad de información personal visible públicamente y evita compartir datos sensibles en línea.
- **Reporta el Ciberbullying:** Si eres víctima, reporta el comportamiento a la plataforma correspondiente y/o a las autoridades. En Chile, puedes contactar a Ciberdelito Santiago para hacer tu denuncia.
- **Guarda Evidencia:** Conserva capturas de pantalla y otros registros de interacciones de ciberbullying como evidencia.
- **No Aliméntes al Acosador:** Evita responder a los comentarios ofensivos y no compartas información personal en respuesta a mensajes amenazantes.
- **Bloquea y Filtra:** No dudes en bloquear o eliminar a personas que te hagan sentir incómodo en redes sociales.
- **Comunicación Abierta:** Habla con amigos, familiares o profesores sobre cualquier experiencia de ciberbullying.

En cuanto a la educación digital, es clave para prevenir y abordar el ciberbullying. Algunos temas importantes que pueden incorporarse en la educación digital son:

- **Concientización sobre el Ciberbullying:** Definición, formas, ejemplos y consecuencias emocionales y psicológicas.
- **Ética Online:** Fomentar el respeto, la empatía y la responsabilidad en el entorno digital.
- **Seguridad en la Privacidad:** Enseñar a configurar y mantener la privacidad en perfiles en línea y explicar los riesgos de compartir información personal.
- **Habilidades de Comunicación en Línea:** Fomentar la comunicación efectiva y respetuosa.
- **Detección y Respuesta:** Reconocer el ciberbullying y la importancia de informarlo.
- **Énfasis en la Empatía:** Fomentar la empatía hacia las experiencias de los demás en el entorno en línea.
- **Prevención y Estrategias de Afrontamiento:** Discutir estrategias para prevenir el ciberbullying y enseñar a afrontarlo.
- **Legislación y Consecuencias Legales:** Informar sobre las leyes relacionadas y las consecuencias de participar en ciberbullying.
- **Desarrollo de Ciudadanía Digital:** Enseñar



a ser ciudadanos digitales responsables y respetuosos.

- Colaboración con Padres y Comunidad: Involucrar a estos grupos en la educación digital.

Integrar estos temas en la educación digital puede crear un entorno en línea más seguro y promover comportamientos positivos entre los estudiantes.

## XI. EVIDENCIAS

En el actual y acelerado mundo digital, la ciberseguridad en la educación se ha vuelto un aspecto crítico. La creciente integración de la tecnología en la experiencia educativa demanda un enfoque riguroso en la seguridad digital, especialmente en entornos escolares. Esta sección analiza incidentes reales que han afectado a estudiantes, proporcionando una perspectiva valiosa sobre los desafíos y amenazas que enfrentamos en este ámbito. Estos casos destacan la importancia de implementar medidas de seguridad digital efectivas en las aulas para proteger la integridad y bienestar de la comunidad educativa.

Uno de estos incidentes ocurrió en Sevilla, donde un joven fue condenado a pagar una multa de 100 euros por publicar en Tuenti un fotomontaje ofensivo de un compañero de clase. La imagen, que permaneció visible durante dos meses, provocó comentarios despectivos de otros estudiantes. El juez consideró que el acto constituyó un "deliberado ataque a la dignidad personal" de la víctima. Además, varios compañeros menores de edad implicados en el caso fueron condenados a trabajos comunitarios.[26]

Otro caso lamentable es el de Phoebe Prince, una estudiante inmigrante irlandesa de 15 años, que se suicidó después de ser acosada física y psicológicamente por sus compañeros de escuela, tanto personalmente como a través de móviles e Internet. Nueve adolescentes fueron juzgados por este acoso, que incluso continuó en línea después de su muerte.[27]

En Cleveland, una confrontación entre dos adolescentes que comenzó en MySpace escaló hasta resultar en un tiroteo. Una de las menores implicadas recibió un disparo en la oreja durante un enfrentamiento que involucró armas de fuego y un grupo de amigos.[28]

Estos casos resaltan la urgencia de abordar la ciberseguridad en los entornos educativos y la necesidad de tomar medidas proactivas para prevenir tales incidentes, protegiendo a los estudiantes en el cada vez más complejo entorno digital.

## XII. CIBERSEGURIDAD PARA NIÑOS Y ADOLESCENTES

El tema de la ciberseguridad para niños y adolescentes es crucial en la era digital actual. Aquí se resumen los riesgos principales y se ofrecen recomendaciones para mantenerse seguros:[29]

- Peligro de Extraños (Stranger Danger): Los niños pueden ser blanco de adultos malintencionados que buscan conectar emocionalmente para causar daño. Es fundamental educar a los niños sobre la importancia de no interactuar con desconocidos en línea y siempre informar a un adulto de confianza si se encuentran en una situación incómoda.
- Phishing: Los niños son especialmente susceptibles a esta táctica de engaño que busca robar información personal. Es vital enseñarles a no compartir datos personales en línea y a ser escépticos ante correos electrónicos o mensajes sospechosos.
- Robo de Identidad: Con el aumento de la actividad en línea y en redes sociales, los niños están en riesgo de que su información personal sea robada. Es importante enseñarles a usar contraseñas seguras y a no divulgar información sensible en internet.[30]
- Adicción a Internet: Aunque no es un riesgo directo de seguridad, puede conducir a comportamientos peligrosos en línea. Fomentar un uso equilibrado y responsable de internet es clave.[30]
- Riesgos Económicos: Las apuestas en línea y estafas financieras pueden atrapar a los niños. Es esencial educarlos sobre los peligros de juegos con opciones de pago y enseñarles a ser cautelosos con las ofertas que parecen demasiado buenas para ser verdad. Para garantizar la seguridad de los niños y adolescentes en línea, es esencial:
  - Educación Continua: Mantener conversaciones regulares sobre los riesgos en línea y cómo manejarlos.
  - Supervisión Adecuada: Monitorear la

actividad en línea de los niños y establecer reglas claras sobre el uso de internet.

- Uso de Herramientas de Seguridad: Instalar software de seguridad y utilizar configuraciones de privacidad en redes sociales y dispositivos.
  - Fomentar la Confianza: Animar a los niños a hablar sobre sus experiencias en línea y a reportar cualquier cosa inusual o preocupante.
- La protección de los niños en el entorno digital es un esfuerzo conjunto que requiere la participación de padres, educadores y los propios niños.

### XIII. CONCLUSIÓN

El estudio profundo de la ciberviolencia en las escuelas ha descubierto una realidad alarmante que ha cobrado mayor relevancia con el acceso generalizado a las tecnologías. Los efectos de la ciberviolencia son múltiples y significativos, afectando no solo a las víctimas, sino también a los perpetradores y testigos en aspectos psicológicos, emocionales y físicos. Esto subraya la urgencia de comprender a fondo este fenómeno y de implementar intervenciones efectivas.

La identificación de factores de riesgo asociados tanto a las víctimas como a los agresores revela la complejidad de la ciberviolencia y la necesidad de atender sus causas subyacentes. A nivel global, la adopción de leyes y políticas escolares específicas demuestra un reconocimiento generalizado de la seriedad de la violencia en línea y la necesidad de adoptar medidas preventivas y correctivas. Además, el análisis del papel de las familias y los educadores resalta la importancia de su colaboración para una respuesta integral a este problema. Los esfuerzos preventivos, incluyendo programas escolares, campañas de comunicación y talleres, son esperanzadores y muestran que existen estrategias efectivas para combatir la ciberviolencia. Este estudio enfatiza que la educación digital es clave para prevenir el ciberacoso y otras formas de ciberviolencia. Este enfoque pedagógico ha demostrado ser una manera efectiva de empoderar a estudiantes, padres y educadores, fomentando la conciencia y promoviendo un comportamiento responsable en línea. En un mundo cada vez más digital, una respuesta efectiva a la ciberviolencia requiere el compromiso de toda la comunidad educativa y debe trascender las fronteras nacionales. La integración de todos estos elementos es fundamental para abordar y mitigar el impacto de la ciberviolencia en las escuelas.

El estudio profundo de la ciberviolencia en las

escuelas ha descubierto una realidad alarmante que ha cobrado mayor relevancia con el acceso generalizado a las tecnologías. Los efectos de la ciberviolencia son múltiples y significativos, afectando no solo a las víctimas, sino también a los perpetradores y testigos en aspectos psicológicos, emocionales y físicos. Esto subraya la urgencia de comprender a fondo este fenómeno y de implementar intervenciones efectivas.

La identificación de factores de riesgo asociados tanto a las víctimas como a los agresores revela la complejidad de la ciberviolencia y la necesidad de atender sus causas subyacentes. A nivel global, la adopción de leyes y políticas escolares específicas demuestra un reconocimiento generalizado de la seriedad de la violencia en línea y la necesidad de adoptar medidas preventivas y correctivas. Además, el análisis del papel de las familias y los educadores resalta la importancia de su colaboración para una respuesta integral a este problema. Los esfuerzos preventivos, incluyendo programas escolares, campañas de comunicación y talleres, son esperanzadores y muestran que existen estrategias efectivas para combatir la ciberviolencia.

Este estudio enfatiza que la educación digital es clave para prevenir el ciberacoso y otras formas de ciberviolencia. Este enfoque pedagógico ha demostrado ser una manera efectiva de empoderar a estudiantes, padres y educadores, fomentando la conciencia y promoviendo un comportamiento responsable en línea. En un mundo cada vez más digital, una respuesta efectiva a la ciberviolencia requiere el compromiso de toda la comunidad educativa y debe trascender las fronteras nacionales. La integración de todos estos elementos es fundamental para abordar y mitigar el impacto de la ciberviolencia en las escuelas.

### XIV. REFERENCIAS

- [1] D. Wall, Cybercrimes and the Internet (From Crime and the Internet, P 1-17, 2001, David S. Wall, ed. -- See NCJ-213504), 2001.
- [2] E. C. Montoya, «Exploración del concepto de violencia y sus implicaciones en educación,» Scielo, 2016.
- [3] M. Vismara, N. Girone, D. Conti, G. Nicolini y . B. Dell'Osso, «The current status of Cyberbullying research: a short review of the literature,» 2022.
- [4] C. S. Eizaguirre Monzón, «Propuesta de un cuestionario para la detección precoz del ciberacoso entre escolares,» 2016.
- [5] P. Alonso Gonzalez, «Online Grooming,» Madrid, 2019.

- [6] M. I. Fajardo Caldera, M. Gordillo Hernández y A. B. Regalado Cuenca, «SEXTING: NUEVOS USOS DE LA TECNOLOGÍA Y LA SEXUALIDAD EN ADOLESCENTES,» *International Journal of Developmental and Educational Psychology*, vol. 1, n° 1, pp. 521-533, 2013.
- [7] D. Donoso Hidalgo y I. González Campos, «El Stalking: Un análisis comparado de la regulación Penal nacional y el Derecho Penal español para una propuesta de tipificación especial en el Código Penal chileno,» Santiago de Chile, 2022.
- [8] L. Adelardi, «Bullying, gordofobia y salud mental,» *Revista Límbica*, vol. III, n° 4, 2022.
- [9] D. M. Douglas, «Doxing: a conceptual analysis,» *Ethics Inf Technol*, Enschede, 2016.
- [10] N. Balluerka, J. Aliri, O. Goni-Balentiaga y A. Gorostiaga, «Asociación entre el bullying, la ansiedad y la depresión en la infancia y la adolescencia: el efecto mediador de la autoestima,» *Revista de Psicodidáctica*, n° 28, pp. 26-34, 2023.
- [11] K. Kopecky y R. Szołkowski, «Cyberbullying, cyber aggression and their impact on the victim – The teacher,» *Telematics and Informatics*, n° 34, pp. 506-517, 2017.
- [12] A. Sourander, A. Brunstein Klomek, M. Ikonen, J. Lindroos, T. Luntamo, M. Koskelainen y H. Helenius,
- [13] «Psychosocial risk factors associated with cyberbullying among adolescents: a population-based study,» *Arch. Gen. Psychiatry*, vol. 67, n° 7, pp. 720- 728, 2010.
- [14] M. E. Morales-Ramírez y M. Villalobos-Cordero, «El impacto del bullying en el desarrollo integral y aprendizaje desde la perspectiva de los niños y niñas en edad preescolar y escolar,» *Revista Electrónica Educare*, vol. 21, n° 3, pp. 25-44, 2017.
- [15] R. MUSALEM B. y P. CASTRO O., «QUÉ SE SABE DE BULLYING,» Santiago de Chile, 2014.
- [16] S. R., « Bullying and victimization among children,» *Adv. Pediatr*, vol. 60, n° 1, pp. 33-51, 2013. O. Y. Díaz, «Bullying, identifying elements, psychological profile and consequences, students in elementary and secondary education,» 2012.
- [17] C. Weidenslaufer, «Acoso cibernético (ciberacoso). Derecho nacional y comparado,» Biblioteca del Congreso Nacional de Chile, 2022.
- [18] España, «Agencia Estatal Boletín Oficial del Estado,» 24 Noviembre 1995. [En línea]. Available: <https://www.boe.es/eli/es/lo/1995/11/23/10/c on>.
- [19] Oficina del Consejo de Revisión de Ley de la Cámara de Representantes, «18 U.S. Code § 2261A - Stalking,» 22 Diciembre 2022. [En línea]. Available: <https://www.law.cornell.edu/uscode/text/18/2261A>.
- [20] Congreso Nacional de Chile, «LEY 21153 | MODIFICA EL CÓDIGO PENAL PARA TIPIFICAR EL DELITO DE ACOSO SEXUAL EN ESPACIOS PÚBLICOS,» 3 Mayo 2019. [En línea]. Available: <https://bcn.cl/2ffd3>.
- [21] Congreso Nacional de Chile, «LEY 21369: REGULA EL ACOSO SEXUAL, LA VIOLENCIA Y LA DISCRIMINACIÓN DE GÉNERO EN EL ÁMBITO DE LA EDUCACIÓN SUPERIOR,» 15 Septiembre 2021. [En línea]. Available: <https://bcn.cl/2rhez>.
- [22] M. E. Rodríguez-Rivas, J. J. Varela, C. González y M. J. Chuecas, «The role of family support and conflict in cyberbullying and subjective well-being among Chilean adolescents during the Covid-19 period,» CellPress, Santiago de Chile, 2022.
- [23] Y.-y. Huang y C. Chou, «Revisiting cyberbullying: Perspectives from Taiwanese teachers,» *Computers & Education*, n° 63, pp. 227-239, 2013.
- [24] A. S. O. M. R. C. F. B. P. Javier Guevara M., «bibliotecadigital.mineduc.cl,» s.f s.f 2018. [En línea]. Available: <https://bibliotecadigital.mineduc.cl/bitstream/handle/20500.12365/18840/E18-0032.pdf?sequence=1&isAllowed=y>.
- [25] G. d. Chile, «¿Cómo y cuando reportar?,» 12 Julio 2019. [En línea]. Available: <https://www.csirt.gob.cl/como-y-cuando-reportar/>.
- [26] «Condenados por atacar la dignidad de un compañero en Tuenti,» 26 Mayo 2009. [En línea]. Available: <http://stop-ciberbullying.blogspot.com/2009/05/condenados-por-atacar-la-dignidad-de-un.html>.
- [27] «Ciberbullying,» [En línea]. Available: <https://www.ciberbullying.com/cyberbullying/casos-de-ciberbullying/>.
- [28] «Un caso de bullying en MySpace acaba en tiroteo,» 5 Abril 2009. [En línea]. Available: <http://stop->

ciberbullying.blogspot.com/2009/04/un-caso-de-bullying-en-myspace-acaba-en.html.

- [29] S. Álvarez, «Casos de delitos informáticos aumentaron un 61% durante 2021 y 2022 Fuente: Chocale.cl - https://chocale.cl/2023/06/casos-de-delitos-informaticos-aumentaron-un-61-durante-2021-y-2022/ Si quieres utilizar este contenido, solo te pedimos citarnos junto a,» 27 Junio 2023. [En línea]. Available: https://chocale.cl/2023/06/casos-de-delitos-informaticos-aumentaron-un-61-durante-2021-y-2022/.
- [30] F. Quayyum, D. S. Cruzes y L. Jaccheri, «Cybersecurity awareness for children: A systematic literature review,» International Journal of Child- Computer Interaction, n° 30, 2021.
- [31] E. PAÍS, «http://stop-ciberbullying.blogspot.com/,» Condenado a pagar 100 euros por reírse en 'Tuenti' de un compañero, p. 1, 23 mayo 2009.
- [32] J. Guevara M., A. Sthioul O., M. Rivera C. y F. Barrientos P., «Ciberacoso: una revisión internacional y nacional de estudios y programas,» Santiago de Chile, 2018.

## XV. BIOGRAFIAS



**Pamela Hermosilla** nacida en Valparaíso, Chile, el 8 de octubre de 1974. Graduada de Universidad Técnica Federico Santa María (UTFM Ingeniero Civil en Informática (UTFSM), Diplomada en Comercio Electrónico y Logística Empresarial (UTFSM), Auditor Interno ISO 9001 (Brain & Cia Consultores), MBA of Chief Information Officer CIO (Abet Open University), Diplomada en Docencia Universitaria de la Pontificia Universidad Católica de Valparaíso (PUCV), Diplomada en Formación Virtual Universitaria (PUCV), Symposium for Entrepreneurship Educators (Luksic Scholars - Babson College). Asesorías: miembro del Consejo Público Privado de la red Fortalece Pyme, Valparaíso - Corfo, integrante del Board de Directores, de la incubadora Chrisalys PUCV. Desarrollo profesional en áreas de Aseguramiento de calidad en gestión de proyectos, Planificación estratégica organizacional, Rediseño curricular basado en competencias, Habilidades de Innovación y emprendimiento en estudiantes de ingeniería, Gamificación en el proceso de enseñanza y aprendizaje.



Dr.(c)Sebastián Berrios nacido el 7 diciembre de 1986. Actualmente candidato a doctor en Ingeniería informática en la Pontificia Universidad Católica de Valparaíso. Graduado de Ingeniería Civil en Computación e Informática en la Universidad De Las Américas. Magíster en Ciencias de la Ingeniería y Magíster en Ingeniería en Informática en la Pontificia Universidad Católica de Valparaíso. Actualmente docente del área de Ciberseguridad y Administrador de TI de la escuela de ingeniería informática de la Pontificia Universidad Católica de Valparaíso. Cursando un Diplomado de Inclusión en Educación en la Pontificia Universidad Católica de Valparaíso, con una duración de 140 horas. Además, se cursó un Diplomado en Seguridad de la Información de 132 horas en la Universidad de Chile y un Diplomado en Ciberseguridad de 96 horas en la misma universidad. También se obtuvo un Diplomado en Ciberseguridad de 100 horas en el Instituto Profesional IACC.



**Dr. Héctor Allende** destacado profesional en el campo de la ingeniería informática. Obtuvo su Doctorado en Ingeniería Informática en 2015 en la Universidad Técnica Federico Santa María, Chile, un reconocido centro de estudios en la región. Antes de ello, en 2009, completó su Magíster en Ciencias de la Ingeniería Informática y se graduó como Ingeniero Civil Informático en la misma universidad. Su formación académica en estas prestigiosas instituciones le ha proporcionado una sólida base en la ingeniería informática, permitiéndole desarrollarse y destacarse en su campo.

# Componentes y Valoración Docente a las Credenciales Digitales con Blockchain

Miguel Cordova  
Continental University  
Huancayo, Perú  
0000-0003-0810-1618

**Abstract**—Esta investigación recoge las buenas prácticas a nivel de la educación formal y no formal de las credenciales digitales, para describir una solución tecnológica basada en Blockchain que a través del estándar OpenBadge integra el LMS Moodle y una interfaz SaS para la gestión de credenciales que permitan la verificación descentralizada y la exportación de la misma a las redes sociales en un grupo de 97 docentes, quienes aprobaron el programa de competencias digitales, se comparten los resultados donde se evidencia una clara aceptación y valoración de esta práctica educativa emergente en sus ítems: utilidad, facilidad, compartir, soporte, valor, satisfacción, importancia, experiencia y la preferencia de tomar un curso próximo que también emitan credenciales digitales.

**Keywords**— *credencial digital, insignias, open badge, blockchain, tecnología.*

## I. INTRODUCCIÓN

Esta investigación, surge del reclamo de muchas empresas e industrias acerca de la escasez mundial del talento [1], [2], [3], [4] y [5], pero se centra, en que también a pesar de dicho reclamo que son válidas, nuestros sistemas educativos y empresariales, aún les cuesta entender acerca de las beneficios y oportunidades que brindan las credenciales digitales; así diversas investigaciones muestran que “los empleadores a menudo no reconocen esas credenciales y prefieren la práctica más familiar de evaluar a los candidatos a un puesto de trabajo en función de sus títulos universitarios y su experiencia” [6] y [7], esto desnuda que “varios profesionales de recursos humanos y los gerentes de contratación tienen dificultades para entender la relevancia de las credenciales alternativas” [7], lo cual puede justificarse por haber un obstáculo técnico “los sistemas automatizados de seguimiento de candidatos que utilizan muchas empresas para seleccionar a los candidatos, a menudo no reconocen las credenciales” [6], pero más grave aún, es que cuestiona – una vez más – la rigidez de nuestros sistemas universitarios dado que les cuesta flexibilizar el diseño curricular, los procesos y los sistemas para lograr una gobernanza que promueva, incorpore, reconozca y acredite las competencias, a través de las credenciales digitales; así este documento, parte de la premisa que hay una fuerza laboral emergente conformada por estudiantes y trabajadores que van valorando y aprovechando espacios de formación formal y no formal que emiten credenciales digitales.

En esta nueva fuerza laboral pospandémica, quedaron atrás los días de la documentación tradicional como los currículums, cartas de presentación, documentos formales para llevar a cabo una matrícula o los certificados tradicionales, algunos empleadores están abiertos a medios nuevos e innovadores de entender las habilidades y

calificaciones de los empleados [8]; así, “casi la mitad de los trabajadores estadounidenses afirman tener algún tipo de credencial alternativa, y entre los que no la tienen, el 49% ha considerado ganarla” [6], en cuanto a la percepción de valor de las credenciales son optimista “el 72% de los trabajadores están de acuerdo en que las credenciales alternativas son una forma asequible de obtener la experiencia necesaria para ingresar a un nuevo trabajo” [6] y el “77% está de acuerdo en que esos programas y certificados aumentarían sus posibilidades de ser contratados” [6]. Así “las credenciales digitales alternativas han generado grandes expectativa en amplios segmentos de la población porque les permite lograr certificaciones que dan fe de las competencias obtenidas” [9], “centrándose en la aplicación práctica de los conocimientos adquiridos (competencias) o de los logros académicos por separado” [10] y que además “toman menos tiempo, son más flexibles y están alineadas con las demandas del mercado laboral” [11].

## II. CREDENCIALES DIGITALES

Las credenciales alternativas hacen referencia a cualquier “certificación profesional, reconocimiento de aprendizaje o insignia que indique las habilidades” [8] logradas “por un estudiante, un trabajador o incluso una persona fuera del sistema educativo formal, en un campo o disciplina” [8]. Los tipos más comunes de credenciales alternativas que poseen los empleados son “los certificados de capacitación (52%), los certificados de finalización de cursos (48%) y las certificaciones industriales o profesionales (38%)” [8], cifras obtenidas del reporte “The Rise of Alternative Credentials in Hiring” [12]. Y es que estas credenciales digitales además de ser reconocidas por más empresas e industrias, son “menos costosas que un título universitario y están diseñados para ayudar a preparar a los trabajadores para mejores trabajos” [7]. Alrededor del 45% de los 1525 trabajadores estadounidenses encuestados [12] tienen una credencial alternativa. De ellos, “el 68% cree que les ha ayudado a progresar en sus carreras” [12]. Las credenciales alternativas a menudo “atraen a los trabajadores que han tomado rutas más tortuosas hacia sus campos” [7], como veteranos, madres de familia, adultos jóvenes que pasaron por alto la universidad, técnicos profesionales que aspiran a un título universitario, a quienes se reincorporaron a la fuerza laboral y personas que cambiaron de carrera; en general, gente que trabaja con deseo de superación académica y profesional, este avance en la mayoría de los casos, proveídos desde la educación no formal - va en sentido contrario - al avance de la educación formal universitaria; cuya tendencia a la disminución de la matrícula universitaria que “en general ha disminuido un 5%, y la cantidad de estudiantes de primer año recién matriculados ha disminuido un 9%” [7] que se presenta

desde el 2019 y se acentuó más en tiempos de pandemia. Muchos futuros estudiantes citan el “alto costo de la universidad y las interrupciones de la pandemia como razones para no inscribirse” [13], el estudio revela que inclusive muchos graduados de la escuela secundaria están “aplazando la universidad, ingresando directamente a la fuerza laboral o al ejército, o educándose a sí mismos fuera del sistema de títulos universitarios” [13]. Así, por ejemplo, “casi 9 de cada 10 miembros de la Generación Z dicen que aprenden a través de medios alternativos, como vídeos de YouTube, programas de certificación y pasantías” [13, p. 3].

Esta preferencia hacia las credenciales digitales, no sólo son valorados por los estudiantes y los trabajadores, sino está cobrando mayor aceptación del sector empresarial y la industria. “La mayoría de 500 ejecutivos estadounidenses y 1200 supervisores encuestados por SHRM consideran que los empleados acreditados tienen un mejor desempeño” [12]. “Las credenciales alternativas son clave para descubrir el talento sin explotar, especialmente cuando se trata de aquellos solicitantes de empleo que pueden no tener la oportunidad de desarrollar habilidades de una manera tradicional, pero que tienen las competencias que necesitan para tener éxito” [14], estos mismos líderes laborales, también consideran que las credenciales digitales “son valiosas para el desarrollo de los empleados y creen que los empleados que las logran, tienen más credibilidad” [12]; sin embargo, aún “los ejecutivos, supervisores y profesionales de recursos humanos aún valoran más la experiencia laboral y los títulos universitarios tradicionales que las credenciales alternativas” [12]. Pero, los beneficios de este tipo de reconocimiento hacia las credenciales digitales, se van haciendo más evidentes; “la mayoría de los ejecutivos, supervisores y profesionales de RR.HH. creen que incluir credenciales alternativas en las decisiones de contratación puede mejorar la diversidad general del lugar de trabajo” [6]. Por ejemplo, cuando los empleadores contratan mediante un proceso de contratación “basado en habilidades” en lugar de basar sus decisiones en currículums, el número de mujeres contratadas en puestos de responsabilidad aumenta casi un 70% [15]. Y en la industria de la tecnología, los bootcamps de programación ya se consideran formas aceptables de educación para los mejores puestos [8]. “Las credenciales digitales pueden permitir el aprendizaje de los trabajadores, ya sea que estén adquiriendo nuevas habilidades o perfeccionando las antiguas, y proporcionan un camino hacia un grupo de talentos más diverso para los empleadores” [6]. Así, hacemos referencia a un nuevo ecosistema educativo para el trabajo “basado en registros y credenciales de aprendizaje interoperables, que permitirá a las personas encuentren trabajos alineados con su experiencia y habilidades y a los empleadores identificar el mejor talento alineado con roles laborales esenciales” [16].

### III. BUENAS PRÁCTICAS DE CREDENCIALES DIGITALES EN LA EDUCACIÓN FORMAL Y NO FORMAL

Según [9], podemos identificar “dos tipos de credenciales alternativas: las formales que son ofrecidas por instituciones de educación superior y las no formales, definidas como credencial para el empleo y la acreditación a los programas diseñados para capacitar personas en el ejercicio de labores técnicas específicas” [17], ofrecidas por los propios empleadores, organizaciones, comunidades y plataformas MOOC que no emiten grados ni títulos de carácter oficial, así que en esta investigación decidimos denominarlos

credenciales digitales que pueden ser complementarios o alternativos.

#### A. Credenciales Digitales Formales

Tomando como referencia a [9], se destacan iniciativas y experiencias muy interesantes y prometedoras acerca de la acreditación y emisión de credenciales digitales alternativas en la academia que busca responder la brecha de competencias denominada “brecha de habilidades” entre lo que las Universidades proveen y lo que el sector empresarial e industrial requiere. Por ejemplo, la Universidad del Sur de Florida (USF), a través del programa Career Readiness Badging Program (CRBP) “ayuda a los estudiantes a pensar sobre sus estudios y experiencias universitarias en términos que se aplican al trabajo del mundo real, así como a comunicar claramente su potencial y valor a posibles empleadores” [18], este programa consta de ocho módulos alineados al desarrollo de competencias blandas y laborales y una novena que es una insignia final que lo acredita para el trabajo.

En los Países Bajos, SurfNet que es una organización colaborativa de más de 100 instituciones ofrece “a más de 750000 estudiantes, profesores y científicos acceso a Internet de alta velocidad e instalaciones de investigación. Como parte de su misión de impulsar la innovación en el sistema de educación superior holandés” [19]. Southern New Hampshire University (SNHU), “está utilizando insignias digitales para que el aprendizaje sea relevante para los jóvenes desatendidos que luchan por ver el valor de la educación tradicional” [20]. Digital Learning Organization (LRNG) está abordando este problema “a través de una plataforma en línea que permite a los jóvenes para buscar oportunidades de aprendizaje que pueden conducir directamente a empleos” [21]. Y con la fusión con SNHU en 2018 “se creó una de las soluciones de aprendizaje y fuerza laboral más grandes e innovadoras en los Estados Unidos, LRNG está ampliando el acceso a la educación superior y transformando vidas a través de vías de titulación flexibles y asequibles y nuevos tipos de oportunidades laborales” [13] y [21].

En la primavera de 2020, la University of North Texas (UNT) lanzó un Registro de aprendizaje integral (CLR) basado en Badgr, “un registro digital verificable que recopila habilidades en forma de insignias y credenciales” [22], “este registro facilita a que los estudiantes las compartan con el mundo exterior” [23]. Madison College “con casi una década de experiencia en la emisión de credenciales digitales en la educación superior, comparte la combinación de datos cualitativos y cuantitativos que recopila y revisa regularmente para monitorear su programa” [24]. Georgia Tech, es una empresa líder en investigación en el uso de la tecnología de blockchain para sistemas de certificación, y “ha creado diversas credenciales digitales alternativas relacionadas con habilidades que se basan en la tecnología de blockchain y que van desde javascript hasta de cocina vegana” [25].

La Universidad de Basilea “se convierte en la primera de Suiza en expedir títulos basados en la blockchain” [26]. El Instituto Tecnológico de Massachusetts (MIT) en el año 2015; a través del MIT Media Lab “comenzó a expedir certificados digitales usando blockcerts para un número limitado de estudiantes” [27]. Más tarde, en 2017, y “por medio de The Learning Machine, una entidad comercial que utiliza la blockchain y blockcerts, comenzó a emitir diplomas a dos grupos de estudiantes en el MIT Media Lab y la Escuela de Negocios de Sloane” [28], el MIT “se ha convertido en un defensor de que los beneficiarios tengan mayor control sobre



los certificados que obtienen para almacenar, verificar y validar credenciales sin depender de intermediarios —como universidades o empleadores— y así eliminar costos adicionales” [27].

### B. Credenciales Digitales No Formales

Las credenciales no formales, “ofrecen formas de demostrar habilidades en campos que no incluyen una licencia ocupacional requerida o un título universitario tradicional de dos o cuatro años” [7]. Se pueden impartir a través de métodos como pasantías, bootcamp y certificados reconocidos por la industria. [9] destaca que es en el ámbito no-formal donde se presentan las principales iniciativas del entrenamiento y reconocimiento mediante certificaciones digitales alternativas, ante la necesidad de un “cambio de enfoque del Demand-Driven al Employer-Led” [9].

Dicha investigación, destaca iniciativas como la US Chamber of Commerce Foundation [29] que “propone nuevos modelos y herramientas que permitan mejorar la enseñanza y las asociaciones con la Industria”, a través de sus programas: Talent Pipeline Management (TPM) que tiene el enfoque de “cadena de suministro para el desarrollo del talento que es auténticamente dirigido por el empleador, construido sobre las mejores prácticas de la industria, y centrado en el ROI del empleador” [30], Job Data Exchange (JDX) que es “una nueva herramienta de datos abiertos y es el vehículo que los empleadores necesitan para avanzar de manera escalable y sostenible hacia la contratación basada en competencias” [31], esto permitirá generar una mayor riqueza en “los metadatos que serán compartidos entre empleados y los formadores del talento necesario que requieren las empresas y la industria en los Estados Unidos” [31] y el Innovation Network (T3) que “en lugar de buscar datos, los solicitantes de empleo podrán mostrar la amplitud de su experiencia en un registro de aprendizaje único e integral” [29, p. 3], esta red que integra a más de 400 organizaciones, trabajan juntas para crear un ecosistema de datos público-privado abierto y descentralizado [29, p. 3].

Otro gran promotor de las credenciales digitales alternativas, es el Banco Interamericano de Desarrollo (BID), que junto a Badgr, crean “programas en toda la región de Latinoamérica y el Caribe para ayudar a las instituciones a migrar al aprendizaje en línea y emitir credenciales digitales para certificar habilidades relevantes para la fuerza laboral” [32], así el BID busca el desarrollo económico, a través del desarrollo de habilidades y competencias verificadas. Otra iniciativa relevante es Open Skills Network (OSN), este grupo que incluye a más de 530 empleadores, entre ellos a Walmart y Western Governors University, tiene como objetivo “preparar a la fuerza laboral del futuro, para mejorar todo el ecosistema, desde la educación basada en habilidades hasta la contratación y los ascensos” [33], pero esta, no es la única iniciativa de Walmart, que invierte miles de millones de dólares en capacitación, como el programa Live Better U, que “ofrece a los empleados la posibilidad de obtener su diploma de escuela secundaria o título universitario” [34], cuyo sistema de formación laboral les permita “rastrear las habilidades y logros de los trabajadores” [34].

IBM, es otro gigante que se centra en las habilidades y no solo en el logro educativo. “En promedio, el 50 por ciento de los puestos publicados de la empresa en los EE. UU. no requieren una licenciatura” [7], a estos los llaman “trabajos de cuello nuevo y están alineados con carreras que requieren el conjunto adecuado de habilidades y un compromiso con el

aprendizaje permanente”, así IBM ofrece a participantes de todo el mundo, la oportunidad de desarrollar nuevas habilidades técnicas con la emisión de credenciales digitales reconocidas por la industria.

Tradicionalmente, “el desarrollo profesional de los educadores ha implicado asistir a clases y seminarios de varios días, y luego tener poca o ninguna oportunidad de reflexionar sobre lo aprendido o aplicarlo en el aula. A menudo, la nueva información simplemente se pierde” [35], para abordar esta preocupación del aprendizaje y la necesidad de hacerlo más experiencial, Digital Promise se asoció con Concentric Sky “para desarrollar una plataforma de micro credenciales en línea que permite a los educadores en cualquier momento de sus carreras obtener habilidades que mejoran la enseñanza y el aprendizaje” [36].

El Proyecto Wellspring, es una iniciativa que “reúne a instituciones educativas y empleadores para impulsar el uso de credenciales digitales en todos los ámbitos y tiene como propósito automatizar la combinación de credenciales con educación y oportunidades, y empoderar a las personas para que encuentren trabajo” [16], así, este “nuevo ecosistema de educación para el trabajo, basado en registros y credenciales de aprendizaje interoperables, permitirá a las personas encuentren trabajos alineados con su experiencia y habilidades y a los empleadores identificar el mejor talento alineado con roles laborales esenciales”. [16].

Otras industrias, tampoco se quedan atrás, así Kony; que desarrolla tecnología para crear aplicaciones de software, “enfrentaba una demanda que excedía la cantidad de diseñadores y desarrolladores que tenían las habilidades para usar las herramientas. Tal escasez podría potencialmente ralentizar el crecimiento empresarial de Kony” [37]. Entonces, en 2018, la compañía lanzó Base Camp, “una comunidad en línea y abierta para capacitar a los desarrolladores profesionales y ciudadanos para que obtengan las habilidades de TI necesarias para acelerar la entrega de aplicaciones creadas con tecnología Kony” [37]. Turner Classic Movies (TCM) ofrece una serie de MOOC sobre la producción audiovisual, para hacer que “el aprendizaje en línea sea más retentivo” y a través de las insignias poder maximizar la “participación del alumno” [38].

## IV. DISEÑO DE CREDENCIALES DIGITALES

El diseño de credenciales digitales comprende dos componentes muy importantes a considerar: componentes pedagógicos y componentes tecnológicos.

### A. Componentes pedagógicos

El diseño de credenciales antes que nada debe ser integral y no debe diseñarse de manera aislada, el presente modelo [39] es una propuesta, “para que las credenciales se relacionen ente sí y requiere de una jerarquía u otra estructura organizativa, para evaluar el tamaño, la duración o el peso de cada credencial frente a las habilidades, competencias o capacidades pertinentes” [39], sólo de ese modo, será posible concebir el “ecosistema de habilidades”, y su vinculación con el mercado laboral. Tener un “sistema general y un esquema agrega rigor y valor para el ecosistema mediante la articulación de una ruta para cada microcredencial y minimiza el riesgo de crear inadvertidamente caminos sin salida o producto huérfanos” [39].

La siguiente figura 1, propuesta por [39], proporciona una vista esquemática de los componentes pedagógicos a considerar al momento de diseñar credenciales.

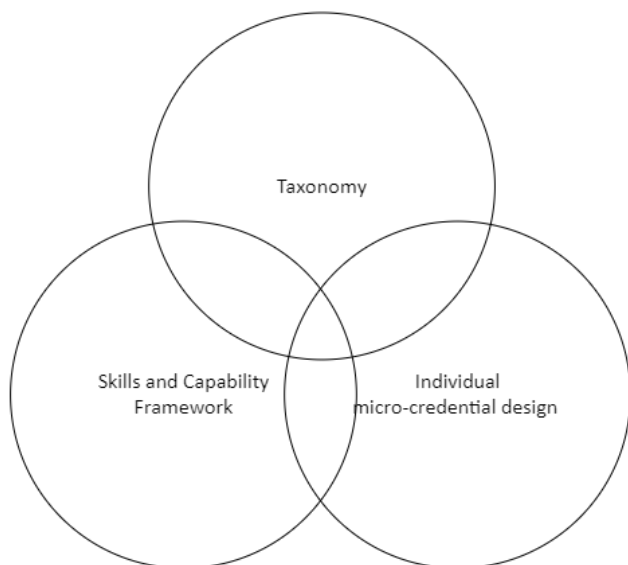


Fig. 1. Esquema de los componentes pedagógicos

1) *Skills and Capability Framework*: Antes que nada, una competencia es “el conjunto combinado de habilidades, deseos y conocimientos necesarios para ser considerado competente en el desempeño o ejecución de una función particular” [40]. Por tanto, un “Marco de Habilidades y Capacidades” brinda una vista amplia o “plan maestro” para todas las habilidades, competencias y capacidades personales que la institución emisora pretende ofrecer y ayuda a las empresas a “identificar niveles de habilidades, brechas y oportunidades” [40]. “El principio del marco es su enfoque en la aplicación de conocimientos, habilidades y competencias relevantes para la industria, en lugar de un currículo más teórico y formal” [39]. Un ejemplo, se muestra en la figura 2; correspondiente al Framework for the Digital Competence of Educators (DigCompEdu) que comprende 22 competencias distribuidas en 6 áreas.

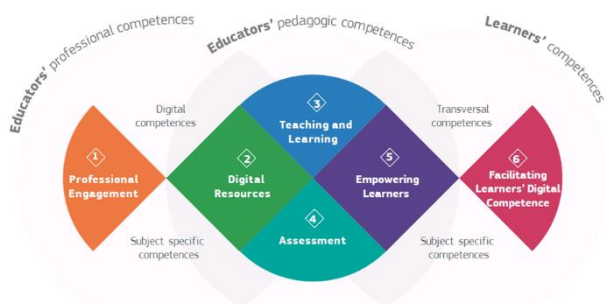


Fig. 2. The European Framework for the Digital Competence of Educators (DigCompEdu)

Los administradores de los Sistemas de Gestión de Aprendizaje (LMS) como Moodle, se pueden crear una estructura de competencia y definir las Competencias asociadas a ella. En los LMSs es posible importar marcos de

competencias, desde Moodle.net [41] se cuenta con un Competency frameworks repository.

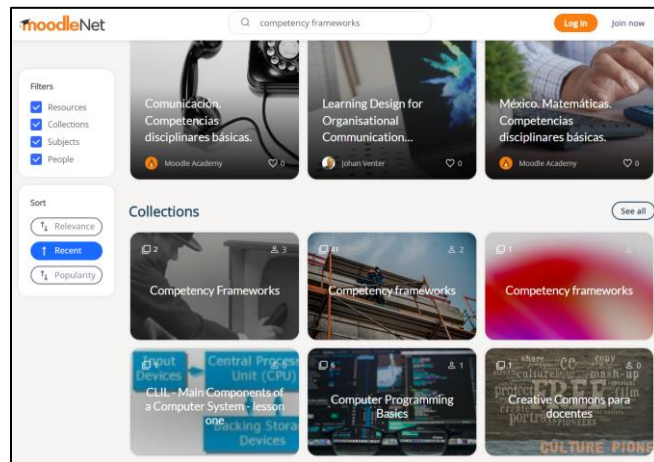


Fig. 3. Repositorio de frameworks de competencias

Entonces, los marcos de competencias pueden ser agregados en los LMS de manera manual partiendo de cero o importando esquemas de competencias (Figura 4).

| Marcos de competencias                 |              |           |          |
|----------------------------------------|--------------|-----------|----------|
| Agregar un nuevo marco de competencias |              |           |          |
| Repositorio de marcos de competencias  |              |           |          |
| Lista de marcos de competencia         |              |           |          |
| Nombre                                 | Competencias | Categoría | Acciones |
| Competencias digitales (CP_05)         | 5            | Sistema   | Editar   |

Fig. 4. Métodos para agregar o subir al repositorio los marcos de competencias

En la siguiente figura 5, se muestra el gestor de competencias, que permite crear, editar o eliminar competencias, que luego pueden ser vinculados a las actividades o evaluaciones de aprendizaje.



Fig. 5. Vista de creación de competencias

2) *Taxonomía*: Una taxonomía de credenciales proporciona la arquitectura general [42], que indica la relación estructural entre las credenciales. Dado que los productos de las credenciales residen principalmente dentro de los dominios de aprendizaje no formal y formal, la taxonomía es deseable para demostrar relaciones y para articular caminos.

La taxonomía, cuyo ejemplo se muestra en la figura 6, también puede proporcionar una “guía clara y estandarizada para el tamaño o el peso de una credencial, capturando atributos a nivel granular para cada uno, como el volumen de aprendizaje, la profundidad, amplitud, complejidad y coherencia del conocimiento, y la habilidades y criterios de evaluación” [39].

Fig. 6. Vista de un ejemplo de taxonomía en Moodle

3) *Diseño del módulo de aprendizaje*: Al diseñar un módulo de credenciales, una decisión clave es si construir o curar (p. ej., usar recursos educativos abiertos). También hay oportunidades para codiseñar con la industria, con proveedores de contenidos (OPM) o socios, basándose en la práctica contemporánea del mundo real. En todos los casos, el proceso comienza definiendo los resultados a lograr, es decir, la adquisición de una habilidad o capacidad, que sólo entonces va seguida de consideraciones relativas al diseño como la evaluación, estrategias, diseño de módulos y contenido.

Es vital el cambio de paradigma del “content-driven” al “backward-design”, esto inicia por redactar una breve descripción del significado de la credencial, donde se precisa lo que el estudiante o trabajador será capaz de hacer y por qué es importante para ellos poseer una habilidad particular o competencia [39].

Los principios de diseño de calidad, en esta fase son vitales porque un curso bien diseñado [43], [44], [45] y [46], garantizará la consecución de la competencias, entre los criterios a considerar podemos destacar: alineamiento constructivo del contenido, actividades y evaluación con las competencias; actividades de aprendizaje que sean relevantes y significativos que promuevan el autoaprendizaje, la colaboración y la interactividad en todos sus formas, actividades que promuevan la participación del alumno; inclusión de información relevante, actual y confiables; inclusivo basado en el enfoque del diseño universal de aprendizaje (DUA); elección apropiada de tecnología educativa que asegure la usabilidad y accesibilidad [39]. Los estudiante también “valoran mucho la posibilidad de personalizar la experiencia creando secuencias de aprendizaje individualizadas basadas en sus conocimientos o habilidades preexistentes, diagnósticos y evaluaciones formativas” [39].

La evaluación debe ser el punto de anclaje pedagógico dentro del ecosistema de habilidades, “para infundir confianza en el valor de una micro credencial” [39], por ello, es esencial la articulación clara de los métodos de evaluación, criterios e instrumentos; las tareas y pruebas no sólo es un requisito para los estudiantes, sino para los revisores y los consumidores de las credenciales para apreciar su verdadero valor, así, “se recomienda en el caso de la evaluación, la adopción de estándares de evaluación de la industria o el envío de evidencias para adjuntar a una credencial” [39], lo cual debiera fomentar el uso de portafolios digitales [47].

A continuación, se presenta la vinculación de las competencias agregadas al LMS y el diseño del módulo de aprendizaje; así en la figura 7, se muestra la vinculación de

una actividad de tipo Tarea con una competencia y en la figura 8, se muestran las competencias asociadas a un curso en el LMS.

Fig. 7. Vinculación de una actividad con una competencia

Fig. 8. Vista de competencias asociadas a un curso en Moodle

## B. Componentes tecnológicos

En la figura 9, se muestran los componentes tecnológicos a considerar, en el diseño de las credenciales digitales.

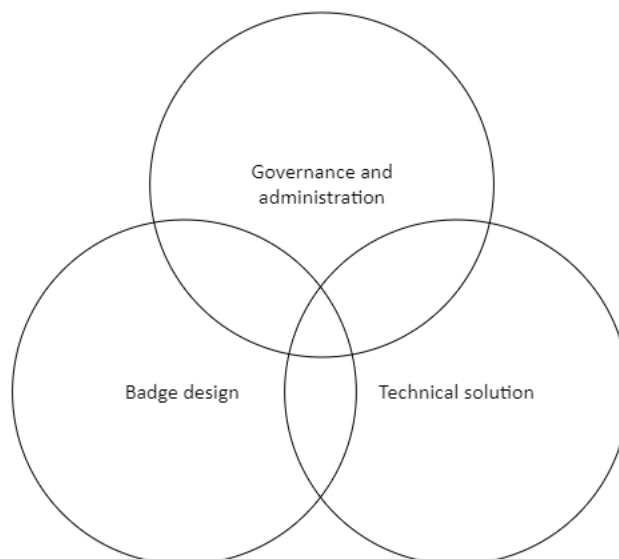


Fig. 9. Esquema de los componentes tecnológicos

1) *Badge design*: Es importante tener en cuenta el público objetivo de la credencial digital y sus preferencias ya sea en forma de certificados o insignias, pero sobre todo los metadatos que serán utilizados por grupos externos a la

organización emisora, por lo que su diseño debe ser el mayor beneficio para este público. Si bien el diseño debe ser distintivo, debe ser identificable con el emisor de la credencial, lo cual debe reflejar la marca de la organización emisora, el color, fuente y uso de la iconografía para representar una habilidad, son factores influyentes, pero deben elegirse con un ojo crítico para determinar si estos elementos contribuyen positivamente al impacto de la credencial.

El diseño de la credencial también debe reflejar la taxonomía, ponderación o nivel de la competencia lograda y de ser el caso, la relación con socios de la industria. Pero “la credencial es más que una imagen” [39], es un “artefacto digital inteligente con metadatos incrustados, y esto es lo que trae a primer plano el potencial real de las credenciales digitales: la capacidad de capturar y compartir metadatos de una manera que sea verificable, confiable y compartible” [39], en la figura 10, se muestra un ejemplo de un certificado emitido.



Fig. 10. Ejemplo del diseño de un certificado emitido.

2) *Governance and administration:* La gobernanza es el mecanismo que mantiene la institución emisora a rendir cuentas con respecto a su estrategia y objetivo. A medida que se conoce y empieza a valorarse estas nuevas prácticas educativas, diversas iniciativas empezarán a surgir; sin embargo, es importante, tener claridad sobre la gobernanza y los procesos administrativos para determinar quién tiene la autoridad para desarrollar y emitir las credenciales [39]. La administración de las credenciales requiere de políticas, normas y procesos, así como el establecimiento y automatización de flujos de trabajo, para determinar la eficacia de los requisitos tales como la garantía de calidad, eficiencia, consistencia y escalabilidad. Estos son necesarios para generar confianza, en los resultados de la iniciativa general y garantizar su sostenibilidad [39], [48] y [49].

3) *Technical solution:* Un requisito esencial es determinar cómo la emisión de la credencial se activará, en qué punto de la ruta de aprendizaje, y de qué tecnología, plataforma o estándar dentro del sistema. La liberación que desencadenará en muchos casos se produce dentro del LMS,

pero a medida que los modelos de acreditación se diversifican, bien pueden surgir otras opciones, como un sistema de cartera electrónica basado en evidencia, una integración al sistema académico (SIS) y a las aplicaciones empresariales. El requisito de emisión afecta la experiencia del usuario, por lo que además de proporcionar una solución técnicamente robusta y automatizada, también debería estar atento a las expectativas del beneficiario.

La configuración o desarrollo de una capacidad de sistema de TI que pueda adaptarse a futuros modelos de emisión y aspiraciones es definitivamente una decisión organizativa clave [39]. Un tema, no menos importante es comprender y decidir el alcance que se pretende alcanzar dentro del ecosistema para adoptar un estándar IMS y en ese aspecto encontramos al Competencies and Academic Standard Exchange (CASE) que “facilita el intercambio de información sobre las competencias de aprendizaje” [50], el Comprehensive Learner Record (CLR) que es “un registro del alumno interoperable moderno y compatible con la web, estructurado para una fácil comprensión, pero lo suficientemente flexible como para admitir una amplia gama de casos de uso para satisfacer las necesidades de los alumnos y trabajadores, registradores y empleadores” [51] y el más conocido Open Badges que incluso ya es parte de la mayoría de los LMS y que “describe un método para empaquetar información sobre logros, incrustarla en archivos de imagen portátiles como insignias digitales e incluye recursos para la validación y verificación basadas en la web” [52], en la figura 11, se muestra la configuración de una insignia mediante el estándar Open Badges.

Fig. 11. Ejemplo de configuración de insignia en Moodle.

## V. ARQUITECTURA DE LA SOLUCIÓN

La solución desarrollada que se muestra en la Figura 1; permite integrar las certificaciones y badges nativos del Moodle que es un sistema de gestión de aprendizaje a un servidor SaS (software como servicio) de almacenamiento y emisión de credenciales digitales basado en Blockchain a través del estándar Open Badge.

La información del blockchain o cadena de bloques, se distribuye a través de “libros de contabilidad”, que registran la información en un conjunto de computadoras; por cada bloque, todos los miembros deben validar cada transacción para que se produzcan, además, todos los involucrados poseen una copia de dicha información, por lo que es imposible alterar los datos anteriores gracias al consenso [53], esta lógica de almacenamiento de manera descentralizada provee de varias ventajas como: mayor confianza, transparencia, descentralizada, inmutable y sin mediadores.

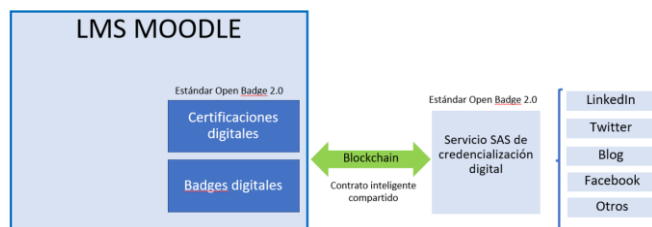


Fig. 12. Arquitectura de la solución basada en Blockchain

Los Open Badges son registros visuales ricos en información de los logros verificables obtenidos por los destinatarios y se comparten fácilmente en la web y a través de las redes sociales. El estándar Open Badges describe un método para empaquetar información sobre logros, incrustarla en archivos de imagen portátiles como insignias digitales e incluye recursos para la validación y verificación basadas en la web. Las insignias abiertas describen quién lo ganó, quién lo emitió, los criterios requeridos y, en muchos casos, incluso la evidencia y demostraciones de las habilidades relevantes [54]. Este estándar elimina la necesidad de que los usuarios descarguen y luego carguen insignias en un sistema, así como la API estándar abierta reduce la necesidad de integraciones entre sistemas.

El servicio SaS de las credenciales proveído por diversos proveedores como Accredible, Credly, Badgr, Sertifier, SimpleCert, CVTrust entre otros más, ofrecen una interfaz web (Figura 2) donde se muestra el certificado o badge digital, con opciones para el usuario para compartir dicho logro por las redes sociales o de manera web a través de un código HTML, además permite la verificación de dicha emisión a través del Blockchain.

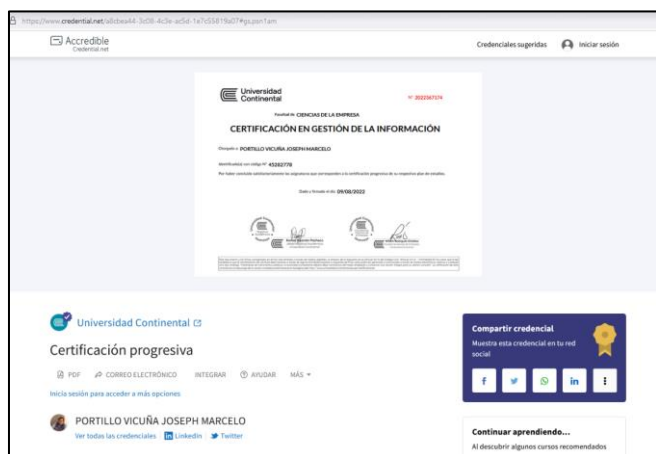


Fig. 13. Interfaz web para la gestión de credenciales digitales

## VI. RESULTADOS

Para evaluar la satisfacción y valoración de las credenciales digitales emitidas por la solución establecida, se han considerado a un grupo de 97 docentes quienes lograron su certificación en competencias digitales, quienes obtuvieron a lo largo del programa de formación credenciales en su forma de certificados e insignias; para tal fin se aplicó un cuestionario de 10 preguntas, cuya prueba de fiabilidad medida a través del Alfa de Cronbach es de 0,926 resultando un valor aceptable como se observa en la Tabla 1, teniendo en cuenta el margen que señalan las autoras y autores habitualmente referenciadas.

TABLA I  
Estadísticas de Fiabilidad

| Alfa de Cronbach | Alfa de Cronbach basada en los elementos tipificados | N de elementos |
|------------------|------------------------------------------------------|----------------|
| ,926             | ,931                                                 | 10             |

En la Tabla 2 puede verse un resumen de los estadísticos del cuestionario en su conjunto, y recoge el coeficiente alfa de Cronbach cuando se suprime cada uno de los ítems. Se observa que al no eliminar ninguna supera la fiabilidad global del instrumento, lo cual es buena dado que no es necesario eliminar ningún ítem.

TABLA II  
Estadísticas de Total de Elementos para el Cuestionario

|                     | Media de la escala si se elimina el elemento | Varianza de la escala si se elimina el elemento | Correlación elemento-total corregida | Alfa de Cronbach si se elimina el elemento |
|---------------------|----------------------------------------------|-------------------------------------------------|--------------------------------------|--------------------------------------------|
| Utilidad            | 41,8351                                      | 101,368                                         | ,754                                 | ,918                                       |
| Facilidad           | 42,1031                                      | 96,302                                          | ,769                                 | ,915                                       |
| Compartir           | 42,3196                                      | 93,907                                          | ,769                                 | ,915                                       |
| Soporte             | 42,3711                                      | 97,527                                          | ,660                                 | ,921                                       |
| Valor               | 42,9072                                      | 94,773                                          | ,609                                 | ,926                                       |
| Satisfacción        | 42,4330                                      | 92,873                                          | ,807                                 | ,913                                       |
| Importancia         | 42,0309                                      | 99,259                                          | ,686                                 | ,920                                       |
| Experiencia         | 42,8969                                      | 89,635                                          | ,766                                 | ,916                                       |
| Repetir Futuro      | 42,0206                                      | 97,458                                          | ,789                                 | ,915                                       |
| Repetir Actualmente | 42,3608                                      | 96,421                                          | ,655                                 | ,921                                       |

El ítem Utilidad se recogió a través de la siguiente pregunta ¿Cómo calificarías la utilidad académica y profesional de compartir tus logros y reconocimientos los certificados e insignias digitales que obtengas?, se observa en la Tabla III que el nivel Totalmente de acuerdo tiene el mayor porcentaje (46,4%), seguida del nivel De acuerdo con 37,1%. Es decir, entre ambos, el 83,5% de los encuestados consideran de utilidad el compartir los certificados e insignias obtenidos.

TABLA III  
Utilidad

| Escala de valoración     | Frecuencia | Porcentaje   | Porcentaje e válido | Porcentaje acumulado |
|--------------------------|------------|--------------|---------------------|----------------------|
| Totalmente en desacuerdo | 1          | 1,0          | 1,0                 | 1,0                  |
| En desacuerdo            | 1          | 1,0          | 1,0                 | 2,1                  |
| Levemente en desacuerdo  | 5          | 5,2          | 5,2                 | 7,2                  |
| Levemente de acuerdo     | 9          | 9,3          | 9,3                 | 16,5                 |
| De acuerdo               | 36         | 37,1         | 37,1                | 53,6                 |
| Totalmente de acuerdo    | 45         | 46,4         | 46,4                | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>        |                      |

El ítem Facilidad se recogió a través de la siguiente pregunta ¿Cómo calificarías la facilidad con la que se pueden



compartir los certificados e insignias por las redes sociales?, se observa en la Tabla IV que el nivel Totalmente de acuerdo tiene el mayor porcentaje (42,3%), seguida del nivel De acuerdo con 32,0%. Es decir, entre ambos, el 74,3% de los encuestados consideran que ha sido fácil el compartir los certificados e insignias obtenidas por las redes sociales.

TABLA IV  
Facilidad

| Escala de valoración     | Frecuencia | Porcentaje   | Porcentaj e válido | Porcentaje acumulado |
|--------------------------|------------|--------------|--------------------|----------------------|
| Totalmente en desacuerdo | 2          | 2,1          | 2,1                | 2,1                  |
| En desacuerdo            | 7          | 7,2          | 7,2                | 9,3                  |
| Levemente en desacuerdo  | 3          | 3,1          | 3,1                | 12,4                 |
| Levemente de acuerdo     | 13         | 13,4         | 13,4               | 25,8                 |
| De acuerdo               | 31         | 32,0         | 32,0               | 57,7                 |
| Totalmente de acuerdo    | 41         | 42,3         | 42,3               | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>       |                      |

El ítem Influencia Social se recogió a través de la siguiente pregunta: El que tus colegas compartan sus logros académicos por las redes sociales ¿En qué grado te motiva a obtener y compartir alguna insignia o certificado?, se observa en la Tabla V que el nivel De acuerdo tiene el mayor porcentaje (37,1%), seguida del nivel Totalmente de acuerdo con 34,0%. Es decir, entre ambos, el 71,1% de los encuestados consideran que motiva a los docentes, que sus colegas obtengan y compartan sus insignias o certificados que obtengan.

TABLA V  
Influencia Social

| Escala de valoración     | Frecuencia | Porcentaj e  | Porcentaj e válido | Porcentaje acumulado |
|--------------------------|------------|--------------|--------------------|----------------------|
| Totalmente en desacuerdo | 6          | 6,2          | 6,2                | 6,2                  |
| En desacuerdo            | 6          | 6,2          | 6,2                | 12,4                 |
| Levemente en desacuerdo  | 3          | 3,1          | 3,1                | 15,5                 |
| Levemente de acuerdo     | 13         | 13,4         | 13,4               | 28,9                 |
| De acuerdo               | 36         | 37,1         | 37,1               | 66,0                 |
| Totalmente de acuerdo    | 33         | 34,0         | 34,0               | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>       |                      |

El ítem Soporte se recogió a través de la siguiente pregunta: ¿Percibes que cuentas con el soporte necesario por parte de la universidad para que compartas correctamente tus insignias y certificados?, se observa en la Tabla VI que el nivel Totalmente de acuerdo tiene el mayor porcentaje (33,0%), seguida del nivel De acuerdo con 30,9%. Es decir, entre ambos, el 63,9% de los encuestados consideran que cuentan con un soporte de parte de la Universidad para que compartan sus credenciales digitales.

TABLA VI  
Soporte

| Escala de valoración     | Frecuencia | Porcentaje   | Porcentaj e válido | Porcentaje acumulado |
|--------------------------|------------|--------------|--------------------|----------------------|
| Totalmente en desacuerdo | 3          | 3,1          | 3,1                | 3,1                  |
| En desacuerdo            | 10         | 10,3         | 10,3               | 13,4                 |
| Levemente en desacuerdo  | 1          | 1,0          | 1,0                | 14,4                 |
| Levemente de acuerdo     | 21         | 21,6         | 21,6               | 36,1                 |
| De acuerdo               | 30         | 30,9         | 30,9               | 67,0                 |
| Totalmente de acuerdo    | 32         | 33,0         | 33,0               | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>       |                      |

El ítem Valor se recogió a través de la siguiente pregunta: Si tuvieras que pagar por tus certificados o insignias que logras ¿El beneficio académico y profesionales que lograrías justificaría dicha inversión económica?, se observa en la Tabla VII que el nivel De acuerdo tiene el mayor porcentaje (28,9%), seguida del nivel Totalmente de acuerdo con 23,7%. Es decir, entre ambos, el 52,7% de los encuestados consideran que estarían dispuestos a pagar, si hubiera un pago por concepto de certificado o credencial digital, estos porcentajes son menores a los resultados obtenidos en los anteriores ítems.

TABLA VII  
Valor

| Escala de valoración     | Frecuencia | Porcentaje   | Porcentaj e válido | Porcentaje acumulado |
|--------------------------|------------|--------------|--------------------|----------------------|
| Totalmente en desacuerdo | 13         | 13,4         | 13,4               | 13,4                 |
| En desacuerdo            | 6          | 6,2          | 6,2                | 19,6                 |
| Levemente en desacuerdo  | 11         | 11,3         | 11,3               | 30,9                 |
| Levemente de acuerdo     | 16         | 16,5         | 16,5               | 47,4                 |
| De acuerdo               | 28         | 28,9         | 28,9               | 76,3                 |
| Totalmente de acuerdo    | 23         | 23,7         | 23,7               | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>       |                      |

El ítem Satisfacción se recogió a través de la siguiente pregunta: ¿Qué nivel de satisfacción te genera el compartir tus certificados e insignias por las redes sociales?, se observa en la Tabla VIII que el nivel De acuerdo tiene el mayor porcentaje (38,1%), seguida del nivel Totalmente de acuerdo con 28,9%. Es decir, entre ambos, el 67,0% de los encuestados se sienten positivamente satisfechos el compartir sus certificados e insignias por las redes sociales.

TABLA VIII  
Satisfacción

| Escala de valoración     | Frecuencia | Porcentaje   | Porcentaje válido | Porcentaje acumulado |
|--------------------------|------------|--------------|-------------------|----------------------|
| Totalmente en desacuerdo | 7          | 7,2          | 7,2               | 7,2                  |
| En desacuerdo            | 5          | 5,2          | 5,2               | 12,4                 |
| Levemente en desacuerdo  | 4          | 4,1          | 4,1               | 16,5                 |
| Levemente de acuerdo     | 16         | 16,5         | 16,5              | 33,0                 |
| De acuerdo               | 37         | 38,1         | 38,1              | 71,1                 |
| Totalmente de acuerdo    | 28         | 28,9         | 28,9              | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>      |                      |

El ítem Experiencia, se recogió a través de la siguiente pregunta: ¿Tuviste alguna experiencia previa de obtener un certificado o insignia digital que lo compartiste por las redes sociales?, se observa en la Tabla IX que el nivel De acuerdo tiene el mayor porcentaje (34,0%), seguida del nivel Totalmente de acuerdo con 22,7%. Es decir, entre ambos, el 56,7% de los encuestados han tenido una positiva experiencia previa de obtener certificados o insignias digitales.

TABLA IX  
Experiencia

| Escala de valoración     | Frecuencia | Porcentaje   | Porcentaje válido | Porcentaje acumulado |
|--------------------------|------------|--------------|-------------------|----------------------|
| Totalmente en desacuerdo | 14         | 14,4         | 14,4              | 14,4                 |
| En desacuerdo            | 8          | 8,2          | 8,2               | 22,7                 |
| Levemente en desacuerdo  | 6          | 6,2          | 6,2               | 28,9                 |
| Levemente de acuerdo     | 14         | 14,4         | 14,4              | 43,3                 |
| De acuerdo               | 33         | 34,0         | 34,0              | 77,3                 |
| Totalmente de acuerdo    | 22         | 22,7         | 22,7              | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>      |                      |

El ítem Repetir en el futuro se recogió a través de la siguiente pregunta: ¿Tienes la intención, en un futuro inmediato de participar en cursos o programas que te permitan obtener insignias o certificados digitales que lo puedas compartir por tus redes sociales?, se observa en la Tabla X que el nivel Totalmente de acuerdo tiene el mayor porcentaje (41,2%), seguida del nivel De acuerdo con 37,1%. Es decir, entre ambos, el 78,3% de los encuestados tienen la intención de participar en cursos o programas que emitan credenciales digitales.

TABLA X  
Repetir en el futuro

| Escala de valoración     | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------------------------|------------|------------|-------------------|----------------------|
| Totalmente en desacuerdo | 2          | 2,1        | 2,1               | 2,1                  |

|                         |           |              |              |       |
|-------------------------|-----------|--------------|--------------|-------|
| En desacuerdo           | 5         | 5,2          | 5,2          | 7,2   |
| Levemente en desacuerdo | 2         | 2,1          | 2,1          | 9,3   |
| Levemente de acuerdo    | 12        | 12,4         | 12,4         | 21,6  |
| De acuerdo              | 36        | 37,1         | 37,1         | 58,8  |
| Totalmente de acuerdo   | 40        | 41,2         | 41,2         | 100,0 |
| <b>Total</b>            | <b>97</b> | <b>100,0</b> | <b>100,0</b> |       |

El ítem Repetir actual se recogió a través de la siguiente pregunta: ¿Actualmente participas en cursos o programas que te permitan obtener insignias o certificados digitales que lo puedas compartir por tus redes sociales?, se observa en la Tabla XI que el nivel Totalmente de acuerdo tiene el mayor porcentaje (35,1%), seguida del nivel De acuerdo con 33,0%. Es decir, entre ambos, el 68,1% vienen desarrollando un curso o programa que emiten credenciales digitales.

TABLA I. REPETIR ACTUAL

| Escala de valoración     | Frecuencia | Porcentaje   | Porcentaje válido | Porcentaje acumulado |
|--------------------------|------------|--------------|-------------------|----------------------|
| Totalmente en desacuerdo | 6          | 6,2          | 6,2               | 6,2                  |
| En desacuerdo            | 6          | 6,2          | 6,2               | 12,4                 |
| Levemente en desacuerdo  | 5          | 5,2          | 5,2               | 17,5                 |
| Levemente de acuerdo     | 14         | 14,4         | 14,4              | 32,0                 |
| De acuerdo               | 32         | 33,0         | 33,0              | 64,9                 |
| Totalmente de acuerdo    | 34         | 35,1         | 35,1              | 100,0                |
| <b>Total</b>             | <b>97</b>  | <b>100,0</b> | <b>100,0</b>      |                      |

## VII. CONCLUSIONES

La decisión de las Instituciones para comprometerse con las credenciales digitales, estarán influenciadas por componentes pedagógicos y tecnológicos presentados en el documento. A nivel organizacional, es importante una cultura al cambio y la disponibilidad de recursos para apoyar a todas las partes interesadas involucradas en la estrategia de implementación dado que se desarrollará o modificará los sistemas administrativos, políticas, reglas de negocio y procesos para permitir nuevos modelos de acreditación, así como las correspondientes actividades de planificación operativa. A nivel pedagógico, es fundamental, asegurarse en tener un sentido claro del propósito y beneficio, por ello debe desarrollarse un plan de participación y comunicación para fomentar una cultura para la innovación. Además, se debe crear una arquitectura general del Marco de habilidades y capacidades incluyendo una taxonomía de credenciales (que articula la granularidad y relación entre las credenciales) así como incorporar los principios y procesos de calidad para diseñar, desarrollar y entregar productos de credenciales que aseguren, cumplan y demuestren las competencias previstas a desarrollar. Otro elemento vital es asegurar que la gobernanza y la administración sean efectivas, evaluando la capacidad de la infraestructura y la tecnología educativa para apoyar la credencialización, y seleccione la plataforma de emisión. Finalmente, se presentaron algunos resultados sobre la



satisfacción y valoración aplicadas a docentes que han recibido credenciales digitales.

## AGRADECIMIENTOS

El autor agradece a la Comisión Europea por su apoyo y financiación parcial y a los socios de la investigación ERASMUS+: Higher Education — International Capacity Building, Yachay (619410-EPP-1-2020-1-PE-EPPKA2-CBHE-JP).

## REFERENCIAS

- [1] «The \$8.5 Trillion Talent Shortage». <https://www.kornferry.com/insights/this-week-in-leadership/talent-crunch-future-of-work> (accedido 28 de agosto de 2022).
- [2] ManpowerGroup, «ManpowerGroup Talent Shortage Study». <https://go.manpowergroup.com/talent-shortage> (accedido 28 de agosto de 2022).
- [3] G. Pelosse, «Council Post: Are Employers Heading For A Talent Shortage Perfect Storm?», *Forbes*. <https://www.forbes.com/sites/forbeshumanresourcescouncil/2022/05/17/are-employers-heading-for-a-talent-shortage-perfect-storm/> (accedido 28 de agosto de 2022).
- [4] «Why is There a Global Talent Shortage and What Can You Do? | Thunderbird». <https://thunderbird.asu.edu/thought-leadership/insights/why-there-global-talent-shortage-and-what-can-you-do> (accedido 28 de agosto de 2022).
- [5] «These are the world's most in-demand jobs», *World Economic Forum*. <https://www.weforum.org/agenda/2022/05/most-in-demand-professions-list-2022/> (accedido 28 de agosto de 2022).
- [6] «SHRM Report: Survey Finds a Rise of Alternative Credentials in Hiring», *SHRM*, 20 de abril de 2022. <https://www.shrm.org/about-shrm/press-room/press-releases/pages/shrm-report-survey-finds-a-rise-of-alternative-credentials-in-hiring.aspx> (accedido 28 de agosto de 2022).
- [7] K. Tyler, «How Alternative Credentials Can Help You Find Employees», *HRMagazine*, p. 1, 2022.
- [8] P. Peralta, «Struggling to hire? Don't overlook alternative credentials», *Empl. Benefit News Online*, 2022, Accedido: 26 de agosto de 2022. [En línea]. Disponible en: <https://www.proquest.com/docview/2653328809/citation/A3EE0D5C63894B42PQ/6>
- [9] M. Cordova, «STANDARDS AND BEST PRACTICES OF ALTERNATIVE DIGITAL CREDENTIALS FOR FORMAL AND NON-FORMAL EDUCATION: CASE DEVELOPED AT THE CONTINENTAL UNIVERSITY», *EDULEARN21 Proc.*, pp. 6291-6300, 2021, doi: 10.21125/edulearn.2021.1273.
- [10] ICDE, «Presente y futuro de las credenciales digitales alternativas (CDA)», enero de 2019. <https://static1.squarespace.com/static/5b99664675f9eea7a3ecce82/t/5cc6a3a40717dc000136783d/1556521901255/ICDE-Informe-CDA-Enero-2019-ES-v02.pdf> (accedido 25 de febrero de 2021).
- [11] L. E. Peláez, A. Toro, y F. A. Vargas, «La Industria 4.0 y las competencias de formación en los programas de ingeniería: una evaluación sobre la demanda de las credenciales alternativas y las microtitulaciones vs la formación de un profesional universitario de ingeniería y su impacto en la calidad desde su desempeño», p. 11.
- [12] SHRM Foundation y Walmart, «Making Alternative Credentials Work: A New Strategy for HR Professionals», p. 19.
- [13] «1 in 3 recent high school grads skipping college because it's a "waste of money"», *Intelligent*. <https://www.intelligent.com/1-in-3-recent-high-school-grads-skipping-college-because-its-a-waste-of-money/> (accedido 28 de agosto de 2022).
- [14] J. Kranc, «"Alternative credentials" taking on more importance in the workplace», *BenefitsPRO*, 2022, Accedido: 26 de agosto de 2022. [En línea]. Disponible en: <https://www.proquest.com/docview/2653384603/abstract/A3EE0D5C63894B42PQ/5>
- [15] J. Cook, «Number of women hired for senior roles increases by almost 70% when using a 'skills-based' hiring process - Business Leader News», *Business Leader*, 10 de marzo de 2022. <https://www.businessleader.co.uk/number-of-women-hired-for-senior-roles-increases-by-almost-70-when-using-a-skills-based-hiring-process/> (accedido 28 de agosto de 2022).
- [16] IMS Global Learning Consortium, «Wellspring Project», 2021. <https://www.imsglobal.org/about/wellspring> (accedido 25 de febrero de 2021).
- [17] S. García-Bullé, «¿Qué son las credenciales alternativas?», *Observatorio de Innovación Educativa*, 26 de abril de 2019. <https://observatorio.tec.mx/edu-news/credenciales-alternativas> (accedido 23 de febrero de 2021).
- [18] Badgr, «University Digital Badging Program Builds Students' Career Readiness», 2021. <https://info.badgr.com/success-stories/usfs-innovative-digital-badging-program-gets-bullish-on-career-readiness.html> (accedido 25 de febrero de 2021).
- [19] «Home | SURF.nl». <https://www.surf.nl/en> (accedido 12 de mayo de 2021).
- [20] Badgr, «Digital Badging Connects Underserved Youth with Opportunity», 2021. <https://info.badgr.com/success-stories/digital-badging-motivates-underserved-students-toward-college-and-jobs-not-necessarily-in-that-order.html> (accedido 25 de febrero de 2021).
- [21] «Welcome to LRNG». <https://www.home.lrng.org/> (accedido 12 de mayo de 2021).
- [22] «Career Ready | USF Career Services». <https://www.usf.edu/career-services/career-ready/> (accedido 12 de mayo de 2021).
- [23] Badgr, «UNT Students Track and Share Marketable Skills with Learner Record», 2020. <https://info.badgr.com/success-stories/first-of-its-kind-learner-record-helps-unt-students-build-track-and-share-marketable-skills.html> (accedido 25 de febrero de 2021).
- [24] «Madison College & Digital Badges: How Their Program Works». <https://resources.credly.com/blog/madison-college-success-story> (accedido 12 de mayo de 2021).
- [25] «Georgia Tech Creates First Online MS in Analytics Degree for Less Than \$10,000 | GTPE». <https://pe.gatech.edu/blog/georgia-tech-creates-first-online-ms-analytics-degree-for-less-10000> (accedido 12 de mayo de 2021).
- [26] «University of Basel Starts Blockchain Based Diploma Courses - Latest Crypto News». <https://kryptomoney.com/university-basel-starts-blockchain-based-diploma-courses/> (accedido 12 de mayo de 2021).
- [27] «La tecnología blockchain transforma la educación - VínculoTIC». <https://vinculotic.com/educacion/tecnologia-blockchain-transforma-educacion/> (accedido 12 de mayo de 2021).
- [28] «Application of Blockchain Technology in Higher Education», *Eur. J. Contemp. Educ.*, vol. 9, n.º 3, sep. 2020, doi: 10.13187/ejced.2020.3.552.
- [29] U.S. Chamber of Commerce Foundation, «The T3 Innovation Network», *U.S. Chamber of Commerce Foundation*, 28 de febrero de 2018. <https://www.uschamberfoundation.org/t3-innovation> (accedido 25 de febrero de 2021).
- [30] TPM Academy, «Details about the TPM Academy Experience», *Talent Pipeline Management (TPM) Academy*, 2020. <https://tpmacademy.uschamberfoundation.org/the-experience/> (accedido 24 de febrero de 2021).
- [31] Job Data Exchange, «Job Data Exchange (JDX)», U.S. Chamber of Commerce Foundation, 3 de agosto de 2018. <https://www.uschamberfoundation.org/workforce-development/JDX> (accedido 24 de febrero de 2021).
- [32] BID, «América Latina y el Caribe: Panorama general», World Bank, 2022. <https://www.bancomundial.org/es/region/lac/overview> (accedido 7 de agosto de 2022).
- [33] «Open Skills Network Receives \$850,000 Grant from Walmart», Western Governors University. <https://www.wgu.edu/newsroom/press-release/2021/07/open-skills-network-receives-850000-grant-walmart.html> (accedido 28 de agosto de 2022).
- [34] «Live Better U Expands». [https://one.walmart.com/content/usone/en\\_us/company/news/popular-content/education-articles/live-better-u-expands.html](https://one.walmart.com/content/usone/en_us/company/news/popular-content/education-articles/live-better-u-expands.html) (accedido 12 de mayo de 2021).
- [35] Badgr, «Digital Promise Micro-credential Program Boosts Teacher Professional Development», 2021. <https://info.badgr.com/success-stories/teacher-professional-development-gets-personal-with-micro-credentials.html> (accedido 25 de febrero de 2021).
- [36] «Micro-credentials - Digital Promise». <https://digitalpromise.org/initiative/educator-micro-credentials/> (accedido 12 de mayo de 2021).
- [37] Badgr, «Temenos Kony Use Base Camp for Open Badges Certification», 2021. <https://info.badgr.com/success-stories/kony-base-camp-badging-platform-guides-app-developers-ascent-to-certification.html> (accedido 25 de febrero de 2021).

- [38] Badgr, «Digital Badges Dramatically Increase MOOC Completion Rates and Learner Engagement», 2020. <https://info.badgr.com/success-stories/turner-classic-movies-success-story.html> (accedido 25 de febrero de 2021).
- [39] D. Rossiter and B. Tynan, "Designing and Implementing Micro-Credentials: A Guide for Practitioners," *Commonwealth of Learning (COL)*, vol. Knowledge Series. Accessed: Aug. 26, 2022. [Online]. Available: <https://oasis.col.org/items/e2d0be25-cbbb-441f-b431-42f74f715532>
- [40] "The Skills Base Competency Framework | Skills Competency," *Skills Base*. <https://www.skills-base.com/competency-framework> (accessed Aug. 29, 2022).
- [41] "search competency frameworks | MoodleNet Central." <https://moodle.net/search?text=competency+frameworks> (accessed Aug. 28, 2022).
- [42] "Estructuras de competencia - MoodleDocs." [https://docs.moodle.org/all/es/Estructuras\\_de\\_competencia](https://docs.moodle.org/all/es/Estructuras_de_competencia) (accessed Aug. 29, 2022).
- [43] A. Sharif and M. Gisbert, "The Impact of Culture on Instructional Design and Quality," *International Journal of Instruction*, vol. 8, no. 1, pp. 143–156, Jan. 2015.
- [44] A. Margaryan, M. Bianco, and A. Littlejohn, "Instructional quality of Massive Open Online Courses (MOOCs)," *Computers & Education*, vol. 80, pp. 77–83, Jan. 2015, doi: 10.1016/j.compedu.2014.08.005.
- [45] R. Small, "Motivation in Instructional Design," *Teacher Librarian*, vol. 27, no. 5, pp. 29–29, Jun. 2000.
- [46] X. Wang, Y. Lee, L. Lin, Y. Mi, and T. Yang, "Analyzing instructional design quality and students' reviews of 18 courses out of the Class Central Top 20 MOOCs through systematic and sentiment analyses," *The Internet and Higher Education*, vol. 50, p. 100810, Jun. 2021, doi: 10.1016/j.iheduc.2021.100810.
- [47] M. M. Merlec, M. M. Islam, Y. K. Lee, and H. P. In, "A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme," *Sensors*, vol. 22, no. 3, Art. no. 3, Jan. 2022, doi: 10.3390/s22031271.
- [48] A. Grech, I. Sood, and L. Ariño, "Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education," *Frontiers in Blockchain*, vol. 4, 2021, Accessed: Aug. 29, 2022. [Online]. Available: <https://www.frontiersin.org/articles/10.3389/fbloc.2021.616779>
- [49] M. C. Lacity and E. Carmel, "Verifiable Credentials in the Token Economy," in *Blockchains and the Token Economy: Theory and Practice*, M. C. Lacity and H. Treiblmaier, Eds. Cham: Springer International Publishing, 2022, pp. 113–138. doi: 10.1007/978-3-030-95108-5\_5.
- [50] IMS Global Learning Consortium, "Competencies and Academic Standards Exchange Real-World Scenarios," *CASE 1.0 Real-World Scenarios*, 2020. <http://www.imsglobal.org/competencies-and-academic-standards-exchange-real-world-scenarios> (accessed Feb. 25, 2021).
- [51] AEFIS, "AEFIS is First Ed Tech Company to Attain IMS Global CLR Certification," Feb. 03, 2021. <https://www.pmnwswire.com/news-releases/aefis-is-first-ed-tech-company-to-attain-ims-global-clr-certification-301221357.html> (accessed Feb. 25, 2021).
- [52] IMS Global Learning Consortium, "Digital Badges," *Open Badges 2.0 (OBv2)*, 2021. <http://www.imsglobal.org/activity/digital-badges> (accessed Feb. 25, 2021).
- [53] FCFM, «¿Qué es Blockchain y cómo se puede aplicar a la educación?», 2019. <https://openlab.uchile.cl/2019/06/03/que-es-blockchain-y-como-se-puede-aplicar-a-la-educacion/> (accedido 15 de abril de 2023).
- [54] IMS Global Learning Consortium. (2020b). Competencies and Academic Standards Exchange Real-World Scenarios. CASE 1.0 Real-World Scenarios. <http://www.imsglobal.org/competencies-and-academic-standards-exchange-real-world-scenarios>

# Confesiones, *sexting*, insultos y amenazas: ciberviolencia en la educación

González, Nadia Constanza

## Resumen

En el intrincado mundo digital de hoy, la ciberviolencia en las escuelas se ha convertido en un desafío desalentador que no podemos ignorar. Desde el *ciberbullying* hasta la suplantación de identidad y el *sexting* no consensuado, los jóvenes enfrentan una serie de amenazas que afectan profundamente su bienestar emocional y su rendimiento académico. Este artículo propone sumergirnos en la complejidad de esta problemática, explorando cómo la tecnología ha amplificado las formas de violencia entre estudiantes. A medida que se exponen las diversas manifestaciones de la ciberviolencia, también se proponen estrategias efectivas para prevenir y abordar este problema. Desde la implementación de políticas escolares claras hasta la educación sobre el uso responsable de la tecnología, hay un abanico de acciones que podemos tomar para proteger a nuestros jóvenes en línea. Además, nos adentramos en el rol crucial de los educadores y las familias en la lucha contra la ciberviolencia, destacando cómo una colaboración sólida puede fomentar una cultura del respeto y la tolerancia en todos los ámbitos de la vida escolar.

## Palabras clave

Ciberviolencia, Educación, Ciberbullying, Confesiones, Ciberamenazas

## I. INTRODUCCIÓN

*"Existen diferentes mecanismos que utilizan los hostigadores para humillar a sus víctimas en forma online como diseminar rumores, insultar, atacar sus publicaciones, inclusive incitar a otros hostigadores para coordinar ataques virtuales a la misma persona"*<sup>[1]</sup>

El *ciberbullying* puede llevar a niños y adolescentes a situaciones emocionales devastadoras es un tema que debe plantearse y prevenirse desde las escuelas. En el contexto escolar, presenta desafíos únicos debido a la constante presencia de la tecnología en la vida de los estudiantes. Las redes sociales, los mensajes en

línea y otras herramientas en línea proporcionan a los acosadores un medio para hostigar a sus víctimas tanto dentro como fuera del entorno escolar. Esta omnipresencia digital significa que las agresiones pueden continuar incluso después de que los estudiantes están en sus casas, creando un ambiente de hostilidad y ansiedad que puede afectar negativamente su bienestar emocional y su rendimiento académico.

*"El acoso escolar y el ciberacoso (...) actualmente son considerados problemas de salud pública y una seria amenaza para el desarrollo, el bienestar y la salud mental de los niños y adolescentes escolarizados."* <sup>[2]</sup>

Es de público conocimiento que este fenómeno aumenta los niveles de estrés, ansiedad y depresión entre los estudiantes. Además, el clima escolar suele deteriorarse, ya que el miedo a convertirse en víctima puede afectar la capacidad de los estudiantes para concentrarse en sus estudios y participar plenamente en la vida escolar.

Pero, el *ciberbullying* no es el único tipo de violencia que vincula la convivencia escolar y la utilización de nuevas tecnologías. A medida que los niños y adolescentes generan otro tipo de vínculos y la tecnología permite la viralización de otro tipo de contenidos, se hacen cada vez más complejas sus interacciones y conflictos también en internet. Algunos tipos de ciberviolencia, además del *ciberbullying*, refieren al *sexting* no consensuado, suplantación de identidad y difusión de contenido violento o perturbador.

Los educadores y los padres también se ven afectados por este fenómeno, ya que enfrentan el desafío de proteger a los estudiantes y promover un entorno escolar seguro y acogedor. La falta de comprensión sobre cómo abordarlo puede llevar a una respuesta inadecuada por parte de las

autoridades escolares, lo que a su vez puede perpetuar el problema y dejar a las víctimas sin el apoyo necesario para superar la situación.

## II. LA CIBERVIOLENCIA EN EL ÁMBITO EDUCATIVO

La ciberviolencia en el aula abarca una amplia gama de comportamientos agresivos y perjudiciales que se llevan a cabo a través de dispositivos electrónicos y plataformas en línea. Estos comportamientos pueden tener un impacto significativo en el bienestar emocional y el rendimiento académico de los estudiantes, así como en el clima general de la escuela.

La forma más conocida de ciberviolencia en el aula es el *ciberbullying*. Se refiere al uso de tecnologías de comunicación digital, como mensajes de texto, redes sociales y correos electrónicos, para acosar, intimidar, humillar o difamar a otros estudiantes. Esto puede incluir insultos, amenazas, comentarios ofensivos o exclusiones deliberadas en redes sociales, foros de discusión o grupos de mensajería. El acoso en línea puede ser constante y difícil de escapar, lo que puede tener un impacto significativo en la salud mental y emocional de la víctima.

Otro tipo de ciberviolencia es el *sexting* no consensuado. Se refiere al intercambio de mensajes, imágenes o videos generalmente de índole sexual que pertenecen a una persona que dio su consentimiento sólo en la índole privada. Esto puede ocurrir cuando un estudiante comparte material íntimo con otro par con la expectativa de privacidad. Sin embargo, el otro no mantiene la promesa de privacidad y lo difunde.

También se ha difundido la práctica de la suplantación de identidad, es decir, la utilización de la identidad de otra persona para enviar mensajes o publicar contenido en línea. Esto puede causar confusión, conflictos y daño a la reputación de la víctima, así como ser utilizado para difundir información falsa o dañina.

Algunos estudiantes participan en la difusión de contenido violento, perturbador o inapropiado en línea, como imágenes de violencia física, videos de peleas o mensajes de odio. Esto puede crear un ambiente de miedo e intimidación en la escuela, y

puede ser especialmente perjudicial para los estudiantes más jóvenes o vulnerables.

La ciberviolencia en el aula tiene el potencial de causar daño significativo a los estudiantes y afectar negativamente el clima escolar. Es fundamental que las escuelas aborden este problema de manera proactiva y efectiva, proporcionando educación sobre el uso seguro y responsable de la tecnología, así como recursos y apoyo para las víctimas de ciberviolencia.

A continuación se abordan más en profundidad cada uno de los temas planteados.

### a. El ciberbullying

Mantener un clima de convivencia positivo y respetuoso es esencial para el bienestar emocional y el desarrollo integral de los estudiantes. La convivencia escolar se refiere al conjunto de relaciones interpersonales, valores, normas y actitudes que prevalecen en una institución educativa. Cuando los estudiantes se sienten seguros, valorados y apoyados en su entorno escolar, están más dispuestos a participar activamente en las actividades académicas, sociales y extracurriculares, lo que contribuye a un mejor rendimiento académico y a una mayor satisfacción con la experiencia educativa.

El *bullying* representa una grave amenaza para la convivencia escolar. Se define como un comportamiento agresivo y repetitivo que implica un desequilibrio de poder, donde una o más personas ejercen su poder sobre otra persona de manera intencional y con el objetivo de causar daño físico, psicológico o emocional. Algunos autores señalan que si bien siempre existe una agresión psicológica, existen distintos tipos de *bullying*: 1) la agresión forma física y/o contra la propiedad; 2) la forma verbal (insultos, motes, burlas, hablar mal de otros, calumnias, menosprecio en público, etc.); 3) la forma social, que aísla al individuo del grupo; y 4) la forma psicológica, en la que se busca provocar miedos e inseguridades a partir de ridiculizaciones<sup>[3]</sup>. Es importante señalar que esta terminología sólo abarca a los casos entre niños o adolescentes y entre pares.

Las primeras investigaciones sobre el *bullying* surgieron en la década de 1970, cuando los

académicos comenzaron a reconocer la gravedad del problema y su impacto en la salud mental y el bienestar de los niños y adolescentes. Estas investigaciones han demostrado que no solo afecta a las víctimas directas, sino que también tiene un impacto negativo en los agresores y en el clima general de la escuela. Los niños y adolescentes que son víctimas de *bullying* tienen un mayor riesgo de experimentar problemas emocionales, como la depresión y la ansiedad, así como dificultades académicas y sociales. Además, los agresores tienen más probabilidades de tener problemas de conducta y enfrentar consecuencias negativas a largo plazo en su desarrollo personal y social.

*“El ciberbullying se define desde el mismo marco del bullying tradicional y se entiende como la intimidación o agresión intencional y continuada, a través de medios electrónicos, como teléfonos móviles o Internet, resultando un desbalance de poder entre el agresor y la víctima”<sup>[4]</sup>.*

El *ciberbullying* se puede definir como el uso deliberado y repetido de tecnologías de comunicación digital, con el fin de acosar, intimidar, humillar o difamar a otros. A diferencia del *bullying* tradicional, el *ciberbullying* puede ocurrir de manera anónima y alcanzar a una audiencia más amplia en un corto período de tiempo. Se caracteriza por *“una invasión permanente hacia la víctima, gran amplitud de la audiencia, rapidez y comodidad en su ejecución, invisibilidad o anonimato que facilita que el acosador se sienta menos culpable e incluso ignore las consecuencias de sus actos, se puede dar en cualquier lugar y en cualquier momento, es imperecedero, la fuerza física o el tamaño no importan al momento de dañar a otro”* <sup>[5]</sup>.

Las escuelas desempeñan un papel importante en la enseñanza de habilidades digitales y en la promoción de un comportamiento en línea responsable y ético ya que generalmente el *ciberbullying* también tiene como protagonistas a compañeros de escuela o de clubes.

## **b. El sexting**

El intercambio de mensajes, imágenes o videos de naturaleza sexual a través de dispositivos

electrónicos, como teléfonos móviles o plataformas de mensajería instantánea se ha convertido en algo popular entre los adolescentes. Esto lleva el nombre de *sexting*.

Aunque el *sexting* puede ser consensual y realizado entre adultos que comparten su contenido de manera mutua y consciente, también puede ocurrir de manera no consensuada, especialmente entre adolescentes, lo que puede llevar a graves consecuencias.

En la adolescencia se produce el desarrollo de la sexualidad y las prácticas como el *sexting* pueden suponer una prueba de confianza en la pareja, no sentirse excluido de los grupos que incurren en estas prácticas o, incluso, pueden ser el resultado de acentuar las características de esta etapa como el exceso de confianza del adolescente y la impulsividad que les impide reflexionar sobre sus consecuencias. Asimismo, algunos autores revelan que la adolescencia sumada a las nuevas tecnologías no es una buena combinación.

*“Actualmente, en nuestra sociedad existe una creciente tendencia a mostrar la intimidad. Esto les lleva a considerar normales conductas como compartir información que los adultos consideran personal y privada”<sup>[6]</sup>.*

Cuando el contenido sexualmente explícito se comparte sin el consentimiento de la persona representada, se convierte en *sexting* no consensuado. Esto puede causar vergüenza, ansiedad y estrés emocional para la víctima, así como dañar su reputación y relaciones personales. Entre los adolescentes, el *sexting* no consensuado puede dar lugar a actos de *ciberbullying*, donde el contenido comprometedor se comparte ampliamente en línea con el objetivo de avergonzar, intimidar o acosar a la víctima.

Cuando un individuo amenaza con compartir imágenes o videos sexualmente explícitos de una persona a menos que esta acceda a sus demandas, que pueden incluir dinero, más contenido sexual o incluso encuentros físicos, ocurre la sextorsión o extorsión sexual.

El *sexting* entre niños o adolescentes también puede ser utilizado por adultos malintencionados

como parte de un proceso de *grooming*, donde manipulan y seducen a jóvenes vulnerables para obtener imágenes, videos sexuales o incluso encuentros reales. Estos depredadores suelen utilizar el contenido comprometedor para chantajear o explotar a sus víctimas <sup>[7]</sup>.

El *sexting* entre adolescentes puede tener consecuencias graves y duraderas, especialmente cuando el contenido se comparte sin consentimiento o es utilizado para fines de acoso, chantaje o explotación. Es fundamental que los jóvenes sean educados sobre los riesgos asociados con estas prácticas y se les brinde apoyo y recursos para proteger su bienestar emocional y su seguridad en línea.

### **c. Identidad digital**

El conjunto de información, características y representaciones que una persona establece en línea a través de su participación en redes sociales, plataformas digitales y otros medios de comunicación en línea, es la identidad digital.

Para los adolescentes, la formación de su identidad digital es un proceso complejo que se desarrolla a medida que exploran y participan en diferentes comunidades en línea, compartiendo contenido, interactuando con otros usuarios y construyendo una presencia en línea, están dando forma a cómo son percibidos por los demás y cómo se ven a sí mismos en el mundo digital. Las redes sociales desempeñan un papel significativo en la formación de la identidad digital de los adolescentes, ya que les proporcionan una plataforma para expresarse, conectarse con otros y presentar una versión de sí mismos al mundo. Sin embargo, también pueden fomentar la comparación social y la búsqueda de validación, ya que los adolescentes tienden a comparar su vida y apariencia con la de sus pares en línea. Esto puede llevar a sentimientos de insuficiencia, baja autoestima y ansiedad por la imagen que proyectan en línea.

Algunas veces, existe una dicotomía entre la identidad digital que los adolescentes desean mostrar en línea y su realidad fuera de las redes sociales. Muchos adolescentes se sienten presionados para mantener una imagen idealizada de sí mismos en línea, mostrando solo los aspectos positivos de sus vidas y ocultando las dificultades y

los desafíos que enfrentan en la vida real. Esto puede llevar a una falta de autenticidad y conexión genuina en línea, así como a sentimientos de alienación y soledad <sup>[8]</sup>.

Si la identidad digital ya supone cierta presión en los adolescentes, la suplantación de identidad entre adolescentes lo es aún más. Este fenómeno consiste en el uso no autorizado de la identidad de otra persona para enviar mensajes, publicar contenido o realizar acciones en línea en su nombre. Esta práctica puede tener graves repercusiones para la víctima, así como para la seguridad y el bienestar de toda la comunidad en línea.

Las consecuencias de la suplantación de identidad entre adolescentes pueden ser graves e incluir: daño a la reputación de la víctima, generar conflictos interpersonales entre la víctima y sus amigos, familiares o compañeros de clase, sensación de vulnerabilidad y falta de control sobre su propia imagen, riesgos de seguridad para la víctima, ya que los perpetradores pueden tener acceso a información personal y privada.

### **d. Difusión de contenido violento**

Estudios han demostrado que la visualización repetida de imágenes de violencia puede desensibilizar a las personas y aumentar la probabilidad de comportamientos agresivos o antisociales <sup>[9]</sup>.

La difusión de contenido violento, perturbador o inapropiado en línea es una forma de ciberviolencia que plantea serios riesgos para la seguridad y el bienestar de los usuarios de Internet, especialmente para los niños y adolescentes. Este tipo de contenido puede incluir imágenes de violencia física, videos de peleas, mensajes de odio y otros materiales que son dañinos, alarmantes o perturbadores.

La propagación de discursos de odio y la incitación a la violencia contra grupos específicos pueden tener consecuencias devastadoras, como el aumento de la discriminación, el acoso y la violencia contra personas marginadas o vulnerables.

Es fundamental que los usuarios de Internet, especialmente los jóvenes, sean educados sobre los riesgos asociados con la exposición a contenido



violento y perturbador en línea. Las familias, las escuelas y las comunidades pueden desempeñar un papel importante en la prevención y la respuesta a la ciberviolencia, proporcionando educación sobre el uso seguro y responsable de Internet, promoviendo la empatía y el respeto hacia los demás, y fomentando la denuncia y la eliminación de contenido violento en línea.

#### e. “Confesiones” de escuelas y clubes

En los últimos años, ha surgido una preocupante tendencia en las redes sociales donde se crean perfiles bajo el nombre de escuelas, clubes u otros grupos, con el propósito de escrachar a individuos, publicar fotos comprometedoras, conversaciones privadas o “confesar” secretos anónimos. Esta práctica, que a menudo se lleva a cabo de manera anónima, puede tener graves repercusiones para la reputación, el bienestar emocional y la seguridad de los individuos afectados <sup>[10]</sup>.

Estos perfiles a menudo publican contenido difamatorio, humillante o vergonzoso sobre estudiantes, profesores u otros miembros de la comunidad escolar, con el objetivo de ridiculizar, avergonzar o acosar a la persona afectada. Algunos perfiles en redes sociales, sobre todo los que permiten a los usuarios enviar “confesiones” anónimas, comparten secretos, rumores o información personal. Si bien esto puede parecer inofensivo, puede ser utilizado como una herramienta para difundir chismes, rumores infundados o información perjudicial sobre otros, lo que puede causar daño emocional y reputacional <sup>[11]</sup>.

La publicación de contenido anónimo puede aumentar el riesgo de acoso, victimización y abuso en línea, especialmente cuando el contenido se comparte de manera viral y llega a una audiencia amplia y desconocida.

Esta tendencia tiene graves repercusiones para la privacidad, la reputación y el bienestar emocional de los individuos afectados. Es fundamental que se tomen medidas para prevenir y abordar este tipo de comportamiento, promoviendo el respeto, la empatía y la responsabilidad en línea.

### III. IMPACTO EN LA VIDA DEL ESTUDIANTE

La ciberviolencia, que incluye el acoso, la difusión de contenido perturbador y la suplantación de identidad en línea, tiene un impacto significativo en el bienestar emocional y el rendimiento académico de los individuos afectados, especialmente de los niños y adolescentes. El *bullying*, que generalmente se circunscribe al ámbito escolar, encuentra en casa de los niños un lugar seguro. El *ciberbullying*, por otra parte, hace que los niños vivan en constante estrés y ansiedad, en todas partes y en todo momento.

*“Cada vez hay más casos que revelan que aproximadamente 1 de cada 2 jóvenes que sufren acoso nunca se lo cuenta a nadie, bien sea por miedo, vergüenza o falta de confianza en los sistemas de apoyo. Los abusos, tanto en Internet como en otros contextos, causan estragos en la salud mental y física de los jóvenes y provocan ataques de estrés que puede causar daño emocional y reputacional”* <sup>[12]</sup>.

La exposición a la ciberviolencia puede tener una serie de efectos negativos en el bienestar emocional de los niños y adolescentes incluyendo: ansiedad, estrés, depresión, baja autoestima, trastornos de estrés postraumático (como pesadillas y evitación de actividades relacionadas con la experiencia traumática) <sup>[13]</sup>. Algunas de estas consecuencias incluyen:

1. Ansiedad y estrés: las víctimas de ciberviolencia pueden experimentar niveles elevados de ansiedad y estrés debido a la constante preocupación por la seguridad personal y la intimidación en línea.
2. Depresión: el acoso cibernético puede provocar sentimientos de tristeza, desesperanza y aislamiento, lo que puede contribuir al desarrollo de la depresión.
3. Baja autoestima: la disminución de la autoestima y la autoconfianza puede ocasionarse debido a los mensajes negativos y humillantes que reciben en línea.
4. Trastornos del sueño: el estrés causado por la ciberviolencia puede interferir en el sueño normal,

provocando insomnio o dificultades para conciliar el sueño.

5. Pensamientos suicidas: en casos extremos, la ciberviolencia puede llevar a pensamientos suicidas o intentos de suicidio, especialmente entre adolescentes y jóvenes que son más vulnerables emocionalmente.

Los problemas emocionales y psicológicos causados por la ciberviolencia pueden manifestarse de varias maneras en el entorno escolar, y los educadores deben estar atentos para identificar y abordar estas señales. Algunas formas en que estos problemas pueden reflejarse en el aula incluyen:

1. Bajo rendimiento académico: las víctimas de ciberviolencia pueden tener dificultades para concentrarse en el aprendizaje debido a la ansiedad, el estrés y otros problemas emocionales relacionados con el acoso en línea. Esto puede resultar en un bajo rendimiento académico y dificultades para completar tareas escolares.

2. Comportamiento retraído o agresivo: los estudiantes afectados por la ciberviolencia pueden mostrar cambios en su comportamiento en el aula, como volverse más retraídos, callados o incluso agresivos. Pueden evitar interactuar con sus compañeros o mostrar signos de irritabilidad y hostilidad.

3. Aislamiento social: las víctimas de ciberviolencia pueden experimentar un mayor aislamiento social en el entorno escolar, evitando actividades extracurriculares, recreos o eventos escolares donde puedan encontrarse con sus agresores.

4. Ausentismo escolar: los problemas emocionales y psicológicos relacionados con la ciberviolencia pueden llevar a un aumento en el ausentismo escolar, ya sea por miedo a enfrentar a los agresores en el entorno escolar o por la necesidad de evitar situaciones que desencadenan ansiedad o estrés.

5. Impacto en el clima escolar: la presencia de ciberviolencia puede tener un impacto negativo en el clima escolar en general, creando un ambiente de desconfianza, intimidación y falta de seguridad para todos los estudiantes.

Es crucial que los educadores estén capacitados para reconocer estos signos y brindar apoyo adecuado a las víctimas de ciberviolencia, así como implementar estrategias para prevenir y abordar este problema en el entorno escolar.

Es fundamental que se tomen medidas para prevenir y abordar la ciberviolencia, protegiendo así el bienestar y el desarrollo de los jóvenes en línea. Según informes recientes de la Organización de las Naciones Unidas una de cada tres víctimas de acoso se ha autolesionado por este motivo, y 1 de cada 10 ha intentado suicidarse <sup>[14]</sup>.

#### IV. PREVENCIÓN Y SENSIBILIZACIÓN

La gestión de la convivencia escolar es una tarea compleja y multifacética que implica promover relaciones positivas, respetuosas y colaborativas entre todos los miembros de la comunidad educativa, incluyendo estudiantes, educadores, padres y personal administrativo. Aunque puede no ser una tarea sencilla, es fundamental para crear un ambiente escolar seguro, inclusivo y propicio para el aprendizaje y el desarrollo integral de los estudiantes.

Se trata de desarrollar políticas, programas y prácticas que fomenten un clima escolar positivo y respetuoso, donde todos los miembros de la comunidad se sientan valorados, seguros y apoyados. Esto incluye la prevención y el abordaje de comportamientos disruptivos, conflictos interpersonales y formas de violencia, como el *bullying* y el *ciberbullying*, así como la promoción de la resiliencia, la empatía y la responsabilidad social entre los estudiantes.

*“Respetar, compartir, comprender y ponerme a disposición del otro, son aprendizajes prioritarios que se convierten en una urgencia para utilizar con seguridad las TIC y ejercer una ciudadanía digital responsable”* <sup>[15]</sup>.

Trabajar en la prevención de las ciberviolencias mediante la alfabetización digital y emocional es una tarea urgente dado que es el modo más efectivo de hacer prevención primaria. Pero la convivencia escolar y la alfabetización digital no son prioridades en las políticas públicas en

Latinoamérica. Aún existen desafíos significativos en la implementación y la efectividad de estas iniciativas, incluyendo la falta de recursos, la resistencia al cambio y la necesidad de una mayor coordinación y colaboración entre las diferentes partes interesadas. Es importante continuar trabajando en el fortalecimiento de la gestión de la convivencia escolar en Latinoamérica y, especialmente, en Argentina reconociendo su importancia para el bienestar y el éxito de los estudiantes.

### **Rol de los educadores y la familia en la lucha contra la ciberviolencia**

Como la violencia y, especialmente la ciberviolencia se trata de fenómenos multicausales y con consecuencias de distinto tipo, no sólo la escuela es la que tiene que actuar, aunque es innegable que tiene un rol fundamental. Los educadores son quienes tienen la responsabilidad de proporcionar orientación, apoyo y recursos a los estudiantes para promover un entorno en línea seguro y respetuoso. Esto incluye enseñar habilidades digitales, como la navegación segura en línea, la gestión de la privacidad y la identificación de comportamientos problemáticos, así como fomentar la empatía, el respeto y la responsabilidad en el uso de la tecnología.

Tanto educadores como la familia, deben trabajar para promover una cultura del respeto y la tolerancia. Esto incluye establecer normas y expectativas claras de comportamiento en línea, así como abordar activamente los casos de ciberviolencia cuando surjan. También deben estar atentos a las señales de ciberviolencia entre los adolescentes y tomar medidas rápidas y efectivas para abordar el problema. Esto puede incluir proporcionar apoyo emocional a las víctimas, mediar en conflictos y trabajar con los agresores para promover la responsabilidad y el cambio de comportamiento.

### **Estrategias de prevención y respuesta por parte de las instituciones educativas**

*“La prevención primaria es la que evita que aparezca la problemática, la secundaria aquella donde se actúa para detectar y controlar los factores de riesgo, y la terciaria, aquella que actúa para*

*corregir o enmendar situaciones ya existentes”* <sup>[16]</sup>.

Las instituciones educativas deben establecer políticas claras y protocolos de actuación para abordar la ciberviolencia. Estas políticas deben definir qué se considera ciberviolencia, cómo se deben reportar los casos, qué acciones se tomarán para abordarlos y qué medidas disciplinarias se aplicarán a los perpetradores. Algunos autores destacan que la mayoría de los protocolos sobre *bullying* y *ciberbullying* son deficientes ya que no tienen como centro la prevención primaria sino la terciaria.

Las instituciones educativas deben trabajar activamente para crear un entorno escolar seguro y acogedor donde los estudiantes se sientan seguros para denunciar incidentes de ciberviolencia. Esto implica fomentar una cultura de confianza y apoyo entre los estudiantes y el personal educativo, así como establecer canales de comunicación abiertos y accesibles para reportar casos de ciberviolencia de manera confidencial. También es importante proporcionar capacitación regular al personal educativo sobre cómo identificar, prevenir y abordar la ciberviolencia de manera efectiva. Esto incluye enseñarles a reconocer los signos de ciberviolencia, cómo intervenir adecuadamente en casos de *ciberbullying* y cómo ofrecer apoyo emocional a las víctimas.

Hoy la alfabetización digital se ha vuelto clave en la escuela de la misma forma que la educación emocional. Estos son los dos aspectos a trabajar. Las escuelas deben promover una cultura de respeto, empatía y tolerancia en la que se valoren las diferencias y se rechaza la violencia en todas sus formas.

## **V. CONCLUSIONES**

Desde el *ciberbullying* hasta la difusión de contenido violento, hemos comprendido la urgente necesidad de abordar estos desafíos para proteger el bienestar emocional y el desarrollo de nuestros jóvenes.

A partir de estas observaciones, se pueden extraer varias conclusiones importantes:

- La ciberviolencia tiene un impacto significativo en el bienestar emocional de

los estudiantes, con efectos que incluyen ansiedad, estrés, depresión y baja autoestima. Este impacto puede afectar negativamente el rendimiento académico y la calidad de vida de los jóvenes.

- Es fundamental implementar estrategias de prevención y sensibilización para abordar la ciberviolencia en el entorno escolar. Esto incluye educar a los estudiantes sobre el uso seguro y responsable de la tecnología, así como promover la empatía, el respeto y la responsabilidad en línea.
- Las escuelas desempeñan un papel crucial en la prevención y respuesta ante la ciberviolencia. Es importante que establezcan políticas claras y protocolos de actuación, así como proporcionen capacitación regular al personal educativo sobre cómo identificar, prevenir y abordar la ciberviolencia de manera efectiva.
- Tanto los educadores como las familias deben trabajar juntos para promover una cultura del respeto y la tolerancia, tanto en línea como fuera de línea. Esto incluye establecer normas claras de comportamiento en línea y abordar activamente los casos de ciberviolencia cuando surjan.

Sin embargo, aunque hemos identificado estrategias efectivas y destacado el papel fundamental de educadores y familias, este viaje está lejos de terminar. Quedan muchas preguntas por responder y áreas por explorar más a fondo. ¿Cómo podemos fortalecer la implementación de políticas escolares contra la ciberviolencia? ¿Qué más podemos hacer para educar a los jóvenes sobre el uso responsable de la tecnología? ¿Cómo podemos fomentar una cultura del respeto y la empatía en todas las interacciones en línea? Estas son solo algunas de las preguntas que pueden servir como punto de partida para futuros estudios e investigaciones.

En última instancia, este viaje nos ha recordado que la lucha contra la ciberviolencia en las escuelas es un esfuerzo continuo y colaborativo que requiere el compromiso de toda la comunidad educativa. Sigamos adelante con determinación y esperanza, sabiendo que juntos podemos crear un entorno en línea seguro y acogedor para nuestros jóvenes.

## VI. REFERENCIAS

- [1] Ginestar, A. (2021, noviembre 5). La peligrosa moda en Instagram en la que escrachan adolescentes. *Mendoza Online*.
- [2] Herrera Lopez, M., y otros. (2018). Bullying y Cyberbullying en Latinoamérica. Un estudio bibliométrico. *Revista Mexicana de Investigación Educativa*.
- [3] Cf. Cardozo, G., Dubini, P., & Lorenzino, L. (2017). Bullying y cyberbullying: un estudio comparativo con adolescentes escolarizados. *Revista Mexicana de Psicología*.
- [4] Herrera Lopez, M., y otros. (2018). Bullying y Cyberbullying en Latinoamérica. Un estudio bibliométrico. *Revista Mexicana de Investigación Educativa*.
- [5] Cardozo, G., Dubini, P., & Lorenzino, L. (2017). Bullying y cyberbullying: un estudio comparativo con adolescentes escolarizados. *Revista Mexicana de Psicología*.
- [6] Incibe. Sexting.
- [7] Ibidem.
- [8] Cf. Zimbrón, A. (2020). Comparación social: un factor que afecta a las personas en Facebook. *Notipress*.
- [9] Cf. Menor Sendra, J. (2018). Influencia en la violencia de los medios de comunicación: guía de buenas prácticas.
- [10] Cf. Ginestar, A. (2021, noviembre 5). La peligrosa moda en Instagram en la que escrachan adolescentes. *Mendoza Online*.
- [11] Cf. La Voz. (s.f.). Confesiones por Instagram y escraches virtuales: nuevos modos de violentos de relacionarse.
- [12] Hackett, L. (2016). El ciberacoso y sus consecuencias para los derechos humanos. *Organización de las Naciones Unidas*.
- [13] Cf. UNICEF. (s.f.). Ciberacoso: Qué es y cómo detenerlo. Lo que los adolescentes quieren saber acerca del ciberacoso.
- [14] Cf. Hackett, L. (2016). El ciberacoso y sus consecuencias para los derechos humanos. *Organización de las Naciones Unidas*.
- [15] Sanchez Castañeda, A. (2018). Acoso Escolar y Cyberbullying. Retos, Prevención y Sensibilización. *UNAM Colección Los Derechos Universitarios en el siglo XX*.
- [16] Vega Osés, A., & Peñalva Velez, A. (2018). Los protocolos de actuación ante el acoso escolar y el ciberacoso en España: un estudio

por comunidades autónomas. *International Journal of New Education*.

## VII. BIBLIOGRAFÍA

Cardozo, G., Dubini, P., & Lorenzino, L. (2017). Bullying y ciberbullying: un estudio comparativo con adolescentes escolarizados. *Revista Mexicana de Psicología*. Recuperado de <https://www.redalyc.org/pdf/2430/243057743003.pdf>

Ginestar, A. (2021, noviembre 5). La peligrosa moda en Instagram en la que escrachan adolescentes. *Mendoza Online*. Recuperado de <https://www.mdzol.com/sociedad/2021/11/5/la-peligrosa-moda-en-instagram-en-la-que-escrachan-adolescentes-198537.html>

Hackett, L. (2016). El ciberacoso y sus consecuencias para los derechos humanos. *ONU*. Recuperado de <https://www.un.org/es/chronicle/article/el-ciberacoso-y-sus-consecuencias-para-los-derechos-humanos>

Herrera Lopez, M., y otros. (2018). Bullying y Cyberbullying en Latinoamérica. Un estudio bibliométrico. *Revista Mexicana de Investigación Educativa*. Recuperado de [https://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S1405-66662018000100125](https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-66662018000100125)

Incibe. Sexting. Recuperado de <https://www.incibe.es/menores/tematicas/sexting>

Instituto Interamericano de Derecho Humanos. (2014). Prevención del acoso escolar Bullying y Cyberbullying. Recuperado de <https://biblioteca.corteidh.or.cr/tablas/30036.pdf>

La Voz. (s.f.). Confesiones por Instagram y escraches virtuales: nuevos modos de violentos de relacionarse. Recuperado de <https://www.lavoz.com.ar/ciudadanos/confesiones-por-instagram-y-escraches-virtuales-nuevos-modos-de-violentos-de-relacionarse/>

Menor Sendra, J. (2018). Influencia en la violencia de los medios de comunicación: guía de buenas prácticas. Recuperado de [https://www.injuve.es/sites/default/files/2018/47/publicaciones/1.\\_influencia\\_en\\_la\\_violencia\\_de\\_los\\_medios\\_de\\_comunicacion.\\_guia\\_de\\_buenas\\_practicas.pdf](https://www.injuve.es/sites/default/files/2018/47/publicaciones/1._influencia_en_la_violencia_de_los_medios_de_comunicacion._guia_de_buenas_practicas.pdf)

Orriel, H. (2022). Cómo funciona el secreto mundo de las confesiones íntimas en Internet. *La Nación*. Recuperado de <https://www.lanacion.com.ar/tecnologia/como-funciona-el-secreto-mundo-de-las-confesiones-intimas-en-internet-nid07042022/>

Peñalva Velez, A., & Napal Fraile, M. (2018). Competencia digital y alfabetización digital de los adultos (profesorado y familias). *International Journal of New Education*. Recuperado de <https://www.revistas.uma.es/index.php/NEIJ/article/view/4892/4682>

Sanchez Castañeda, A. (2018). Acoso Escolar y Cyberbullying. Retos, Prevención y Sensibilización. *UNAM Colección Los Derechos Universitarios en el siglo XX*. Recuperado de <https://www.defensoria.unam.mx/web/publicaciones/CIBERBULLYING.pdf>

Segura Checa, J. A. (2018). Propuesta de un marco educativo para una sociedad sostenible. *International Journal of New Education*. Recuperado de <https://www.revistas.uma.es/index.php/NEIJ/article/view/4469/4683>

UNICEF. (s.f.). Ciberacoso: Qué es y cómo detenerlo. Lo que los adolescentes quieren saber acerca del ciberacoso. Recuperado de <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo#2>

Vega OSÉS, A., & PEÑALVA-VÉLEZ, A. (2018). Los protocolos de actuación ante el acoso escolar y el ciberacoso en España: un estudio por comunidades autónomas. *International Journal of New Education*. Recuperado de <https://www.revistas.uma.es/index.php/NEIJ/article/view/4924/4686>

Zimbrón, A. (2020). Comparación social: un factor que afecta a las personas en Facebook. *Notipress*. Recuperado de <https://notipress.mx/tecnologia/comparacion-social-un-factor-que-afecta-a-las-personas-en-facebook-3790>

## VIII. AUTOR



**González, Nadia Constanza.** Es Licenciada en Comunicación Social (UNSTA), Profesora en Comunicación Social (UMaza), Magíster en Dirección y Administración de Empresas (UNSTA), Experta en Tecnología Educativa (UTN) y se encuentra cursando el Doctorado en Comunicación en la línea de investigación de Nuevas Tecnologías (UNC).

Es Secretaria Académica de la Facultad de Ciencias Jurídicas, Políticas y Sociales de la Universidad del Norte Santo Tomás de Aquino y Directora del Proyecto Investigación: "La niñez y la comunicación digital: retos virales, grooming y ciberbullying". Fue Coordinadora Nacional de Relaciones Institucionales y Académicas de la ONG Grooming Argentina del 2022 al 2023. Dirigió y coordinó Diplomaturas en Ciberdelitos contra la niñez en la Universidad Provincial de Córdoba, la Universidad Nacional de Villa María, la Universidad Católica de Salta y la Universidad del Norte Santo Tomás de Aquino.

# Convivencia Digital en el Ámbito Educativo: Prevención y Acción ante las Ciber Violencias

María Paula Vega, Ana Haydee Di Iorio, María Fernanda Rosales, Facultad de Ingeniería, Universidad FASTA

**Abstract--** En el contexto de la educación superior, la función de las universidades no solo se limita a la formación de profesionales competentes en sus campos específicos, sino que se amplía hacia la responsabilidad de cultivar ciudadanos conscientes y éticos. La creciente incidencia de situaciones problemáticas relacionadas con la socialización digital y ciber violencias en entornos académicos subraya la necesidad de una formación integral de toda la comunidad educativa que trascienda las fronteras disciplinarias. Se presenta en este trabajo las medidas de acción y prevención, realizadas desde la Universidad FASTA, a través de la línea de I+D “Cuidado de las personas en el Mundo Digital – Internet Sana” para abordar las situaciones de ciber violencias dentro del aula, en el ámbito universitario.

**Index Terms--** ciber violencias - convivencia digital

## I. INTRODUCTION

Los educadores encargados del acompañamiento de las y los estudiantes precisan contar con directrices claras y con una capacitación actualizada para afrontar tanto enfoques preventivos como intervencionistas, que brinden un conjunto de estrategias para prevenir, abordar y resolver los conflictos que emergen en el ámbito virtual. Se debe tener en cuenta que, conocer el manejo de una tecnología no garantiza automáticamente la capacidad de lidiar con los riesgos asociados a su uso, entre los que se encuentran experiencias de sufrimiento y situaciones peligrosas, como por ejemplo las ciber violencias, el ciberacoso y la extorsión sexual, entre otras. Los procesos de construcción de subjetividad actuales presentan cualidades particularmente complejas (Inmediatez, fantasía del saber inagotable, lo diferido en la comunicación, corporalidad digital, lo interactivo, etc.) generando al mismo tiempo nuevas problemáticas, desafíos e incluso peligros [1]. La construcción de la identidad de los jóvenes se vincula cada vez más con el consumo, especialmente de tecnologías y de los productos asociados con ellas [2]. Pero asimismo se señala que es preciso ser conscientes que también en las redes sociales el poder está distribuido desigualmente. La convergencia digital determina la reorganización de los modos de acceso a los bienes culturales y de las formas de comunicación [3].

## II. PERSPECTIVA ACADÉMICA SOBRE LA NECESIDAD DE FORMACIÓN INTEGRAL EN CIUDADANÍA DIGITAL EN LA EDUCACIÓN SUPERIOR

Generalmente se vincula la socialización digital a las infancias y adolescencias, sin embargo, no está limitada exclusivamente a estas etapas madurativas del desarrollo. Las problemáticas que surgen de esta nueva forma de socialización, no se encuentran atadas a la cronología del individuo ni a su madurez psicosocial, sino que atraviesan de manera diversa todas las etapas vitales. La universidad, como institución educativa de nivel superior, debiera abordar de manera sistemática y profunda esta realidad, proporcionando las herramientas y orientaciones necesarias para la adecuada socialización digital de sus estudiantes. En este contexto, la socialización digital no solo se refiere a la competencia técnica en el uso de herramientas digitales, sino también a la capacidad de los individuos para participar de manera ética y respetuosa en los espacios virtuales. La transmisión de normas y pautas que rigen la interacción en línea se vuelve esencial en la formación integral de los estudiantes. La universidad, al asumir este compromiso, contribuye no solo al desarrollo académico y profesional de sus estudiantes, sino también a su preparación para ser ciudadanos digitales responsables en la sociedad.

## III. ACCIONES REALIZADAS POR LA UNIVERSIDAD FASTA PARA ABORDAR LAS CIBER VIOLENCIAS

Las ciber violencias en entornos educativos requieren un enfoque integral que aborde tanto la prevención como la acción una vez ocurridos los actos. Estos dos vectores, la prevención y la acción, deben ser considerados de manera transversal en diferentes momentos cruciales de la vida estudiantil, desde el último año del secundario hasta el perfil del egresado de la universidad.

### A. Programas de Convivencia Digital

La Facultad de Ingeniería de la UFASTA ha trabajado en la temática de los cuidados de las personas en el mundo digital desde 2012. Inicialmente, la iniciativa "Internet Sana" [4] se enfocó en acciones de divulgación, concientización y capacitación sobre los riesgos en Internet, especialmente dirigida a infancias y adolescencias. La firma de un convenio



con la Fundación Grooming Argentina en 2015 llevó a la María Paula Vega, Ana Haydee Di Iorio, María Fernanda Rosales, Facultad de Ingeniería, Universidad FASTA “Convivencia Digital en el Ámbito Educativo: Prevención y Acción ante las Ciber Violencias” L 2 creación de un eje de Responsabilidad Social en el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense - InFo-Lab, denominado "Internet Sana," para abordar la problemática desde la investigación, desarrollo tecnológico, extensión y transferencia en la temática. A lo largo del tiempo, otras facultades de la UFASTA y otras instituciones, tales como la Defensoría del Pueblo, la Subsecretaría de Niñez y Adolescencia de la Municipalidad de General Pueyrredon y la Unidad Fiscal de Contención Temprana de Conflictos Penales del Ministerio Público de la Provincia de Buenos Aires, se sumaron a las diversas acciones y proyectos de la línea. En un mundo cada vez más digital e irreversiblemente conectado, la línea de trabajo ha alcanzado la madurez necesaria para que la temática se transforme en una línea de investigación independiente, y se oriente a la producción y extensión del conocimiento en el campo del "Cuidado de las personas en el mundo digital" (Internet Sana). Al convertirse en toda una línea de investigación, deja de pertenecer a la Facultad de Ingeniería, y pasa a depender de Rectorado, encontrando así un espacio más apropiado e interdisciplinario para desarrollar investigaciones, extensión y transferencia. Las actividades realizadas hasta el momento han tenido un impacto significativo en la comunidad, tanto desde una perspectiva cualitativa como cuantitativa. Los proyectos de investigación y desarrollo han generado conocimiento e instrumentos metodológicos, como la “Guía de actuación docente frente a situaciones de ciberacoso” [5] que actualmente se aplican en colegios de gestión estatal y de gestión privada de la Municipalidad de General Pueyrredon y de la provincia de Buenos Aires, con perspectiva a ser aplicada en otras provincias. Decenas de colegios han adoptado estos materiales para mejorar la convivencia digital en sus espacios. Las actividades de extensión (charlas, jornadas y talleres) dirigidas a estudiantes, docentes, directivos y padres, han sido ampliamente aceptadas, con la participación de numerosos estudiantes y docentes en cada colegio donde se han llevado a cabo [6]. Específicamente los talleres se destacan no solo por su contenido, sino también por su capacidad de adaptarse a las necesidades particulares de cada institución, curso y grupo etario. Aunque cada taller tiene su particularidad, todos persiguen una serie de objetivos fundamentales. El enfoque principal es promover la reflexión crítica entre los estudiantes, incentivándolos a cuestionar y comprender las implicancias de la convivencia digital en su entorno educativo y en la sociedad en la que se encuentran inmersos; a partir de la integración de conceptos teóricos y su aplicación práctica. Al mismo tiempo, se busca que adquieran conciencia sobre la importancia de la identidad y la huella digital, medidas de seguridad y protección en línea, el manejo adecuado de la privacidad y la prevención del ciberbullying, la convivencia digital, los ciberdelitos y de las potenciales situaciones de ciber violencia, promoviendo una comprensión profunda de los conceptos y

problemas relacionados.

### *B. Intervención en Programas de Convivencia Digital*

Para abordar el tema de las ciber violencias en forma completa, se deben tener en cuenta todos los momentos por lo que pasa un estudiante en su trayectoria universitaria: desde el último año del secundario como articulación al nivel superior, hasta la definición de su perfil como egresado, donde se espera pueda ejercer en su ser profesional todos aquellos conocimientos, actitudes y valores adquiridos dentro de la universidad.

- Último año del Secundario En el último año del secundario, es fundamental la implementación de programas de sensibilización y educación digital que empoderen a los estudiantes con conocimientos sobre los riesgos asociados con las ciber violencias y las estrategias para prevenirlas. Además, se debe ofrecer orientación y recursos para reportar y abordar cualquier incidente que pueda surgir.

- Ingreso a la Universidad Al ingresar a la universidad, se deben continuar estas iniciativas de prevención, adaptándolas a las necesidades y desafíos específicos de este nuevo contexto educativo. En el caso de la Universidad FASTA, por ejemplo, en el Programa de Iniciación a la Vida Universitaria - PIVU - se brinda capacitación sobre el uso responsable de la tecnología y la navegación segura en línea, la convivencia y la convivencia digital. Asimismo, se establecen políticas claras contra las ciber violencias y procedimientos para abordarlas de manera efectiva en el curso de ingreso a la vida universitaria [7].

- Acompañamiento en la carrera universitaria Durante el transcurrir del estudiante por la vida universitaria, se deben promover espacios seguros y de confianza donde se pueda exponer abiertamente sus experiencias y preocupaciones relacionadas con las ciber violencias. Es importante la implementación de programas de apoyo emocional y psicológico, así como servicios de asesoramiento legal y mediación para aquellos que hayan sido afectados. En el marco del compromiso de la Universidad FASTA con la prevención y abordaje de las ciber violencias, se ha establecido un sólido Código de Convivencia que establece normas claras y expectativas éticas para todos los miembros de la comunidad. Este código incluye disposiciones específicas relacionadas con el uso responsable de la tecnología y la promoción de un entorno digital seguro y respetuoso. Además, la Universidad FASTA ha implementado un Protocolo de Actuación para Casos de Violencia, Abuso y Discriminación, diseñado para brindar una respuesta rápida y efectiva ante situaciones de ciber violencia que puedan surgir en el entorno universitario. Este protocolo establece procedimientos claros y transparentes para la recepción, investigación y resolución de denuncias, así como para la atención y apoyo integral a las personas afectadas. Además, se llevan a cabo campañas de sensibilización y capacitación para

toda la comunidad universitaria, con el fin de promover una cultura de prevención y protección frente a las ciber violencias. Este enfoque integral, 3 que combina la prevención a través del Código de Convivencia con una acción rápida y efectiva a través del Protocolo de Actuación [8], refleja el compromiso de la Universidad FASTA con la promoción de un entorno educativo seguro, inclusivo y libre de violencia. Por otro lado, la Universidad FASTA cuenta con un Gabinete de Contención permanente al cual cualquier miembro de la comunidad que se sienta víctima de alguno de los supuestos establecidos en el protocolo, podrá acudir para recibir atención, contención, escucha, orientación y asesoramiento. A tal fin, la Universidad habilita diversos medios de comunicación en los cuales está garantizada la confidencialidad sobre los hechos y la reserva sobre las identidades, en la medida en que la víctima así lo desee.

- Competencias en el perfil del egresado El perfil del egresado de una institución educativa debe reflejar no sólo un alto nivel de competencia académica, sino también un compromiso con la dignidad digital [9] y el respeto por los demás en el entorno digital. Los egresados deben estar equipados con las habilidades y valores necesarios para prevenir y abordar las ciber violencias en sus futuras trayectorias profesionales y personales asegurando que los egresados sean agentes de cambio positivo en la sociedad digital. En tal sentido, en la Universidad FASTA, se busca identificar rasgos de identidad del graduado que hacen a la persona, ajena a su rol profesional y a la profesión, y competencias genéricas como el conjunto de conocimientos, habilidades, actitudes y aptitudes que se esperan que obtenga, y que hacen a la persona en su rol universitario un graduado de la Universidad FASTA al final de su proceso formativo [10].

#### IV. PROBLEMÁTICAS

En el contexto universitario, las relaciones y vínculos entre estudiantes juegan un papel crucial en la dinámica académica y social. Sin embargo, estas relaciones pueden ser el escenario donde se manifiestan formas de acoso u hostigamiento. La violencia general en este ámbito se manifiesta a través de conductas de hostigamiento, intimidación o malos tratos, que pueden generar miedo o desánimo en cualquier miembro de la comunidad universitaria, ya sea empleado o estudiante, subordinado o no. Estas conductas pueden ocurrir tanto dentro como fuera del ámbito laboral o académico, y pueden manifestarse a través de medios físicos o virtuales. Estas dinámicas de violencia en las relaciones entre estudiantes pueden tener un impacto significativo en el bienestar emocional y académico de quienes las experimentan, así como en el clima general de convivencia en el aula y en la comunidad universitaria. Por lo tanto, es fundamental que las instituciones adopten medidas proactivas para prevenir y abordar estas formas de violencia, promoviendo una cultura de respeto, empatía y colaboración entre todos los miembros de la comunidad universitaria. Un caso particular, es el de la violencia de género, que constituye una problemática actual de

envergadura [11]. Esta afectación de la convivencia [12], los daños a la reputación, a la victimización y revictimización en el marco de agresiones diversas, se configura como un fenómeno que requiere abordajes transdisciplinarios desde lo técnico, legal, educacional y sanitario y especialmente desde una perspectiva de género. La violencia puede adoptar múltiples facetas, como la física, que busca producir lesiones o daño al cuerpo de una persona; la psicológica, que procura causar daño emocional o disminución de la autoestima mediante el hostigamiento, amenazas o ridiculización; la sexual, que vulnera el derecho a decidir libremente sobre la vida sexual a través de intimidación o acoso; la económica o patrimonial, que busca afectar los recursos económicos o patrimoniales de una persona; la simbólica, que utiliza mensajes o expresiones hostiles y humillantes; y el bullying, que constituye cualquier forma de maltrato psicológico, verbal, físico o social, repetido y prolongado en el tiempo, tanto en el ámbito físico como virtual. Los vínculos entre estudiantes, docentes y personal administrativo son fundamentales en el entorno universitario, pero también pueden ser vulnerables a diferentes formas de violencia que afectan la convivencia y el clima institucional. En la prevención de ciber violencias y en el desarrollo de estrategias de convivencia digital, una buena práctica resulta el aprendizaje en comunidad a través de las problemáticas propias de la población y la experiencia en el territorio [13]. Entre los tipos de violencia que pueden darse en estos vínculos se encuentran:

- Violencia simétrica (entre pares): Esta forma de violencia puede manifestarse en el acoso virtual, hostigamiento o acoso entre estudiantes o docentes. Las interacciones en línea, como los mensajes intimidatorios o difamatorios, la exclusión social en grupos en línea y la difusión de rumores maliciosos, pueden crear un ambiente tóxico y perjudicar la salud emocional y el rendimiento académico de los afectados.

- Violencia asimétrica (con diferente jerarquía): Los docentes y el personal administrativo pueden ejercer violencia de autoridad aprovechando su posición de poder, ya sea para obtener servicios o conductas indebidas. De la misma manera, los estudiantes pueden ejercer actos de ciber violencias contra los docentes. A. Ejemplos de casos de problemáticas reales

##### Caso 1: Ciberacoso Estudiantil por Motivos Étnicos

En una carrera universitaria presencial se realizan encuentros sincrónicos a través de una plataforma, donde un estudiante sufre ciberacoso basado en motivos étnicos. La situación se agrava cuando sus compañeros realizan comentarios ofensivos sobre "modismos" de su lenguaje, burlas sobre su vocabulario, peinados y vestimenta, realizando una ridiculización de rasgos faciales, y provocando que el estudiante decida no encender la cámara durante las clases en línea. Este ciberacoso afecta directamente su rendimiento académico y su participación activa en los encuentros virtuales.

Agravios:

- "¿Por qué hablas así? No te entendemos. Deberías aprender a hablar como nosotros."
- "Tu forma de expresarte es extraña. ¿Realmente perteneces aquí?"
- Ridiculización de rasgos faciales mediante emojis y comentarios despectivos.

#### Impacto:

- Bienestar Emocional: El estudiante sufre consecuencias emocionales significativas debido a los comentarios ofensivos, lo que se traduce en ansiedad y estrés.
- Rendimiento Académico: La situación afecta negativamente su rendimiento académico, ya que la participación activa en clases es esencial para el aprendizaje.
- Participación en Encuentros Virtuales: La presión y el acoso llevan al estudiante a evitar mostrar su cámara, limitando su interacción con el grupo y su participación en actividades colaborativas.

#### Intervención:

- Se realizó un taller con todo el curso con un enfoque de generar conciencia y reflexionar respecto a la formación integral del profesional, la no discriminación y la aceptación de las diferencias.

#### Caso 2: Copia y Ciberacoso en Grupo de WhatsApp

En el entorno de una carrera de educación a distancia, durante el período de ingreso la Gestora de Asuntos Estudiantiles de la carrera arma un grupo de WhatsApp para intercambiar información académica, fechas importantes de exámenes y aportes de las asignaturas, abandonando luego el grupo. En este grupo, un estudiante expresa su desaprobación por la práctica de copiar y compartir respuestas, comentando "Estamos en esta carrera para formarnos y aprender, no me parece ético copiarse y pasar las respuestas". A raíz de este comentario, el estudiante es objeto de agresiones verbales y ciberacoso.

#### Agravios:

- "¿Quién se cree este 'sabelotodo'? Todos estamos aquí para pasar, no para aprender."
- Burlas constantes sobre la responsabilidad académica del estudiante.
- Creación y difusión de memes con su rostro, utilizados para ridiculizarlo en el grupo.

#### Impacto:

- Angustia y Rechazo: El estudiante experimenta una profunda angustia debido a las agresiones verbales y la discriminación, generando un ambiente hostil.
- Aislamiento: La actitud del grupo lo lleva al aislamiento, limitando su participación activa y afectando su experiencia académica.
- Impacto Emocional Duradero: Las agresiones, memes y ciberacoso dejan un impacto emocional duradero en el estudiante, afectando su confianza y bienestar mental.

#### Intervención:

- Se creó un espacio de escucha y contención al estudiante. Esta situación se dio previo a la existencia del Protocolo de Actuación para Casos de Violencia, Abuso y Discriminación. Estos casos que se están presentando fueron algunos de los que motivaron la creación de este protocolo.

#### Caso 3: Exposición y Ciberacoso hacia una Docente

En un espacio áulico del último año del nivel secundario, una docente se encuentra escribiendo en el pizarrón de espaldas a la clase. En ese momento, un estudiante toma una foto sin su conocimiento y la viraliza en redes sociales y grupos estudiantiles. Esta acción, realizada con la intención de exponer y ridiculizar, genera incomodidad, invade la imagen personal de la docente y pone en juego su reconocimiento.

#### Agravios:

- Comentarios detallados sobre la apariencia de la docente acompañando la imagen viralizada.
- Burlas sobre su forma de enseñar, utilizando la foto para ridiculizar su postura mientras escribe en el pizarrón.

#### Impacto:

- Incomodidad y Vulnerabilidad: La docente se siente invadida en su privacidad, generando incomodidad y vulnerabilidad.
- Daño a la Imagen Profesional: La exposición pública afecta la imagen profesional del docente, poniendo en peligro su reconocimiento y respeto en la comunidad educativa.
- Distracción en el Entorno Académico: La distracción causada por la situación afecta el ambiente de aprendizaje y el rendimiento de los estudiantes.

#### Intervención:

- Se creó un espacio de escucha y contención al docente, y se intervino en el aula con los estudiantes. Se dictaron talleres con los docentes sobre cómo actuar en casos de ciber violencias y se recomendó la incorporación de estas situaciones en el código de convivencia de cada asignatura.

## V. A MODO DE CONCLUSIÓN Y NUEVOS DESAFÍOS

En la era digital, las universidades se encuentran ante un panorama complejo y dinámico, donde las relaciones interpersonales se entrelazan con la tecnología. Este nuevo escenario obliga a reflexionar sobre los desafíos emergentes y el papel crucial que desempeña en la formación de ciudadanos responsables y empáticos. Es imperativo que ante los casos de ciber violencias las universidades adopten estrategias integrales para prevenir y abordar las diferentes formas de violencia que surgen en el entorno digital. En este contexto de desafíos y riesgos asociados a la interacción digital, la implementación de un código de convivencia en los entornos educativos cobra una relevancia significativa. Estos códigos no solo buscan prevenir y abordar los conflictos derivados de las ciber violencias, sino que también representan un compromiso con la promoción de valores fundamentales como

el respeto, la empatía y la responsabilidad en el uso de las tecnologías. Al establecer directrices claras y coherentes, el código de convivencia 5 proporciona un marco sólido para fomentar un ambiente seguro y saludable en el ámbito educativo, promoviendo así la reflexión crítica, el diálogo constructivo y el desarrollo de habilidades emocionales en los estudiantes. Por otro lado, con la implementación de Protocolos de Actuación se busca propiciar en la comunidad universitaria un ambiente libre de discriminación, hostigamiento, violencia, promoviendo condiciones de igualdad y equidad; adoptar medidas de prevención como principal método para combatir este tipo de situaciones; generar ámbitos de confianza y seguridad para que las personas afectadas puedan exponer su situación, a fin de hacerla cesar de inmediato y establecer, en su caso y a través de los procedimientos de investigación vigentes las responsabilidades y sanciones que pudieren corresponder; y asesorar, contener y orientar a las personas afectadas. Los códigos de convivencia y los protocolos de actuación son herramientas clave en el abordaje de las ciber violencias para construir entornos digitales seguros y saludables donde cada individuo pueda desarrollarse plenamente y alcanzar su máximo potencial. Esto permite que todos se perciban como parte del problema y de la solución, que no se busque identificar agresores o víctimas desde estereotipos, sino de entender las situaciones que se generan en la convivencia como comportamientos que pueden ser vividos como agresivos, situaciones de acoso o actos delictivos. La retroalimentación realizada con docentes, el área de gestión universitaria y el feedback con los estudiantes luego de las intervenciones permite también establecer un proceso continuo de evaluación y reformulación de los nuevos desafíos de la Universidad actual en forma conjunta. Por último, estos nuevos escenarios digitales obligan a continuar pensando, escuchando y teorizando las experiencias, en relación al rol de la educación, a la misión de la Universidad y a la prevención de las ciber violencias.

## VI. REFERENCIAS

[1] Vega et. (2020). Guía de actuación para docentes frente a situaciones de ciberacoso. Ed. Universidad FASTA. Mar del Plata. [Online]. Disponible en: <https://info-lab.org.ar/images/pdf/ECUIDADOS.pdf>

[2] N.G. Canelini, “Lectores, espectadores e internautas”, ed. Gedisa, (2007)

[3] N.G. Canelini, “Lectores, espectadores e internautas”, ed. Gedisa, (2007)

[4] Universidad FASTA (2024). Internet Sana. [Online]. Disponible en: <http://infolab.ufasta.edu.ar/internetSana/>

[5] Vega et. al (2020). Guía de actuación para docentes frente a situaciones

de ciberacoso. Ed. Universidad FASTA. Mar del Plata. Disponible en: <https://info-lab.org.ar/images/pdf/ECUIDADOS.pdf>

[6] Vega et. (2020). Programas de intervención en la comunidad educativa frente a las situaciones conflictivas mediadas por la tecnología en el ámbito escolar. [Online]. Disponible en: [https://49jaiio.sadio.org.ar/pdfs/sts/STS\\_18.pdf](https://49jaiio.sadio.org.ar/pdfs/sts/STS_18.pdf)

[7] Universidad FASTA (2024). Ingreso a la Universidad. [Online]. Disponible en: <https://www.ufasta.edu.ar/ingreso/programa-de-ingreso/>

[8] Universidad FASTA (2023). Protocolo de actuación para casos de violencia, abuso y discriminación en la universidad FASTA. [Online]. Disponible en: <https://www.ufasta.edu.ar/wp-content/uploads/2023/11/Protocolo-de-actuacion-para-casos-de-violencia-abuso-y-discriminacion-en-la-Universidad-Fasta.pdf>

[9] Mena, Juan Carlos (2021). Dignidad Digital. [Online]. Disponible en: <https://www.youtube.com/watch?v=3-JXCvkhQ8>

[10] Mena, Juan Carlos (2018). Resolución Rector UFASTA 375-18. Rasgos de la Identidad del Graduado de UFASTA. [Online]. Disponible en: [https://www.ufasta.edu.ar/wp-content/uploads/2020/06/Rasgos-de-Identidad\\_Graduado-Ufasta-2.pdf](https://www.ufasta.edu.ar/wp-content/uploads/2020/06/Rasgos-de-Identidad_Graduado-Ufasta-2.pdf)

[11] Congreso de la Nación Argentina. (2021). Ley Micaela. Ed. ICN. [Online]. Disponible en: <https://www.argentina.gob.ar/generos/ley-micaela>

[12] Fondo de las Naciones Unidas por la Infancia (2006). [Online]. Disponible en: [https://www.unicef.org/Revised\\_CPD\\_Dom\\_Rep\\_-\\_Spanish\\_-\\_8\\_Nov\\_06\(1\).pdf](https://www.unicef.org/Revised_CPD_Dom_Rep_-_Spanish_-_8_Nov_06(1).pdf)

[13] Levin, E. ¿Hacia una infancia virtual?: la imagen corporal sin cuerpo. (2006)

# Derechos Humanos, Inteligencia Artificial, Ética y Constitucionalismo Digital

1

Colombo, Cristiano, Profesor del Programa de Maestría Profesional en Derecho de la Empresa y de los Negocios da UNISINOS e da Facultad Verbo Jurídico. Engelmann, Wilson, Profesor del Programa de Postgrado en Derecho - Maestría y Doctorado y Maestría Profesional en Derecho de la Empresa y de los Negocios.

**Resumen:** El uso de la inteligencia artificial (IA) está entrando en los más variados sectores de la vida de la sociedad. Los sistemas de toma de decisiones se destacan en el Poder Judicial, educación, salud, entre otras aplicaciones. La regulación de la IA, al representar un uso global y no restringido al espacio de cada país, presenta características específicas. Por tanto, la directriz ética definida por los Derechos Humanos, canalizado hacia un constitucionalismo digital y principista, podría suponer un cambio. El artículo aborda estas conexiones a través de una investigación bibliográfica y documental. La investigación mostró que el constitucionalismo digital, estructurado en principios por la directriz de Derechos Humanos, es un camino creativo para desarrollar.

**Palabras-clave:** *Derechos humanos; Inteligencia artificial; Constitucionalismo digital; Principios jurídicos.*

**Abstract:** The use of artificial intelligence (AI) is entering the most varied sectors of society's life. Decision-making systems stand out in the Judiciary, education, health, among other applications. The regulation of AI, as it represents a global use and not restricted to the space of each country, presents specific characteristics. Therefore, the ethical guideline defined by Human Rights, channeled towards a digital and principled constitutionalism, could represent a change. The article

addresses these connections through bibliographic and documentary research. The research showed that digital constitutionalism, structured in principles by the Human Rights guideline, is a creative path to develop.

**Keywords:** *Human rights; Artificial intelligence; Digital constitutionalism; Legal principles.*

## I. INTRODUCCIÓN

El estudio está dedicado a la Inteligencia Artificial, con el fin de buscar reflexionar sobre lineamientos éticos, basados en los Derechos Humanos, canalizados por un constitucionalismo digital y principista.

En la Sección II se presentarán las relaciones entre Derechos Humanos, Inteligencia Artificial, Ética y Constitucionalismo Digital. El artículo aborda estas conexiones a través de una investigación bibliográfica y documental.

## II. LOS DERECHOS HUMANOS, LA INTELIGENCIA ARTIFICIAL, ÉTICA Y EL CONSTITUCIONALISMO DIGITAL

El siglo XXI está marcado por el rápido avance de diversas tecnologías, entre las que destacan las nanotecnologías y la Inteligencia Artificial (IA). El acceso humano a la escala nanométrica, que equivale a una mil millonésima parte de un metro, ha permitido el desarrollo de sistemas tecnológicos que pueden emular algunas capacidades humanas, como: pensar, actuar, pensar racionalmente y actuar de forma racional (adaptado de Preparing ..., 2016). A partir de estos supuestos, y teniendo en cuenta la ausencia de consenso sobre lo que debe considerarse como "inteligencia artificial", se parte del siguiente concepto, que destaca la IA como un concepto complejo y polifacético, que debe vincularse a artefactos

<sup>1</sup> Este trabajo es el resultado parcial de las investigaciones realizadas por los autores en el marco de los siguientes proyectos de investigación: a) Convocatoria CNPq n. 09/2020 - Becas de Productividad Investigadora - PQ, proyecto titulado: "Vías de resignificación de la Teoría General de las Fuentes del Derecho: el Sandbox normativo como elemento estructurador de la comunicación reticular entre Derecho y nanotecnologías"; b) "Sistema de Derecho, nuevas tecnologías, globalización y constitucionalismo contemporáneo: retos y perspectivas", Edital FAPERGS/CAPES 06/2018 - Programa de Internacionalización de Postgrado en RS. Este trabajo también está vinculado a las investigaciones realizadas por los autores en los siguientes Centros Internacionales de Investigación: CEDIS - Centro de Investigación y Desarrollo sobre Derecho y Sociedad, de la Facultad de Derecho de la Universidade Nova de Lisboa, Portugal; del Instituto Jurídico Portucalense, de la Universidad Portucalense, ciudad de Oporto, Portugal; y del CEAD - Centro Francisco Suárez - Centro de Estudios Avanzados en Derecho de la Universidad Lusófona de Lisboa, Portugal.

Cristiano Colombo: Postdoctorado en Derecho, Pontificia Universidad Católica de Rio Grande do Sul (PUCRS). Doctor y Magíster en Derecho, Programa de Postgrado en Derecho de la Universidad Federal de Rio Grande do Sul

(UFRGS). Profesor Titular de la Maestría Profesional en Derecho de la Empresa y de los Negocios de Unisinos; Profesor de Licenciatura en Derecho y Relaciones Internacionales de Unisinos; Profesor de Licenciatura en Derecho de la Facultad Verbo Jurídica; Investigador Fapergs (2021-2023). Correo electrónico: cristianocolombo@unisinos.br

Wilson Engelmann: Doctor y Master en Derecho Público, Programa de Postgrado en Derecho de la Universidad de Vale do Rio dos Sinos - UNISINOS, Brasil; realizó Pasantía Post-Doctoral en Derecho Público-Derechos Humanos, en el Centro de Estudios de Seguridad (CESEG) de la Universidad de Santiago de Compostela, España; Profesora e Investigadora del Programa de Postgrado en Derecho - Maestría y Doctorado y Maestría Profesional en Derecho de la Empresa y de los Negocios, ambos de UNISINOS; Becaria de Productividad en Investigación del CNPq; Líder del Grupo de Investigación JUSNANO; e-mail: wengelmann@unisinos.br; ORCID: <https://orcid.org/0000-0002-0012-3559>.

tecnológicos, a determinados métodos o a determinada área científica, en algunos casos, situándose aún en subáreas, que están en constante modificación, que requieren componentes de hardware y software, y que contiene componentes en condiciones de aprender, es decir, capaces de cambiar el comportamiento del sistema en función de los datos presentados y del procesamiento de estos datos.<sup>2</sup> Es un tipo de automatización que tiene como objetivo “clasificar objetos, evaluar y juzgar eventos, identificar diferencias y similitudes, y así reconocer cosas, actividades y personas”.<sup>3</sup> Se observa que la IA está siempre vinculada a un proceso de aprendizaje, estructurado a partir de datos: cuanto mayor sea el número de datos de que disponga el sistema, mayor será su nivel de aprendizaje. Aún así, en la línea conceptual, es importante señalar que Floridi critica el término “Inteligencia Artificial”, por ser el “divorcio” del actuar desde la “necesidad de ser inteligente”. Por tanto, presenta la ecuación “IA = agere sine intelligere”. Destaca que, anteriormente, “actuar, ser inteligente e intencionalidad” eran inseparables.<sup>4</sup> Y, añade Floridi, esta separación es la gran fuente de “nuevos desafíos éticos que plantea la IA”.<sup>5</sup>

Bertaso y Marcos presentan la Inteligencia Artificial “como un conjunto de tecnologías que permiten la elaboración de datos y la formulación de pautas a través de métodos computacionales altamente automatizados”.<sup>6</sup> Además, plantean una cuestión importante, respecto de las actividades humanas, en el sentido de que la Inteligencia Artificial ¿debe integrarse o convertirse en un sustituto?<sup>7</sup> Refuerzan que los optimistas entienden que “los sistemas de IA estarán a nuestro servicio, nos ayudarán en diversas tareas y, en general, en el pleno cumplimiento de la vida humana”. Por otro lado, los pesimistas defienden la incompatibilidad de la vida entre personas y máquinas, siendo la Inteligencia Artificial “una nueva forma de barbarie y, en consecuencia, la obligación de combatirla”.<sup>8</sup> De todas formas, sostienen que ser inteligente está ligado a hacer cosas bonitas y buenas, con ventajas para ellos y la comunidad.<sup>9</sup> Federico Cabitza advierte que, en la relación entre tecnología y ética, conviene evitar considerar la IA como algo dotado de “agencia”, que tiene “capacidad autónoma de acción”, para que

no conduzca a el error de atribuir a las máquinas “una identidad, una voluntad autónoma”.<sup>9</sup>

Lo Reglamento del Parlamento Europeo y del Consejo Europeo (denominada Ley de IA) presenta la categoría conceptual de “sistema de inteligencia artificial”, como un software que, desarrollado a partir de un conjunto variado de técnicas y enfoques orientados a un determinado conjunto de objetivos definidos por el ser humano, generan salidas como contenidos, predicciones, recomendaciones o decisiones que influyen en los entornos con los que interactúan.<sup>10</sup>

Esta concepción destaca la importancia de la participación del ser humano en la definición de los objetivos que debe alcanzar el sistema de IA. Cabitza destaca que los artefactos, en su “hacer”, traducen un “programa de acción”, que puede entenderse como “una serie de instrucciones”, a partir de un *script*. En las máquinas, “el *script* está codificado en términos de un algoritmo”.<sup>11</sup> La ejecución del algoritmo revela una función, que “determina una serie de objetivos definidos por el ser humano”. Por tanto, debemos reflexionar sobre la posibilidad de “inscribir comportamientos éticos en los scripts de las máquinas y sus algoritmos”.<sup>12</sup> Si tiene una característica fundamental: la tecnología debe permanecer bajo control humano.<sup>13</sup> Dicha garantía asegura una protección de los derechos y garantías fundamentales (en el plan regulador interno), además de ser un elemento protector para salvaguardar los Derechos Humanos (en el plan regulador externo).

El mantenimiento y fortalecimiento de esta barrera de salvaguarda servirá para hacer frente a uno de los riesgos que a menudo se señalan en relación con los avances de la IA: que el ser humano pueda perder el control sobre el sistema. Esta línea de preocupación es subrayada por Luciano Floridi, cuando afirma: “La IA no es simplemente otra utilidad que necesita ser regulada cuando está madura. Es una fuerza poderosa que está remodelando nuestras vidas, nuestras interacciones y nuestros entornos”.<sup>14</sup> Analizando el escenario actual del desarrollo de la IA, puede decirse que únicamente está en su “infancia”, es decir, que aún hay margen para avanzar y no cabe duda de que la mencionada remodelación de Floridi puede hacerse realidad.

En la literatura se pueden encontrar indicios de varias etapas de la IA, como en el caso de Kaplan y Haenlein: la primera

<sup>2</sup> KÖNIG, Pascal D.; KRAFFT, Tobias D.; SCHULZ, Wolfgang; ZWEIG, Katharina A. Esencia de la IA: ¿Qué es la IA? En L. DiMatteo, C. Poncibò y M. Cannarsa (Eds.). *The Cambridge Handbook of Artificial Intelligence: Global perspectives on Law and Ethics*. Manuales de Derecho de Cambridge. Cambridge: Cambridge University Press, 2022, pp. 18-34. Doi: 10.1017/9781009072168.005.

<sup>3</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>4</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021, p. 150.

<sup>5</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021, p. 150.

<sup>6</sup> BERTOLASO, Marta; MARCOS, Alfredo. *Umanesimo tecnologico*. Roma: Carocci Editore, 2023, p. 9.

<sup>7</sup> BERTOLASO, Marta; MARCOS, Alfredo. *Umanesimo tecnologico*. Roma: Carocci Editore, 2023, p. 9.

<sup>8</sup> BERTOLASO, Marta; MARCOS, Alfredo. *Umanesimo tecnologico*. Roma: Carocci Editore, 2023, p. 10.

<sup>9</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>10</sup> Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas para la Inteligencia Artificial (Reglamento sobre Inteligencia Artificial) y se modifican determinados actos legislativos de

la Unión. Bruselas, 21.4.2021 COM (2021) 206 final. 2021/0106 (COD). Disponible en: [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF). Consultar texto recientemente aprobado: <https://www.europarl.europa.eu/news/pt/press-room/20240308IPR19015/reglamento-inteligencia-artificial-parlamento-aprova-legislacao-historica>. Consultado el 15 de marzo de 2024.

<sup>11</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>12</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>13</sup> CODAGNONE, Cristiano; LIVA, Giovanni; RODRIGUEZ DE LAS HERAS BALLELL, Teresa. *Identificación y evaluación de la legislación comunitaria existente y en proyecto en el ámbito digital: Estudio para la comisión especial sobre Inteligencia Artificial en la Era Digital (AIDA)*, Departamento de Políticas Económicas, Científicas y de Calidad de Vida, Parlamento Europeo, Luxemburgo, 2022. Disponible en: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL\\_STU\(2022\)703345\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_STU(2022)703345_EN.pdf). Consultado el 15 de marzo de 2024.

<sup>14</sup> FLORIDI, Luciano. La legislación europea sobre IA: breve análisis de su enfoque filosófico. En J. Mökander; M. Ziosi (eds.). *El Anuario 2021 del laboratorio de ética digital, Digital Ethics Lab Yearbook*. Suiza AG: Springer Nature, 2022.

etapa es la llamada inteligencia artificial limitada, ya que depende de la "alimentación" de datos promovida por la acción humana; sin condiciones para resolver problemas de forma autónoma. Este es el estado actual del desarrollo de la IA. La segunda etapa se caracteriza por la llamada "inteligencia artificial general", que se aplica en muchos ámbitos y es capaz de resolver varios problemas de forma autónoma. Lo que más llama la atención es la posibilidad de superar o igualar las actividades humanas en diversos ámbitos. A partir de ahí, se abre el espacio para la tercera etapa, la llamada "superinteligencia artificial", que podrá aplicarse a cualquier ámbito, siendo capaz de resolver problemas al instante y pudiendo superar a los humanos en todas las áreas.<sup>15</sup>

Las fases de desarrollo de la IA también ponen de manifiesto nuevos niveles de riesgo, el principal de los cuales es la posibilidad de realizar acciones humanas en todos los ámbitos. Stefano Rodotà, en su libro *Il mondo nella rete: quali i diritti, quali i vincoli*, 2014, menciona que estamos viviendo la "dictadura del algoritmo", con la posibilidad de su profundización y expansión, generando una despersonalización de la sociedad, donde la persona del decisor desaparece gradualmente, de hecho sustituida por el procedimiento automatizado; desaparece y la persona considerada en sí misma, transformada en un objeto de poderes incontrolables.<sup>16</sup> Con ello, se tiene un personaje que roza la consideración de "aterrador", dados los posibles impactos. Otro ejemplo que puede extraerse de la sociedad alemana, pero que probablemente se encuentre en cualquier lugar en el que se utilice la IA: el riesgo de los programas policiales predictivos sustentados en una información inadecuada o en predicciones erróneas, que pueden resultar sesgadas, cubriendo siempre las mismas zonas y a las mismas personas (o grupo específico de personas). Un caso concreto, con esta base fáctica, fue llevado ante el Tribunal Constitucional alemán: "¿pueden los programas informáticos de vigilancia, orientados en su uso hacia fines predominantemente predictivos, ser utilizados por las fuerzas policiales en la prevención y la lucha contra la aparición de fenómenos de carácter delictivo? El juicio de este caso comenzó a finales de diciembre de 2022 y se completó a principios de 2023. El Tribunal prohibió el uso de esta forma de supervisión. El uso predictivo se basa, en esa medida, en modelos matemáticos y otras técnicas de naturaleza analítica en el proceso de aplicación de la ley, con el fin último de identificar posibles actividades delictivas y, también, a sus autores potenciales y previsibles. En este caso real, la vida está "imitando a la ficción", que se retrató en la película "Minority Report", Tom Cruise se enfrenta a una acusación de asesinato que aún no ha cometido por parte de tres "videntes" que pueden ver el futuro, mientras que el Tribunal Constitucional alemán se enfrenta ahora, en el mundo real y ya no únicamente en el trasfondo de la ficción, a una denuncia presentada por la Sociedad Alemana de Derechos Civiles sobre la legalidad del

uso del potente software "Gotham" de la empresa estadounidense Palantir y destinado a fomentar la vigilancia policial en los estados de Hesse y Hamburgo. Denominado en Hesse "Hessendata", este software es capaz de buscar entre voluminosas cantidades de datos procedentes y recogidos en los distintos medios de comunicación y, en última instancia, permite elaborar perfiles de presuntos delincuentes antes incluso de que se produzcan. Preocupación por la privacidad, dado el carácter sensible y personal de los datos recogidos, riesgos asociados a la seguridad de dichos datos y a su intercambio ilegítimo con terceros para otros fines, riesgo de falta de precisión, ya que la fiabilidad de la policía predictiva está estrechamente ligada a la calidad de los datos y a la integridad de sus usuarios. Basta pensar, por ejemplo, que las estadísticas criminales recogidas en función de políticas racistas o xenófobas tenderán a potenciar las predicciones racistas, impulsando a una vigilancia policial excesiva y desproporcionada en determinados márgenes de población y alimentando un verdadero círculo vicioso de estigmatización permanente de los mismos grupos e individuos.<sup>17</sup>

Más allá de estas situaciones, también cabe destacar: la IA puede utilizarse para analizar toda su salud financiera, incluidos los gastos, los ahorros y otras deudas, para obtener una imagen más amplia del consumidor: si se diseñan correctamente, estos sistemas pueden proporcionar un acceso más amplio a créditos asequibles. Pero uno de los mayores peligros es el sesgo involuntario, en el que los algoritmos acaban denegando préstamos o cuentas a determinados grupos, como las mujeres, los inmigrantes o las personas de color. Parte del problema es que la mayoría de los modelos de IA solo pueden aprender de los datos históricos que se les han suministrado, lo que significa que aprenderán a qué tipo de cliente se ha prestado anteriormente y qué clientes han sido señalados como poco fiables. De este modo, existe el peligro de que estén sesgados en cuanto a cómo es un "buen" prestatario: el género y la etnia suelen desempeñar un papel importante en los procesos de toma de decisiones de la IA basados en los datos que se le han enseñado. Además, algunos modelos están diseñados para ser ciegos a las llamadas características protegidas, lo que significa que no deben tener en cuenta la influencia del género, la raza, la etnia o la discapacidad. Pero estos modelos de IA aún pueden discriminar como resultado del análisis de otros datos, como los códigos postales, que pueden correlacionarse con grupos históricamente desfavorecidos que nunca han solicitado, obtenido o pagado préstamos o hipotecas. Y en la mayoría de los casos, cuando un algoritmo toma una decisión, es difícil que nadie entienda cómo ha llegado a esa conclusión, lo que da lugar a lo que comúnmente se conoce como el síndrome de la "caja negra". Esto significa que los bancos, por ejemplo, pueden tener dificultades para explicar qué podría haber hecho de forma diferente un solicitante para optar a un préstamo o a una tarjeta de crédito, o si cambiar el sexo de un solicitante de

<sup>15</sup> KAPLAN, Andreas; HAENLEIN, Michael. Siri, Siri, en mi mano: ¿Quién es la más bella del país? Sobre las interpretaciones, ilustraciones e implicaciones de la inteligencia artificial. En: *Business Horizons*, v. 62, p. 15-25, 2019.

<sup>16</sup> RODOTÀ, Stefano. *Il mondo nella rete: quali i diritti, quali i vincoli*. Bari, Roma: Editori Laterza, 2014.

<sup>17</sup> SILVA, MARIO TAVARES DA. *VIGILANCIA POLICIAL PREDICTIVA Y DERECHOS FUNDAMENTALES*. 30 DE DICIEMBRE DE 2022. DISPONIBLE EN: [HTTPS://EXPRESSO.PT/OPINIAO/2022-12-30-POLICIAMENTO-PREDITIVO-E-](https://expresso.pt/opiniaO/2022-12-30-POLICIAMENTO-PREDITIVO-E-)

DIREITOS-FUNDAMENTAIS-46FCE25A. CONSULTADO EL 15 MARZO 2024; GOLDENBERG, RINA. ALEMANIA: EL SOFTWARE DE VIGILANCIA POLICIAL, UN QUEBRADERO DE CABEZA LEGAL - TBEN - 12/22/2022. THE BHARAT EXPRESS NEWS, 22 DE DICIEMBRE DE 2022. DISPONIBLE EN: [HTTPS://WWW.THEBHARATEXPRESSNEWS.COM/GERMANY-POLICE-SURVEILLANCE-SOFTWARE-A-LEGAL-HEADACHE-TBEN-12-22-2022/](https://www.thebharatexpressnews.com/germany-police-surveillance-software-a-legal-headache-tben-12-22-2022/). CONSULTADO EL 15 MARZO 2024.



hombre a mujer podría dar lugar a un resultado diferente.<sup>18</sup> Los riesgos que conllevan estas consecuencias por el uso de sistemas de IA se denominan "discriminación algorítmica"<sup>19</sup>. Cabe decir que, dado que el desarrollo de la IA se encuentra aún en la primera fase caracterizada anteriormente, la "inteligencia" del sistema depende de la selección y alimentación de datos promovida por los seres humanos. Parece difícil que alguien sea absolutamente neutral en la selección de los datos que se insertarán en el sistema. Aquí se presenta un gran reto y un riesgo, porque el sistema discriminará a partir del contenido de los datos que se hayan seleccionado para alimentarlo.

Stefano Rodotà plantea preguntas adecuadas al contexto así desvelado: "aparecen robots virtuales, precisamente los algoritmos que permiten el funcionamiento de los ordenadores que gobiernan determinadas actividades, y robots sociales, que serían aquellos a los que ya es necesario reconocer "una pequeña humanidad" ¿Es una pequeña humanidad como única posibilidad o el primer paso hacia una "humanidad" integral de las máquinas?<sup>20</sup> ¿Tendríamos el nacimiento del llamado "posthumano", como una nueva categoría de humanos nacidos con características tecnológicas, que precisamente los distinguen de los "humanos" anteriores?

Por su parte, Paolo Benanti se refiere a la histórica portada de la Revista Time, de 1983, que abordaba a la computadora como personalidad del año, con el título "La Máquina del Año", destacando la competencia entre seres humanos y máquinas.<sup>21</sup> Y, en este sentido, alerta sobre las "manipulaciones electrónicas" de los seres humanos, sobre todo, sobre la "capacidad de controlar los flujos de información dentro de nuestro sistema nervioso", en un fenómeno llamado "andamio", que "viste cuerpos hipermodernos, promoviendo un filtro entre nosotros y la realidad".<sup>22</sup> Respecto a la nanotecnología, Benanti se refiere expresamente a que las nuevas tecnologías buscan resultados complejos en el campo de la "conciencia" y las "emociones humanas", con "partículas elementales del cuerpo humano". Son Nanomáquinas, que interactúan con el sistema biológico, para modificar el proceso de información, alterando la realidad cognitiva.<sup>23</sup>

Además, Benanti se refiere a una característica única del homo sapiens, su "condición tecnohumana", que se revela en la forma

en que "los seres humanos comprenden y actúan en su existencia", una interacción mediada por instrumentos y artefactos tecnológicos.<sup>24</sup> Reconoce al ser humano como diferente de todos los animales, en que tiene la capacidad de salir de la "chiusura ambiente", es decir, de un ser que está siempre en proceso de formación, en el sentido de trascender la realidad establecida, de la propia condición biológica.<sup>25</sup> Una "eccedenza umana", generando un impacto en la relación humano-artefacto-mundo.<sup>26</sup>

Además, advierte que los algoritmos son "injustamente reduccionistas", ya que no observan el contexto, ejemplificando el hecho de que alguien no paga una factura porque está en el hospital, no porque sea un moroso persistente. Y afirma que "no podemos perder todos los matices secundarios, pero sí esenciales a nuestro ser".<sup>27</sup>

Así, se insiste en la necesidad de "tomarse en serio" algunas facetas de los riesgos que el amplio y profundo desarrollo de la IA podría acarrear al ser humano. Se trata de equilibrar riesgos y oportunidades.<sup>28</sup> Aquí vale la pena traer a colación a Stefano Rodotà, cuando menciona: "El ser humano, y su custodia, resultan así no ser una resistencia a lo nuevo, al temor al cambio, o una infravaloración de sus beneficios. Se presentan como conocimiento consciente de una transición que no se puede separar de los principios en los que el ser humano sigue reconociéndose, abriéndose no obstante a un mundo más amplio y en continua transformación. No es la compañía de unos pocos, ni de un balladé. El compromiso necesario requiere una transformación cultural, una amplia atención civil y una acción pública coherente. Hablar de una política de lo humano es, entonces, exactamente lo opuesto a las prácticas corrientes que quieren apropiarse de cada aspecto de lo vivo."<sup>29</sup>

Se podría hacer un breve comentario sobre esta perspectiva aportada por Rodotà: efectivamente se necesitará una acción pública coherente, que implique decisiones y opciones, ante las posibilidades que traen los avances de la IA. Sin embargo, y cada vez más, es necesario prestar atención a los movimientos generados por la acción privada, especialmente cuando se trata de la regulación de esta tecnología y de otras que conforman la

<sup>18</sup> MAKORTOFF, Kalyeena. "Los riesgos que plantea la IA son reales": la UE se moviliza para vencer a los algoritmos que arruinan vidas. *The Guardian*, domingo 7 de agosto de 2022. Disponible en: <https://www.theguardian.com/technology/2022/aug/07/ai-eu-moves-to-beat-the-algorithms-that-ruin-lives>. Consultado el 15 de marzo de 2024.

<sup>19</sup> TUNES, Suzel. Algoritmos parciales. *Revista Pesquisa FAPESP*, v. 287, p. 62-67, enero de 2020. Disponible en: <https://revistapesquisa.fapesp.br/algoritmos-parciais/>. Consultado el 15 marzo 2024.

<sup>20</sup> RODOTÀ, Stefano. Del ser humano al posthumano. FERNÁNDEZ DEL CASTILLO, Tomás de la quadra-Salcedo; PIÑAR MAÑAS, Jose Luis (Directores). *Sociedad digital y Derecho*. Madrid: Ministerio de Industria, Comercio y Turismo - RED. Es - Boletín Oficial del Estado, 2018, capítulo 2, p. 90.

<sup>21</sup> BENANTI, Paolo. Postumano, troppo postumano. Roma: Castelvecchi Editore, 2017, p. 7.

<sup>22</sup> BENANTI, Paolo. Postumano, troppo postumano. Roma: Castelvecchi Editore, 2017, p. 7.

<sup>23</sup> BENANTI, Paolo. Postumano, troppo postumano. Roma: Castelvecchi Editore, 2017, p. 7.

<sup>24</sup> BENANTI, Paolo. Human in the Loop. Decisioni Umane e Intelligenze Artificiali. Firenze: Mondadori Education, 2022.

<sup>25</sup> BENANTI, Paolo. Human in the Loop. Decisioni Umane e Intelligenze Artificiali. Firenze: Mondadori Education, 2022. "Cierre ambiental"

<sup>26</sup> BENANTI, Paolo. Human in the Loop. Decisioni Umane e Intelligenze Artificiali. Firenze: Mondadori Education, 2022. "Cierre ambiental"

<sup>27</sup> BENANTI, Paolo. Le macchine sapienti, Intelligenze Artificiali e decisioni umane. Bologna: Marietti, 2018, 41.

<sup>28</sup> BERTOLASO, Marta; MARCOS, Alfredo. Umanesimo tecnologico. Roma: Carocci Editore, 2023, p. 11.

<sup>29</sup> RODOTÀ, Stefano. Del ser humano al posthumano. FERNÁNDEZ DEL CASTILLO, Tomás de la quadra-Salcedo; PIÑAR MAÑAS, Jose Luis (Directores). *Sociedad digital y Derecho*. Madrid: Ministerio de Industria, Comercio y Turismo - RED. Es - Boletín Oficial del Estado, 2018, capítulo 2, p. 93.

llamada "Cuarta revolución industrial" <sup>30</sup>. ¿Cuál es la razón? Las transformaciones, o la metamorfosis del mundo<sup>31</sup>, según Ulrich Beck, también requieren acciones creativas y ampliadas para dar cuenta de las llamadas "lagunas normativas", que plantean algunas preguntas desafiantes: 1) "¿Quién debe determinar la nocividad de los productos y las tecnologías en el riesgo que entrañan, y sus dimensiones? ¿La responsabilidad incumbe a los que generan esos riesgos o a los que se benefician de ellos? ¿Se incluye o excluye a las personas afectadas o potencialmente afectadas por ellos?"; 2) "¿Qué debe considerarse prueba suficiente y -en un mundo en el que necesariamente tratamos con conocimientos impugnados o con conocimientos que no conocemos y que nunca tendremos en el sentido clásico- quién decide esto?" y 3) "Si existen peligros y daños, ¿quién debe decidir sobre la compensación de los afligidos y quién se ocupa de garantizar que las generaciones futuras se enfrenten a menos riesgos existenciales?"<sup>32</sup>

Todas estas preguntas aún no revelan concepciones suficientes para abordar una o varias respuestas. Por ello, el reto se lanza por su ecuación, teniendo en cuenta algunas categorías que aún son ajenas a la mayoría de la doctrina jurídica, como es el caso de trabajar con pruebas sobre los efectos e impactos que puede generar la IA. Aún no se dispone de un traje de IA perfecto y acabado. Por lo tanto, ¿el ámbito jurídico seguirá sin poder proponer una arquitectura reglamentaria?

La ciencia jurídica debe aprender a tratar y regular las "pruebas", guiándose por el "principio de cognoscibilidad", es decir, "[...] los límites de lo que podemos conocer con certeza mediante las ciencias naturales y de lo que aún no podemos saber son imprecisos, ya que mucho de lo que parece irrefutable en un momento dado aún puede sufrir una revisión posterior".<sup>33</sup>

Esta falta de certidumbre sobre los contornos del hecho tecnológico - en este caso, la IA- debería impregnar la ingeniería reguladora, que aún pretende operar sobre la certeza y la previsibilidad de lo que se conoce y, por tanto, de lo que se regula.

Las lagunas normativas, ya sea en la reglamentación existente o en las dificultades para elaborar nuevos marcos normativos, están relacionadas con las siguientes razones: la delimitación

muy limitada del contexto fáctico de aplicación o una exclusión cuestionable del ámbito de aplicación de un acto pertinente; la ausencia de normas sustantivas que regulen una cuestión específica que merezca atención normativa, lo que genera un espacio no previsto y no regulado debido a la redacción de las disposiciones legales; y un espacio normativo no cubierto relacionado con actos jurídicos interrelacionados, porque los avances que trae consigo la IA son inter y transdisciplinarios.<sup>34</sup>

La IA y otras tecnologías digitales emergentes comparten algunas características disruptivas que explican la necesidad de revisar los conceptos actuales y reconsiderar las normas vigentes. Cabe decir, que la perturbación también será percibida por el Derecho y sus metodologías reguladoras. Estos rasgos distintivos, de potencial disruptivo, son: autonomía, complejidad, opacidad, apertura a múltiples posibilidades de efectos positivos y negativos, muchos aún desconocidos, dependencia de los datos y vulnerabilidad.<sup>35</sup>

Aquí, Cabitza se refiere a dos neologismos, "algocrazia" y "aloretica", importantes a ser considerados en la relación entre Ética, Derecho e Inteligencia Artificial. La "algocrazia" como forma de "sociedad de la información", basada en "el predominio de los algoritmos". Se trata de un "nuevo sistema", que "se presenta como una alternativa a los sistemas tradicionales de burocracia y mercado", como la "división del trabajo" y busca generar "productividad, eficiencia y ganancias".<sup>36</sup> En este sentido, el algoritmo se convierte en "un símbolo de una voluntad sin nombre y sin nombre y de una capacidad difusa e incontrolable de controlar el comportamiento de los demás".<sup>37</sup> Es una metodología que apuesta por la racionalidad, con un enfoque utilitario y rentable.<sup>38</sup> Resulta que hay situaciones en la vida que "podemos considerar irreducibles a la conversión a algoritmos", Cabitza llama "Androritmo", en el sentido de su imposibilidad de "conversión algorítmica". Se trata del "conjunto de cualidades" imprescindibles para "comprender al ser humano", como lo imprevisto, la temeridad, la duda, la ambigüedad.<sup>39</sup> Así, en este contexto, se debe reconocer el carácter "andrítmico" de la vida humana, como la "aceptación de la pluralidad y la incertidumbre de la vida".<sup>40</sup>

<sup>30</sup> SCHWAB, Klaus. *La cuarta revolución industrial*. São Paulo: EDIPRO, 2016.

<sup>31</sup> BECK, Ulrich. *La metamorfosis del mundo: nuevos conceptos para una nueva realidad*. Traducción María Luiza X. de A. Borges; revisión técnica María Cláudia Coelho. Río de Janeiro: Zahar, 2018 (En formato Kindle).

<sup>32</sup> BECK, Ulrich. *La metamorfosis del mundo: nuevos conceptos para una nueva realidad*. Traducción María Luiza X. de A. Borges; revisión técnica María Cláudia Coelho. Río de Janeiro: Zahar, 2018 (En formato Kindle), Posición 1588.

<sup>33</sup> GABRIEL, Markus. *El significado del pensamiento: la filosofía desafía a la inteligencia artificial*. Traducción de Lucas Machado. Petrópolis, RJ: Vozes, 2021, p. 179.

<sup>34</sup> Adaptado de: CODAGNONE, Cristiano; LIVA, Giovanni; RODRIGUEZ DE LAS HERAS BALLELL, Teresa. *Identificación y evaluación de la legislación comunitaria existente y en proyecto en el ámbito digital*: Estudio para el comité especial sobre Inteligencia Artificial en la Era Digital (AIDA), Departamento de Políticas Económicas, Científicas y de Calidad de Vida, Parlamento Europeo, Luxemburgo, 2022. Disponible en: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL\\_S\\_TU\(2022\)703345\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_S_TU(2022)703345_EN.pdf). Consultado el 15 marzo 2024.

<sup>35</sup> DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN, Responsabilidad por las tecnologías digitales emergentes - Acompañamiento del documento Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al

Comité de las Regiones, Inteligencia artificial para Europa, SWD(2018) 137 final. Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, Informe sobre las implicaciones de la inteligencia artificial, el Internet de los objetos y la robótica para la seguridad y la responsabilidad, COM(2020) 64 final, Bruselas, 19.2.2020. Informe sobre la responsabilidad por la inteligencia artificial y otras tecnologías emergentes. Disponible en: <https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en>. Consultado el 15 marzo 2024.

<sup>36</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>37</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>38</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>39</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>40</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021, p. 73.

A su vez, la “algorética” se dedica a “inscribir valores éticos en las máquinas”, “y a diseñar algoritmos que sean capaces de producir valoraciones éticas, ante situaciones siempre nuevas e impredecibles”.<sup>41</sup> No se trata sólo de aplicar cuestiones éticas sólo en el diseño del algoritmo, sino de aplicarlas “en las distintas fases del ciclo de vida de los productos y sistemas”, tanto “en el análisis, el diseño y la validación”. Cabitza ejemplifica, por ejemplo, en la recopilación de datos, observando los riesgos del no respeto a las minorías, la discriminación étnica, así como en lo que respecta a las funciones de vigilancia y síntesis de contenidos.<sup>42</sup> En términos prácticos, el diseñador debe elegir “la acción más prudente”, prestando atención al “principio de responsabilidad” y al “enfoque de precaución”.<sup>43</sup>

Así, las características disruptivas generan las “lagunas reguladoras”, potenciadas por el “principio de cognoscibilidad” y señalan la incapacidad estructural de los modelos reguladores tradicionales. Para hacer frente a estos retos en el ámbito de la regulación, se abren las siguientes posibilidades: la formulación de las estructuras del llamado “constitucionalismo digital”, anclado en principios ya reconocidos en varios países, guiado a través de la pauta ética que proporcionan los derechos humanos y con la práctica de un constante y continuo ensayo regulador de las estructuras normativas creadas en “laboratorios reales”.

El constitucionalismo digital puede considerarse como una doctrina que deriva de la necesaria redimensión del constitucionalismo tradicional -centrado en el panorama interno de cada país- donde la Constitución es la ley suprema y que salvaguarda los derechos fundamentales. Sin embargo, en la medida en que los límites geográficos de cada país son más porosos para la movilización de personas, bienes y servicios, como consecuencia de la globalización y de la digitalización de todo, esa perspectiva del constitucionalismo ya no resulta suficiente, puesto que los “derechos fundamentales” están vinculados a una noción interna del Derecho.

El constitucionalismo digital es una nueva vertiente del constitucionalismo contemporáneo, que representa una nueva etapa en la evolución del constitucionalismo, que marca un cambio revolucionario e implica la transición hacia nuevos valores y la valorización de principios vinculados a la protección nacional e internacional de los derechos humanos en la era digital. En esta expresión, “digital” no califica directamente el término “constitucionalismo”, sino que es un adverbio que transmite la idea de que uno se está refiriendo al

constitucionalismo relacionado con un entorno digital. “El constitucionalismo digital, en consecuencia, comparte los valores fundamentales y los objetivos generales del constitucionalismo contemporáneo, pero se centra en el contexto específico afectado por el advenimiento de la tecnología digital. [...] Por lo tanto, se puede definir como la ideología que pretende establecer y garantizar la existencia de un marco normativo para la protección de los derechos fundamentales y el equilibrio de poderes en el entorno digital.”<sup>44</sup>

Otra característica de esta nueva vertiente del constitucionalismo es la presencia de actores normativos privados - como las empresas que operan con IA y otras organizaciones - junto a los actores públicos tradicionales. Esta peculiaridad del entorno digital exige desvincular el concepto de constitucionalismo de la dimensión estatal para poder apreciar plenamente la emergencia de los poderes de los actores privados. Esta interpretación es el resultado de un proceso de generalización y posterior redefinición del concepto de constitucionalismo en relación con el entorno digital.<sup>45</sup>

Este entorno se caracteriza por el reparto del proceso de creación normativa entre actores privados y públicos, con prevalencia de las acciones de los primeros - con modelos de autorregulación, estructurados por principios globalmente aceptados y vinculados a la IA- y bajo el control cualitativo de los segundos, principalmente garantizando la incorporación de los derechos humanos. De este modo, nacen estructuras de “autorregulación regulada”, guiadas por los elementos estructuradores de la innovación responsable y la integración de salvaguardas y medidas para mitigar los riesgos que podría generar la IA.<sup>46</sup>

Otra “novedad” que entra en este “entorno regulador” es la modelización de espacios de prueba, del tipo “Regulatory Sandbox” y/o “Regulatory Living Lab”, que son laboratorios reales, generalmente estructurados en parques tecnológicos u otros espacios reales de uso de sistemas de IA, donde se practican los modelos de autorregulación regulada, se observan los resultados y se realizan ajustes en los modelos probados, si es necesario.

¿Qué concepción de los Derechos Humanos utiliza en estos modelos de regulación? Adoptamos la perspectiva de John Gerard Ruggie, que diseñó el marco estructurado en tres pilares: proteger, respetar y remediar<sup>47</sup>, sentando las bases del actual escenario plural y en constante cambio, que desafía la producción legislativa tradicional. Estos principios rectores se

<sup>41</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021, p. 59-60. En este particular, el Papa Francisco utilizó el término al hablar de nuevas tecnologías. Disponible en <https://www.vaticannews.va/pt/igreja/news/2020-11/por-uma-algor-etica.html>, consultado en marzo de 2024.

<sup>42</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

<sup>43</sup> FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021, p. 73.

<sup>44</sup> CELESTE, Edoardo. Constitucionalismo digital: una nueva teorización sistemática. *International Review of Law, Computers & Technology*, v. 33, n. 1, 2019, p. 86-87, <https://doi.org/10.1080/13600869.2019.1562604>.

<sup>45</sup> TEUBNER, Gunther. Constitucionalismo societal; ¿alternativas a la teoría constitucional centrada en el Estado? En JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther (Edit.). *Gobernanza transnacional y constitucionalismo*. Estudios Internacionales de Teoría del Derecho Privado. Oxford: Hart, 2004, p. 3-28.

<sup>46</sup> Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas para la Inteligencia Artificial (Reglamento sobre Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021 COM(2021) 206 final. 2021/0106 (COD). Disponible en: [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF). Consultado el 04.01.2023, números de documento 71 y 72.

<sup>47</sup> RUGGIE, John Gerard *Cuando los negocios no son sólo negocios*: las empresas multinacionales y los derechos humanos. Traducción de Isabel Murray. São Paulo: Planeta Sostenible, 2014. Documento disponible para Kindle.

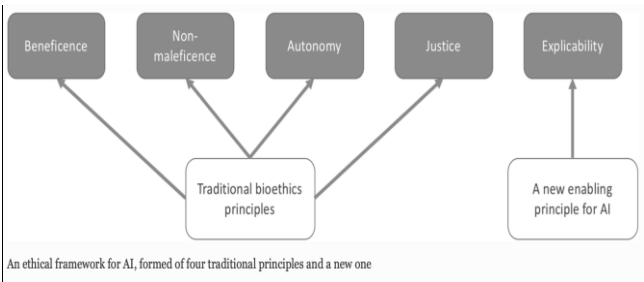
basan en el reconocimiento de que: a) Los Estados tienen la obligación de respetar, proteger y hacer efectivos los derechos humanos y las libertades fundamentales. Además de este actor, también se pone en escena [...] (b) el papel de las empresas como organizaciones especializadas de la sociedad, que desempeñan determinadas funciones necesarias para cumplir todas las normas jurídicas aplicables y respetar los derechos humanos. De ahí surge (c) la necesidad de que los derechos y las obligaciones vayan acompañados de remedios apropiados y eficaces (rayanos en las "sanciones") cuando se violan.<sup>48</sup>

La incorporación de estos tres pilares <sup>49</sup> dará legitimidad a las arquitecturas de autorregulación que las organizaciones lleguen a estructurar. Hay otro detalle muy importante, que se acerca a una característica "cuasi" estatal de los instrumentos normativos que se crearán: "estos principios rectores se aplican a todos los Estados y a todas las empresas, transnacionales o no, independientemente de su tamaño, sector, ubicación, propiedad y estructura".<sup>50</sup>

Así, los derechos humanos -entendidos aquí como el respeto a la vida humana sana (sin descuidar ninguna forma de vida) y la protección del medio ambiente- se proyectan sobre estos tres pilares de Ruggie, que aseguran por tanto el "carácter regulado" de la autorregulación. Estos elementos del marco de Ruggie dialogan estructuralmente con los principios vinculados a la construcción de la llamada Inteligencia Artificial Responsable y se insertan orgánicamente en la composición del "constitucionalismo digital".

La organización de los principios toma como inspiración el trabajo desarrollado por Luciano Floridi y sus colegas, basado en los principios de la Bioética, como se muestra en la siguiente figura:

Figura 1: Principios fundamentales de la estructuración del marco



<sup>48</sup> RUGGIE, John Gerard Consejo de Derechos Humanos Decimoséptimo periodo de sesiones; Tema 3 del programa: Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo. *Informe del Representante Especial del Secretario General sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas comerciales*. Este documento está fechado el 21 de marzo de 2011. Disponible en: <https://www.right-docs.org/doc/a-hrc-17-31/>. Consultado el 15 marzo 2024.

<sup>49</sup> Según PARKER, Christine y HOWE, John. "El proyecto diplomático de Ruggie y su falta de infraestructura reglamentaria". MARES, Radu (Edit.). *The UN guiding principles on business and human rights: foundations and implementation*, Martinus Nijhoff Publishers, Boston, 2012, p. 273-301, se podría añadir un cuarto pilar, "representado por la obligación cívica de la sociedad civil de participar, ayudando a legitimar y movilizar la implicación de los actores de la sociedad civil, en funciones como el seguimiento y la evaluación del proceso" (p. 290-1).

<sup>50</sup> RUGGIE, John Gerard Consejo de Derechos Humanos Decimoséptimo periodo de sesiones; Tema 3 del programa: Promoción y protección de todos

Fuente: <sup>51</sup>

La primera etapa del marco se basa en los principios presentados anteriormente, tratando de garantizar los siguientes fundamentos: "Qué se puede hacer: mejorar el rendimiento humano, sin eliminar la responsabilidad humana"; "Qué se puede conseguir: aumentar las capacidades sociales, sin reducir el control humano"; "Cómo se puede interactuar: cultivar la cohesión social, sin erosionar la autodeterminación humana". Se puede observar que estos tres ejes estructuradores pretenden asegurar la centralidad del ser humano en la toma de decisiones sobre los avances con la IA, asumiendo la consiguiente responsabilidad. La IA es una creación humana y debe permanecer bajo control humano. A partir de los ejes presentados, cada uno de los principales principios estructurantes del marco comienzan a operar desde el siguiente contexto significativo: (a) beneficencia: busca promover el bienestar, preservar la dignidad humana y sostener el planeta; (b) no maleficencia: vinculada a la privacidad, la seguridad y el pleno ejercicio del "cuidado" en la preservación de la humanidad del ser humano; (c) autonomía: preservar y garantizar el pleno ejercicio del poder de decisión sobre los avances de la IA y la mitigación de sus impactos negativos; (d) justicia: orientada a promover la prosperidad y preservar la solidaridad. A estos principios se añade el principio de explicabilidad, que posibilita los demás principios a través de la inteligibilidad y la responsabilidad. <sup>52</sup> En esta línea, los sistemas de IA deben ser transparentes, verificables, con decisiones bajo "supervisión humana" y "orientadas al bien común". Así, las normas deben inspirarse en principios jurídicos y éticos, en consonancia con el humanismo tecnológico.<sup>53</sup>

Tomando estos principios rectores principales y utilizando los diversos principios publicados en varias fuentes <sup>54</sup>, se puede hacer la siguiente organización de principios instrumentales:

| Autonomía                 | No maleficencia                | Caridad                       | Justicia               |
|---------------------------|--------------------------------|-------------------------------|------------------------|
| Poder de decisión         | Control de riesgos             | Promoción del bienestar       | Equidad                |
| Control humano            | Seguridad                      | Beneficiar a la sociedad      | Derechos fundamentales |
| Transparencia             | Atención y cuidado             | Generar beneficios asequibles | No discriminación      |
| Apertura a la comprensión | Protección de datos personales | Sostenibilidad                | Evitar los prejuicios  |

los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo. *Informe del Representante Especial del Secretario General sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas comerciales*. Este documento está fechado el 21 de marzo de 2011. Disponible en: <https://www.right-docs.org/doc/a-hrc-17-31/>. Consultado el 15 marzo 2024.

<sup>51</sup> FLORIDI, Luciano; COWLS, Josh; BELTRAMETTI, Monica *et al.* AI4People - un marco ético para una buena sociedad de la IA: oportunidades, riesgos, principios y recomendaciones. *Minds and Machines*, v. 28, p. 689-707, 2018. <https://doi.org/10.1007/s11023-018-9482-5>

<sup>52</sup> Ibid.

<sup>53</sup> BERTOLASO, Marta; MARCOS, Alfredo. *Umanesimo tecnologico*. Roma: Carocci Editore, 2023, p. 11.

<sup>54</sup> CANCA, Cansu. Operacionalización de los principios éticos de la IA. *Communications of the ACM*, v. 63, n. 12, 2020. Disponible en: <https://aiethicslab.com/operationalizing-ai-principles/>. Consultado el 15.03.2024; AI Ethics Lab. Disponible en: <https://aiethicslab.com/the-box/>.

|                            |                                     |                                     |                                |
|----------------------------|-------------------------------------|-------------------------------------|--------------------------------|
| Explicabilidad             | Privacidad                          | Excelencia científica               | Inclusión                      |
| Libertad                   | Explicabilidad                      | Diseño centrado en el usuario       | Diversidad                     |
| Derechos fundamentales     | Reproductividad                     | Un enfoque centrado en las personas | Accesibilidad                  |
| Protección de la intimidad | Precisión                           | Explicabilidad                      | Apertura para auditoría        |
| Valores humanos            | Fiabilidad                          |                                     | Gobernanza transparente        |
|                            |                                     |                                     | Explicabilidad                 |
|                            | Aplicación responsable              |                                     | Regulación y cumplimiento      |
|                            | Prevenir una carrera armamentística |                                     | Preservación de la solidaridad |

Los principios básicos que dan cabida a los principios instrumentales integran el marco normativo y señalan el respeto de los derechos humanos, materializados en la triada presentada por John Gerard Ruggie: proteger, respetar y remediar. Con estos principios, hemos diversificado los materiales para hacer posible la eficacia de una inteligencia artificial responsable. Según Bertolaso y Marcos: “Si la IA pudiera contribuir a la profundización de un principio de humanidad que nos ayudaría a comprender mejor las potencialidades incluidas en la naturaleza humana, como la dignidad y la libertad.”<sup>55</sup> Estos aspectos forman parte integrante del "constitucionalismo digital" y permiten una relectura del constitucionalismo nacional tradicional, además de proporcionar una base para la protección del ser humano en el espacio internacional y globalizado. Cabe destacar que el "constitucionalismo digital" es un medio para renovar y reforzar el constitucionalismo nacional, alineándolo con los nuevos retos que plantea la creciente digitalización de la vida. No es necesario movilizar todos los principios instrumentales a la vez, sino que se dejan aperturas creativas para su combinación, en función del tipo de organización a la que deba servir el modelo y siempre con pruebas en entornos de Sandbox normativo o Living Lab.

I. REFERENCIAS BIBLIOGRÁFICAS

Inventario mundial de directrices éticas de la IA, abril de 2020. Disponible en: <https://inventory.algorithmwatch.org/about>. Consultado el 15 de marzo de 2024.

Laboratorio de Ética de la IA. Disponible en: <https://aiethicslab.com/the-box/>. Consultado el 15 marzo 2024.

BECK, Ulrich. La metamorfosis del mundo: nuevos conceptos para una nueva realidad. Traducción Maria Luiza X. de A. Borges; revisión técnica Maria Cláudia Coelho. Río de Janeiro: Zahar, 2018 (En formato Kindle).

Consultado el 15.03.2024; ZHANG, Daniel; MASLEJ, Nestor; BRYNJOLFSSON, Erik *et al.* *The AI Index 2022 Annual Report*, AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, marzo de 2022. Disponible en: [https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report\\_Master.pdf](https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf). Consultado el 15.03.2024; FJELD, Jessica; ACHTEN, Nele; HILLIGOSS, Hannah *et al.* *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*. Serie de publicaciones del Berkman

BENANTI, Paolo. *Postumano, troppo postumano*. Roma: Castelvecchi Editore, 2017.

BENANTI, Paolo. *Human in the Loop. Decisioni Umane e Intelligenze Artificiali*. Firenze: Mondadori Education, 2022.

BENANTI, Paolo. *Le macchine sapienti, Intelligenze Artificiali e decisioni umane*. Bologna: Marietti, 2018.

BERTOLASO, Marta; MARCOS, Alfredo. *Umanesimo tecnologico*. Roma: Carocci Editore, 2023.

CANCA, Cansu. Operacionalización de los principios éticos de la IA. *Communications of the ACM*, v. 63, n. 12, 2020. Disponible en: <https://aiethicslab.com/operationalizing-ai-principles/>. Consultado el 15 de marzo de 2024.

CELESTE, Edoardo. Constitucionalismo digital: una nueva teorización sistemática. *International Review of Law, Computers & Technology*, v. 33, n. 1, 2019, p. 76-99 <https://doi.org/10.1080/13600869.2019.1562604>.

CODAGNONE, Cristiano; LIVA, Giovanni; RODRIGUEZ DE LAS HERAS BALLELL, Teresa. Identificación y evaluación de la legislación comunitaria existente y en proyecto en el ámbito digital: Estudio para el comité especial sobre Inteligencia Artificial en la Era Digital (AIDA), Departamento de Políticas Económicas, Científicas y de Calidad de Vida, Parlamento Europeo, Luxemburgo, 2022. Disponible en: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL\\_STU\(2022\)703345\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_STU(2022)703345_EN.pdf). Consultado el 15 de marzo de 2024.

DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN, Responsabilidad por las tecnologías digitales emergentes - Acompañamiento del documento Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Inteligencia artificial para Europa, SWD(2018) 137 final. Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, Informe sobre las implicaciones de la inteligencia artificial, el Internet de los objetos y la robótica para la seguridad y la responsabilidad, COM(2020) 64 final, Bruselas, 19.2.2020. Informe sobre la responsabilidad por la inteligencia artificial y otras tecnologías emergentes. Disponible en: <https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en>. Consultado el 15 marzo 2024.

FJELD, Jessica; ACHTEN, Nele; HILLIGOSS, Hannah *et al.* *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*. Serie de publicaciones del Berkman Klein Center for Internet & Society Research. Publicación de investigación n. 2020-1, 15 de enero de 2020. Disponible en: <https://cyber.harvard.edu/publication/2020/principled-ai>. Consultado el 15.03.2024; Inventario mundial de directrices éticas de la IA, abril de 2020. Disponible en: <https://inventory.algorithmwatch.org/about>. Consultado el 05 de marzo de 2024.

<sup>55</sup> BERTOLASO, Marta; MARCOS, Alfredo. *Umanesimo tecnologico*. Roma: Carocci Editore, 2023, p. 11.

<https://cyber.harvard.edu/publication/2020/principled-ai>. Consultado el 15 de marzo de 2024.

FLORIDI, Luciano; COWLS, Josh; BELTRAMETTI, Monica et al. AI4People - un marco ético para una buena sociedad de la IA: oportunidades, riesgos, principios y recomendaciones. *Minds and Machines*, v. 28, p. 689-707, 2018. <https://doi.org/10.1007/s11023-018-9482-5>.

FLORIDI, Luciano. La legislación europea sobre IA: breve análisis de su enfoque filosófico. En J. Mökander; M. Ziosi (eds.). *El Anuario 2021 del laboratorio de ética digital*, Digital Ethics Lab Yearbook. Suiza AG: Springer Nature, 2022.

FLORIDI, Luciano; CABITZA, Federico. *Intelligenza Artificiale: L'uso delle nuove macchine*. Firenze: Giunti Editore, 2021.

GABRIEL, Markus. El significado del pensamiento: la filosofía desafía a la inteligencia artificial. Traducción de Lucas Machado. Petrópolis, RJ: Vozes, 2021.

GOLDENBERG, Rina Alemania: El software de vigilancia policial, un quebradero de cabeza legal - TBEN - 12/22/2022. *The Bharat Express News*, 22 de diciembre de 2022. Disponible en: <https://www.thebharatexpressnews.com/germany-police-surveillance-software-a-legal-headache-tben-12-22-2022/>. Consultado el 15 marzo 2024.

KAPLAN, Andreas; HAENLEIN, Michael. Siri, Siri, en mi mano: ¿Quién es la más bella del país? Sobre las interpretaciones, ilustraciones e implicaciones de la inteligencia artificial. *Business Horizons*, v. 62, p. 15-25, 2019.

KÖNIG, Pascal D.; KRAFFT, Tobias D.; SCHULZ, Wolfgang; ZWEIG, Katharina A. Esencia de la IA: ¿Qué es la IA? En L. DiMatteo, C. Poncibò y M. Cannarsa (Eds.). *The Cambridge Handbook of Artificial Intelligence: Global perspectives on Law and Ethics*. Cambridge Law Handbooks, pp. 18-34. Cambridge: Cambridge University Press. Doi: 10.1017/9781009072168.005.

MAKORTOFF, Kalyeena. "Los riesgos que plantea la IA son reales": la UE se moviliza para vencer a los algoritmos que arruinan vidas. *The Guardian*, domingo 7 de agosto de 2022. Disponible en: <https://www.theguardian.com/technology/2022/aug/07/ai-eu-moves-to-beat-the-algorithms-that-ruin-lives>. Consultado el 15 de marzo de 2024.

PARKER, Christine; HOWE, John. El proyecto diplomático de Ruggie y su falta de infraestructura reglamentaria. MARES, Radu (Edit.). *Los principios rectores de la ONU sobre empresas y derechos humanos: fundaciones y aplicación*. Boston: Martinus Nijhoff Publishers, 2012.

PREPARÁNDOSE para el futuro de la Inteligencia Artificial. Oficina Ejecutiva del Presidente Consejo Nacional de Ciencia y Tecnología Comité de Tecnología, octubre de 2016. Disponible en: <https://obamawhitehouse.archives.gov/sites/default/files/white>

[house\\_files/microsites/ostp/NSTC/preparing\\_for\\_the\\_future\\_of\\_ai.pdf](house_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf). Consultado el 15 de marzo de 2024.

PROPUESTA de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas para la Inteligencia Artificial (Reglamento sobre Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21.4.2021 COM(2021) 206 final. 2021/0106 (COD). Disponible en: [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF). Consultado el 15 de marzo de 2024.

RODOTÀ, Stefano. Del ser humano al posthumano. FERNÁNDEZ DEL CASTILLO, Tomás de la quadra-Salcedo; PIÑAR MAÑAS, Jose Luis (Directores). *Sociedad digital y Derecho*. Madrid: Ministerio de Industria, Comercio y Turismo - RED. Es - Boletín Oficial del Estado, 2018, Capítulo 2, p. 87-93.

RODOTÀ, Stefano. *Il mondo nella rete: quali i diritti, quali i vincoli*. Bari, Roma: Editori Laterza, 2014.

RUGGIE, John Gerard Consejo de Derechos Humanos Decimoséptimo periodo de sesiones; Tema 3 del programa: Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo. Informe del Representante Especial del Secretario General sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas comerciales. Este documento está fechado el 21 de marzo de 2011. Disponible en: <https://www.right-docs.org/doc/a-hrc-17-31/>. Consultado el 15 marzo 2024.

RUGGIE, John Gerard Cuando los negocios no son sólo negocios: las empresas multinacionales y los derechos humanos. Traducción de Isabel Murray. São Paulo: Planeta Sostenible, 2014. Documento disponible para Kindle.

SCHWAB, Klaus. *La cuarta revolución industrial*. São Paulo: EDIPRO, 2016.

SILVA, Mario Tavares da. Vigilancia policial predictiva y derechos fundamentales. 30 de diciembre de 2022. Disponible en: <https://expresso.pt/opiniaao/2022-12-30-Policiaamento-preditivo-e-direitos-fundamentais-46fce25a>. Consultado el 15 marzo 2024.

TUNES, Suzel. Algoritmos parciales. *Revista Pesquisa FAPESP*, v. 287, p. 62-67, enero de 2020. Disponible en: <https://revistapesquisa.fapesp.br/algoritmos-parciais/>. Consultado el 15 marzo 2024.

ZHANG, Daniel; MASLEJ, Nestor; BRYNJOLFSSON, Erik et al. *The AI Index 2022 Annual Report*, AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, marzo de 2022. Disponible en: [https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report\\_Master.pdf](https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf). Consultado el 15 de marzo de 2024.

# DESAFÍOS DEL DERECHO EDUCATIVO EN LA POSMODERNIDAD

## CHALLENGES OF EDUCATIONAL LAW IN POSTMODERNISM

Patricia Casana de Burga

**Abstract--** It is argued that educational law, as a specialized legal discipline, faces a challenge that it shares with law as a whole: to recover the brightness and vitality, clouded by its divorce with reality and the voices that accuse it of being an obstacle to social change.

The necessary understanding of the postmodern students is highlighted, in a liquid context, by the solid generations, who are the great decision makers on issues that concern them. It is also recognized that traditional approaches have failed and that innovation is truncated by a mismatch between what the legal system seeks in terms of educational quality and what it actually obtains.

Finally, some challenges of educational law and its operators are outlined. Both the legal discipline and the old-fashioned lawyers have to go through a process of liquefaction consistent with the mindset of university students, under threat of being considered part of the problem that leads to increasing student desertion and, what is worse, of the threat regarding the end of the university.

**Index terms -** educational law, postmodernism, university, digital era.

### I. INTRODUCCIÓN

El derecho es un sistema dogmático, poco flexible, de cambio lento y no muy cercano a la realidad. Esas características eran no solo normales, sino hasta deseables en la modernidad, cuando era considerado un catalizador del orden y el progreso y el estabilizador por excelencia de los valores sociales. Así, soportaba con éxito las voces que le atribuían ser un obstáculo para el cambio. El paradigma posmoderno, sin embargo, plantea un gran reto para el derecho, disciplina que ya no ostenta el brillo y la vitalidad de sus momentos cumbre. La educación, en su doble dimensión de derecho fundamental y servicio público esencial, es, por así decirlo, un *boom*. Se le reconoce una naturaleza esencial para el desarrollo social y, en consecuencia, se le asignan los más altos presupuestos públicos, a la par que se hiperregula el servicio educativo. En ese contexto, de un derecho “sólido” con normativa exuberante, la universidad se encuentra con estudiantes posmodernos,

“líquidos” en terminología de Bauman, cuyas necesidades y expectativas debe atender de manera flexible e innovadora: son personas con una distinta valoración del tiempo y del espacio, buscan más que un empleo un propósito, están más interesadas en las experiencias que en la realidad o en la razón, no son desestructuradas sino que tienen estructuras autoconstruidas, son diversas y fluidas.

Uno de los retos del derecho educativo, como disciplina jurídica especializada, es proporcionar el marco teórico y conceptual para la construcción y reconstrucción normativa continua, de modo que las políticas públicas y el marco legal promuevan —no obstaculicen— que las universidades estén en aptitud de dar una oportuna respuesta a las necesidades y demandas de los estudiantes posmodernos.

Los enfoques tradicionales vienen fallando y, en términos generales, las generaciones más jóvenes ya no soportan la educación actual, mayoritariamente de tipo industrial y anclada en el siglo XX. Es necesario volver a despertar el amor por el aprendizaje en personas nuevas, que no desean ingresar a sistemas caducos; en caso contrario, harán *zapping* para evitar la educación superior universitaria, favoreciendo rutas de aprendizaje alternativas en plena ebullición.

La universidad atraviesa más que una crisis de adaptación una de identidad. Ello no es de extrañar si se considera que el siglo XXI trajo la avalancha que prometía y, con el rostro del COVID-19, nos puso enfrente lo que parece ser no una época de cambios sino un verdadero cambio de época. De pronto ya no basta con introducir mejoras en las antiguas estructuras, pues se cuestiona al sistema educativo y a la universidad de raíz y no en aspectos puntuales.

Según la Real Academia Española, una era es un “Extenso período histórico caracterizado por una gran innovación en las formas de vida y de cultura”. La revolución digital marcó un hito que impulsó un cambio cultural profundo y vertiginoso. Nos vemos sumergidos en una explosión de información, difícil de masticar y fácil de engullir, y eso nos obliga a reconfigurarnos.

La era digital aparece un sinfín de oportunidades para el desarrollo humano, pero también una legión de riesgos. En



cuanto a las oportunidades, amplía el acceso a la educación y brinda recursos para el aprendizaje. En cuanto a los riesgos, al exceso de información se unen su baja calidad y la incertidumbre acerca de su veracidad. Distinguir lo *fake* es un arte que pocos dominan y el autoengaño florece en el “régimen de la información” al que alude Han (2022), en el contexto de la digitalización.

En ese maremágnum, a falta de vacuna, se acude al reclamado *pensamiento crítico* como antídoto contra el consumo indiscriminado, superficial y cosmético de bits y memes. Así, se vuelve los ojos hacia el sistema educativo como formador de *personas íntegras y pensantes* capaces de discriminar entre lo real y lo virtual, lo principal y lo accesorio, lo efímero y lo permanente, la forma y el fondo.

La universidad es la arena en la que se forma y reforma la cosmovisión de los profesionales, quienes —antes que los *influencers*— son los llamados a liderar el desarrollo humano sostenible. Esos profesionales de nuevo cuño no se pueden formar en una universidad-torre-de-marfil, sino en casas de estudio que, lejos de aferrarse al *statu quo* y desdeñar los vertiginosos avances tecnológicos, recupere el rol protagónico que, como actor social, viene perdiendo.

Los decisores en temas educativos, no pocos con pensamiento analógico, proclamaron en su momento que el estudiante es el centro de la educación e incidieron en la calidad educativa y sus atributos. Hoy se preguntan, desconcertados, ¿de qué estudiantes hablamos?, ¿qué se entiende por educación de calidad?

Algunos, con una mirada adultocéntrica, no dudan en referirse a una denominada “generación de cristal”, con estudiantes sobreprotegidos y débiles, sin los méritos suficientes para cursar estudios superiores porque no estarían dispuestos a esforzarse hoy por un futuro mejor mañana. Otros, con mayor criterio, analizan qué hay detrás —o, aún mejor, adentro— de personas que se enfocan en vivir el hoy como un conjunto de momentos-fragmentos, en comprender sus emociones, en valorar lo efímero y lo intangible y en buscar experiencias compatibles con sus propósitos.

Como se desprende de lo que señala Duarte Quapper (2015, p. 20), en el imaginario social ser joven se ve como algo no solo transitorio, sino problemático, pues se asocia con ser inmaduro y desobediente. El control adulto se justifica por ese estatus juvenil, que lleva implícito un proceso de maduración. El objetivo es que el joven llegue a ser lo que el orden social establecido reclama. Agregamos nosotros que ese orden social, justamente, es el que está fuertemente en entredicho.

Ahora bien, la edad normativa para seguir estudios universitarios de pregrado es, en el Perú, entre los 17 y los 23 años. La Superintendencia Nacional de Educación Superior Universitaria reporta que en el año 2020 solo el 28,5 % de los jóvenes entre 16 y 20 años, edad de acceso temprano, estudiaba en la universidad. Asimismo, que los estudiantes de 25 o más años, representaron en el mismo año un cuarto de la matrícula en pregrado a nivel nacional (Sunedu, 2021, p. 74). En lo que concierne a los docentes universitarios peruanos, al 2020, el 35,6 % tiene entre 50-64 años y el 14,1 % 65 años a más. Solo el 9,1 % corresponde a profesores menores de 34 años. (Sunedu, 2021, p. 113).

En relación con lo anterior, más que un posible desencuentro entre “los jóvenes” y “los viejos”, en la era digital se podría

advertir una colisión entre “los jóvenes digitales” y los “viejos analógicos”.

La adultez, como estado de desarrollo pleno y definitivo, se redefine. Sawyer et. al. (2018), propugnan que si antes la adolescencia terminaba a los 19 años, hoy en día se extiende hasta los 24. Para ello, toma en cuenta los cambios en los roles sociales. Lo cierto es que existe la categoría de “adulcentes” (adultos adolescentes) que crean su propio espacio, con nuevos hitos vitales a otro ritmo, abrazan el aprendizaje a lo largo de toda la vida y el autodidactismo.

Respecto a la calidad educativa, muchos la vinculan con alcanzar determinado puesto en algún *ranking*, algunos de escasa fiabilidad, o con la empleabilidad de los egresados, mientras otros —con mayor amplitud— la asocian con formar y reformar los cimientos para una vida plena que se metamorfosea continuamente.

Sea cual fuere el enfoque, el derecho educativo es requerido para cristalizar los valores y proporcionar los principios y reglas que han de regir en el sistema universitario, tanto si estos se mantienen anclados en el pasado como si responden a las demandas de nuevo cuño. Es momento de elegir.

Esta ponencia busca plantear algunas reflexiones sobre los desafíos que enfrentan el derecho educativo y, más que eso, sus operadores, quienes le dan vida a través de las políticas públicas, la legislación, la hermenéutica, la jurisprudencia y, en general, todas las manifestaciones del derecho. Esos operadores —abogados, jueces, fiscales, legisladores, autoridades universitarias, etcétera— nacidos y criados en un mundo “sólido”, hoy advierten lo borroso de los antiguos márgenes, la desaparición de varias fronteras conceptuales, la fusión de lo real y lo virtual, y la comunión entre lo natural y lo artificial.

El propósito es contribuir con una línea de discusión para vivificar el derecho educativo, de modo que en nuestro tránsito de salida generacional podamos coexistir de manera pacífica y fructífera con quienes ya están con un pie en el metaverso o, por qué no, en el multiverso.

## II. EL DERECHO ¿OBSTÁCULO O INSTRUMENTO PARA EL CAMBIO SOCIAL?

El derecho, como sistema normativo y conjunto de conocimientos vinculados a fenómenos jurídicos, tiene como cimiento una amalgama de principios apriorísticos, axiomas, máximas, brocardos, aforismos y adagios. Así, por ejemplo, los abogados acuden al *dura lex, sed lex* para dar por zanjado que una norma se debe cumplir sin dudas ni murmuraciones, mientras que desde la otra orilla escuchan un antes trémulo, pero hoy fortalecido, *lex injusta non est lex*, esgrimido en una suerte de resucitación del derecho natural. Las elaboraciones jurídicas teóricas se califican no pocas veces como desfasadas o de otra época. Incluso, se acusa al derecho de ser “un pesado lastre que frena el progreso social” (Novoa Monreal, 2007, p. 13).

Adornado el repertorio lingüístico por enunciados en latín, particularmente por los remanentes de la vieja escuela que los valoran con retrospección idílica, el ampuloso lenguaje jurídico —del cual quizás sea ejemplo este texto— constituye una primera barrera para la comunión entre el derecho y la realidad. Además, cuando aún es incipiente el resultado de las políticas

de simplificación del lenguaje jurídico adoptadas en diversos países<sup>1</sup>, irrumpe la terminología propia del *Legaltech* y del *Lawtech*. Hoy en día hay cosas nuevas, identidades por descubrir y necesidades por visibilizar, que requieren ser nombradas para que cobren existencia legal.

Lo cierto es que en la transformación del derecho —y, consecuentemente, de la abogacía— impulsada por la transformación digital, interesa menos la utilización de herramientas tecnológicas que la construcción de un sistema jurídico transparente, claro y flexible para todos —no solo para quienes integran el cenáculo de juristas— que permita una nueva y continua categorización de los múltiples hechos sociales “disruptores” que acaecen y seguirán acaeciendo, cada vez con mayor frecuencia y velocidad.

El descontento frente al derecho se liga con la secularmente proclamada amenaza del fin de los abogados. Susskind (2008) advirtió que los profesionales del derecho que no evolucionen serán sustituidos por sistemas inteligentes, por personal menos costoso apoyado por la tecnología o por legos armados de herramientas *on-line* del tipo “hágalo usted mismo”. Ni hablemos ya de la inteligencia artificial y de los robots. Al parecer, ni el derecho ni la abogacía les estarían siguiendo el paso a los múltiples fenómenos tecnológicos que se suceden vertiginosamente y que han pasado a ser fenómenos sociales.

A contrapelo de lo señalado, la gran habilidad retórica de los letrados parece defender un *statu quo* propio del siglo XX, con revisiones endogámicas en torno a los mismos tópicos legales. Ahora bien, descartada una postura nihilista, escéptica o desencantada, consideramos que el reto es, justamente, desbrozar el derecho a partir de preguntas ontológicas.

### III. EL ESTUDIANTE POSMODERNO

La Ley 30220, Ley Universitaria peruana, consagra el principio del interés superior del estudiante; de manera concordante, la Política de Aseguramiento de la Calidad Educativa, aprobada mediante Decreto Supremo 016-2015-MINEDU, se sustenta en el principio del estudiante como centro. No es necesario abundar en citas de dispositivos legales que formalicen esta postura, que constituye un giro copernicano que incluye el salto de la educación centrada en la enseñanza hacia la educación centrada en el aprendizaje. En tal sentido, es de rigor indagar acerca de quién es ese estudiante de hoy. Para ello, nos situaremos en el tránsito entre la modernidad y la posmodernidad, esta última como proceso cultural con distintas corrientes aparecidas a partir de mediados del siglo XX.

En el medioevo, los estamentos y una cultura teocéntrica estructuraban la sociedad; es precisamente en ese contexto en el que nace la universidad, cuyos principios clave, según Bicocca (2016), son la universalidad del saber, la autonomía

institucional, el espontáneo deseo de conocer y el ocio necesario para la reflexión. Destáquese que una de las condiciones para aprender es contar con tiempo libre para reflexionar. Hoy en día la palabra *ocio* y su derivado *ocioso* son casi malas palabras, pues vienen asociadas con la *pérdida de tiempo*. En buena cuenta, esta asociación se cimenta en el Renacimiento y en la ética protestante, cuna del capitalismo<sup>2</sup> y raíz de su principal aforismo: *el tiempo es oro*.

Sin embargo, no se considera “ocioso” navegar por las redes sociales durante horas, con independencia del propósito, en tanto tenga sentido “para uno”. Por otra parte, en un mundo que reclama a las mayorías combinar el estudio con el trabajo, ese espacio de ocio reflexivo parece una entelequia.

Hoy en día, las cosas ligadas a la temporalidad envejecen mucho más rápido que antes. Se convierten en pasado al instante, y, de este modo, dejan de captar la atención. El presente se reduce a picos de actualidad. Ya no dura. (Han, 2015, p. 18)

Ya en la modernidad, Descartes, con su famoso lema *Cogito, ergo sum* (*Pienso, luego existo*), introdujo la dualidad entre el pensamiento y el mundo material. En el ideario modernista, prima el sujeto.<sup>3</sup> A su vez, ese sujeto moderno piensa y razona, para a partir de ello comprender el mundo y la realidad. A diferencia de lo que sucedía en la época medieval, Dios ya no está en el centro. La nueva visión es antropocéntrica y racionalista.

La razón pasa a ser el caleidoscopio para mirar el mundo,<sup>4</sup> mientras que la realidad pasa a un segundo plano, en el sentido de que no se la considera como algo absoluto: su caos puede ser efectivamente alterado, rediseñado, corregido o dominado por el hombre mediante la razón, que trae aparejadas la ciencia y la tecnología. El hombre se sintió poderoso con la maquinaria, medios de transporte, vías de comunicación, motores y demás manifestaciones de la Primera Revolución Industrial.

En cuanto al sistema educativo, este se asemeja a la producción en serie, con su uniformidad (y el uso de uniformes), la adhesión a determinados estándares, el control y, en general, la búsqueda del dominio del caos (representado por las individualidades, las diferencias y las diversidades). La escolarización obligatoria, con el requerimiento de atención de un gran número de estudiantes, fue tributaria del modelo panóptico de Bentham.

No en vano, Michel Foucault (2002), en uno de sus libros más influyentes, asimiló *escuela* y *cárcel* en un único concepto. Foucault refiere que las libertades del siglo XIX se sostienen en una sociedad disciplinaria. Las instituciones educativas se diseñaron para constreñir el radio de acción de los estudiantes encerrándolos en sus carpetas, con una disposición en filas de cuerpos uniformados mirando al frente a la autoridad que administra el aparato disciplinario, cuya función es correctiva. Agrega Foucault que el examen es utilizado como vehículo para calificar, clasificar y castigar. Piénsese también en el fordismo

<sup>1</sup> En el Perú el Decreto Legislativo 1342 regula acerca del lenguaje y el acceso a la justicia. Señala que “Los operadores del sistema de justicia evitarán usar términos en latín o cualquier otro arcaísmo que dificulte la comprensión de las expresiones y términos legales que contiene sus actos o resoluciones.”

<sup>2</sup> Ver, especialmente, Max Weber.

<sup>3</sup> Léase a Kant, Hegel o Kirkegaard, entre otros.

<sup>4</sup> Como momento cumbre de ello piénsese en la entronización de la Diosa Razón en el altar mayor de la catedral de Notre Dame, durante el período de la *Terreur* de la Revolución Francesa.

de principios del siglo XX y trasládese la imagen de una fábrica —o de una cárcel o de un hospital— a una institución educativa.

La modernidad formuló grandes promesas: la promesa del progreso, de la ilustración, de la razón como garante de leyes justas, de un mundo pacífico y ordenado con abundancia para todos. La nueva utopía ofreció dominar la naturaleza, frenar los estallidos sociales e, incluso, diseñar un nuevo orden moral. Así se refleja en la iconografía de la época, en la arquitectura, en su heráldica y en sus textos constitucionales. El tamaño de esas promesas se vio reflejado en grandes edificaciones, como el campus universitario, sólido y monumental. Lo cierto es que la modernidad fracasó, pues, antes que la paz que nace de la justicia y el progreso, nos legó guerras mundiales, campos de concentración nazis, guetos, gulags, Chernobil, y demás.

Hoy el estudiante posmoderno, desencantado, rechaza las totalizaciones, un único orden, la linealidad (el bucle comienzo-desarrollo-fin), la estandarización, los corsés (físicos y mentales) y lo que denomina “etiquetas”; todo eso propio del *mundo sólido*. El tiempo lo percibe fragmentado y la vida *rebanada en episodios y salpicada por nuevos comienzos* (Bauman, 2021, p. 10). Así, cambia de profesión, inicia estudios superiores tras varios años de haber concluido la secundaria; se muda con cierta frecuencia; opta por no tener descendencia o tenerla a edades antes consideradas “tardías”, mediante, por ejemplo, embriones criopreservados; redefine su género o sus roles de género; se decanta por ser *influencer-tiktoker* profesional y —conjuntamente— funcionario del Estado; mantiene una relación poliamorosa o está en una *situationship*. La enumeración no concluye aquí.

En suma, ya no está encasillado por las edades normativas para hacer —o dejar de hacer— tal o cual cosa. Percibe distintas realidades sucediendo en paralelo, en ventanas que abre y cierra, e interactúa con otras personas sin necesidad de identificar jerarquías que se aplanan hasta desaparecer. Se plantea (desde una posición biocentrista) interactuar con los animales (y con las plantas) en una relación entre seres sintientes y no como sujeto-objeto. Así, no sería de extrañar que, en un futuro cercano, el estudiante posmoderno reclame que la universidad tenga guarderías para sus “perrhijos” o “gathijos”, en tanto deja en casa a sus plantas, que serían las “mascotas”. Esta postura que a las personas *sólidas* les podría parecer irrisoria, va aún más allá si se traslada a los llamados *plant parents*.

Según el *New York Post*, muchos milenials (entre 25-39 años) adoptan plantas como prueba para saber si son lo suficientemente responsables para hacerse cargo de una mascota animal. Ese es el contexto del sujeto posmoderno, cuyo yo individual es responsable de construir tanto su estructura como sus propias realidades, algo que cansa y atemoriza.

Por una parte, suena liberador decirle a alguien que puede ser lo que quiera ser; pero, por otra, intimida saber que debe autoconstruir su mundo y luego cargar con él. Según Bauman (2021, p. 23), ese “derecho a ser” incluye el “derecho a ser dejado en paz”, para autodefinirse y autoafirmarse; sin embargo —agrega— esa naturaleza inacabada o “no definitiva” genera ansiedad. No en balde, atender la salud mental es un aspecto en boga en el ámbito educativo y una exigencia legal para renovar la licencia de las universidades peruanas.

Por si fuera poco, en el mundo *líquido* se vive no solo en la “sociedad de riesgo” beckettiana, (Beck, 1998), sino en la sociedad de las opciones cuasiinfinitas, que dejan el mal sabor de boca de sentir que siempre estamos perdiéndonos de algo. Quizás ello explica la imposibilidad de prescindir, aunque sea momentáneamente, de lo que en palabras de Marco Aurelio Denegri sería una prótesis esclavizante: el celular. Es común, y hasta de rigor, revisar permanentemente los *posts* o tuits, dar y recibir *likes*, subir fotografías, etcétera, mientras el docente facilita una sesión de aprendizaje; todo ello, sin distinguir cuál es la actividad principal y cuál la secundaria.

Hoy en día el espacio ya casi no cuenta, ha sido desplazado por el tiempo y las (multi)dimensiones. El tiempo es de instantes, de fragmentos, lo que va muy de la mano con la tecnología. Sentimos que puede ser rebobinado: por eso no prestamos atención. Cuando no es posible rebobinar “la cinta” que es la vida, nos fastidiamos fugazmente y dejamos pasar ese momento para fijar nuestra atención en otra cosa, porque —total— hay tantos estímulos que atender. Sin mayor destreza en el *mindfulness*, es decir, sin atención plena, es comprensible preguntar en una sesión sincrónica si “se está grabando” para verla luego.

Así como el espacio ha sido desplazado por el tiempo, la realidad ha sido destronada por las experiencias. Los estudiantes no quieren irritantes *clases*, sino *experiencias de aprendizaje*. Según Han (2022), hemos pasado de las posesiones a las experiencias; si se adquiere cosas, en realidad lo que se compra son las emociones que nos dan, por fugaces que sean. Desde esta óptica, quizás ha perdido sentido, por ejemplo, que para la ley peruana un crédito académico equivalga a dieciséis horas de teoría o el doble de práctica, cuando para los estudiantes tiene más valor el aprender haciendo de la práctica, que les genera experiencias de aprendizaje y emociones más intensas.

Otro aspecto que destaca Han (2022) es la transición a la era de las *no-cosas*. En el mundo sólido habitamos la tierra y tenemos un cielo sobre nuestras cabezas; eso nos da estabilidad. Sin embargo, hoy —siempre según Han— habitamos Google Earth y la nube. En ese mundo intangible, los estudiantes posmodernos demandan el estímulo de la sorpresa y de la contingencia; quizás por ello no es descabellado el término docente-clown, no como “payaso”, sino como generador de experiencias que brinden emociones, como vehículo para el aprendizaje.

En línea con lo esbozado, se sitúa la crítica de los docentes sólidos a los estudiantes líquidos, a quienes se acusa de no prestar atención, ser desenfocados, mirar al vacío, no cumplir con los horarios y variar rápidamente de intereses, dispersándose detrás de “objetivos o blancos variables y en movimiento” (Bauman, 2021, p. 27), entre un rosario de quejas e imputaciones que inician con el consabido *en mi época y culminan con un nostálgico todo tiempo pasado fue mejor*.

#### IV. LA UNIVERSIDAD, CRISIS DE IDENTIDAD EN LA ERA DIGITAL

La universidad es una institución antigua que se adhiere a la tradición y, por qué no, al pasado. Ello no es, *per se*, un demérito. Podría, sin embargo, serlo si se queda atrapada en lo lineal, lo continuo, lo uniforme y lo similar.

A lo largo del tiempo, nos hemos valido de la analogía como recurso cognitivo. El pensamiento analógico demanda buscar los conocimientos adquiridos en el pasado, identificar sus características o cualidades y cotejarlos con el nuevo objeto de estudio, para encontrar lo común o similar. Comparamos y buscamos esa relación de semejanza, encantados cuando hallamos una repetición, porque implica continuidad y se apega a lo natural.

Lo digital, a contrapelo, acepta lo artificial. Una forma de pensar digital es una forma diferente de pensar, donde rigen las reglas de la no similitud, la discontinuidad y la arbitrariedad. En el presente, coexistimos personas del siglo XX con personas del siglo XXI; la diferencia más saltante no radica, precisamente, en la fecha de nacimiento, sino en la forma de pensar.

En el ámbito de la educación, cabe traer a colación lo señalado por Bauman (2013, p. 21):

Otra de las inestimables contribuciones de Bateson (...) es la distinción que hace entre tres niveles de educación. El más primario sería la mera transferencia de información para ser memorizada. El segundo, el “deuteroaprendizaje”, tendría por objetivo el dominio de un “marco cognitivo”, en el que la información adquirida o hallada puede, en el futuro, ser abstraída e incorporada. Pero también existiría un tercer nivel, que consistiría en enseñar unas aptitudes que permitieran desmembrar y volver a organizar el marco cognitivo predominante, o bien desecharlo por completo sin sustituirlo por un elemento de reemplazo.

La universidad de la era digital ya se encuentra, o debería encontrarse, en ese tercer nivel. No se trata, por cierto, de ser nihilista y rechazar todo lo pasado, pero estamos en un proceso no solo de cambio sino de resignificación de la educación superior, que la pandemia por COVID-19 agilizó. En ese proceso, a la par que se realizan análisis teóricos y se formulan propuestas concretas de intervención, es necesario preguntarnos si se requiere darle un nuevo contenido a antiguas categorías o, inclusive, si es necesario crear nuevas categorías.

A través del lenguaje se puede transformar la realidad y construirla. Claro que no basta intervenir en el lenguaje para lograr que haya un despliegue en la acción, pero sin una intervención narrativa se favorece el *statu quo*.

Si el reto es lograr un cambio cualitativo entre un estado previo de la educación superior a uno posterior, es necesario resignificarla y, por ende, resignificar a las instituciones de educación superior. ¿Qué entendemos por Universidad hoy?

La Ley Universitaria peruana señala que la Universidad es una comunidad académica formada por estudiantes, docentes y egresados. Más allá de eso, ¿es un espacio simbólico y relacional de acceso restringido cuya finalidad es formar profesionales que respondan a las demandas del mercado? ¿Es decir, es un centro de formación de empleados o emprendedores? La respuesta es no.

La Universidad debe formar profesionales y ciudadanos que lideren el desarrollo sostenible de la Nación. Pero ¿Lo hace? Ese es uno de los retos de la educación superior en el Perú hacia el 2030.

El significado de lo que es la Universidad está en descomposición y lo que se instaló en un momento dado en la conciencia y en la percepción de los actores sociales y las comunidades como uno de los “grandes relatos” está mutando.

Nos encontramos apenas en un proceso de interacción que instituye la base dialéctica para la transformación de su contenido y su resignificación.

Si la Universidad ya no es una institución sólida, sino por el contrario un actor social débil, entonces ¿Podrá ser la arena en la que se formulen las grandes preguntas de la humanidad? Si no es así, entonces podrá seguir llamándose igual, pero ya no será eso que habíamos categorizado como tal.

## V. LOS RETOS DEL DERECHO EDUCATIVO

Uno de los retos del derecho educativo es contribuir desde el sistema jurídico a que se concreten las innovaciones y los cambios que, en el marco de su autonomía, proponen las instituciones educativas y, en particular, las universidades para atender las demandas de las nuevas generaciones.

En línea con lo anterior, los operadores del derecho educativo deben interiorizar que no hay vuelta atrás, que o lo tunean y se tunean a sí mismos—sí, tunear es un verbo registrado en el Diccionario de la lengua española— o la realidad social se les seguirá escapando en ese creciente proceso de anomia denominado informalidad.

Se requiere humildad para aceptar que los procesos legales se diseñan de manera parcelada y compleja, como un laberinto del fauno, y hacer algo al respecto. Los resultados, kálficos, alimentados por largos plazos que no se cumplen y profusa y enmarañada legislación, frenan no pocas iniciativas y elevan los costos de transacción. Con ello, se afecta el acceso a la educación, bajo el mantra de la defensa de la calidad educativa, a cuya sombra crecen los cada vez más abundantes mecanismos de supervisión y fiscalización de las universidades.

El derecho educativo debe hacer posible la materialización de una educación transfronteriza, ineludible en medio de la globalización. Ese es un desafío emergente en el marco de las relaciones sin fronteras que la digitalización impone.

El derecho educativo debe distinguirse por la transdisciplinariedad y el dinamismo. Sin desdeñar el abordaje desde el punto de vista del paradigma clásico, debe ser capaz de tener una mirada desde la complejidad del mundo actual. Ello requiere de abogados capaces de interactuar con profesionales de distintas especialidades, no solo para cumplir con una formalidad y “socializar” ideas preconcebidas grabadas en piedra, sino para abrir el cerrado mundo jurídico hacia esa realidad que se les va de las manos.

El derecho educativo puede ser esa piedra de toque que en un momento de quiebre como el actual no se limite a la formulación de declaraciones. En el escenario presente no se necesitan simples gestos y menos muecas: el llamado blablablá hace tiempo que dejó de ser atractivo.

Los abogados especializados en derecho educativo tienen como función social servir a la materialización del derecho fundamental a la educación en condiciones de equidad. Como servidores de la Justicia y colaboradores de los magistrados — de la justicia ordinaria y la justicia constitucional— deben encauzar una correcta aplicación e interpretación del derecho, sobre la base de principios del derecho educativo, así como colaborar con el desarrollo de políticas públicas “que tengan un carácter transformador” (Unesco, 2017, p. 96).

Se requiere asumir la defensa de la universidad para atemperar la minimización de su autonomía, recuperar la confianza en sus autoridades y servir mejor a la educación superior en un

escenario posmoderno. En esa tarea, las facultades de derecho tienen la palabra: ¿dónde se forman esos abogados de nuevo cuño diestros en el diseño de un sistema jurídico flexible y en la interpretación razonada de las normas sobre la base de principios universales, en comunión con los hechos sociales?

Unesco (2017). *Revisión de las políticas públicas del sector de educación en Perú*. París: Unesco.  
<https://unesdoc.unesco.org/ark:/48223/pf0000260875>

## VI. BIBLIOGRAFÍA

- Bauman, Z. (2013). *Sobre la educación en un mundo líquido*. Madrid: Artes Gráficas Huertas, S.A.
- (2021). *Mundo consumo. Ética del individuo en la aldea global*. Barcelona: Paidós.
- Beck, U. (1998). *La sociedad del miedo. Hacia una nueva modernidad*. Barcelona: Paidós Básica.
- Bicocca, M. (2016). La idea de Universidad. Un análisis filosófico de sus principios vitales en la Edad Media y su cambio a partir del pensamiento de Martha Nussbaum.  
[https://bdigital.uncu.edu.ar/objetos\\_digitales/8561/003-bicocca-sm-9-1-2016.pdf](https://bdigital.uncu.edu.ar/objetos_digitales/8561/003-bicocca-sm-9-1-2016.pdf)
- Han, B.-C. (2022). *Infocracia. La digitalización y la crisis de la democracia*. Buenos Aires: Taurus.
- Denegri, M.A. Las prótesis esclavizantes.  
<https://www.youtube.com/watch?v=m5MjKx5xcH8>
- Duarte Quapper, C. (2015). El adultocentrismo como paradigma y sistema de dominio. Análisis de la reproducción de imaginarios en la investigación social chilena sobre lo juvenil. Tesis para optar el grado académico de doctor en sociología. Universidad Autónoma de Barcelona.  
<https://www.tdx.cat/bitstream/handle/10803/377434/cdq1de1.pdf?sequence=1>
- Foucault, M. (2002). *Vigilar y castigar. Nacimiento de la prisión*. Buenos Aires: Siglo veintiuno editores.
- Han, Byung-Chul (2022). *No cosas. Quiebres del mundo de hoy*. Buenos Aires: Taurus.
- (2015). *El aroma del tiempo. Un ensayo filosófico sobre el arte de demorarse*. Barcelona: Herder Editorial, S.L.
- New York Post (2020). Millennials say being a ‘plant parent’ is harder than they expected  
<https://nypost.com/2020/01/24/millennials-say-being-a-plant-parent-is-harder-than-they-expected/>
- Novoa Monreal, E. (2007). *El derecho como obstáculo al cambio social*. México: Siglo XXI editores.
- Real Academia Española. *Diccionario de la lengua española*, 23.ª ed. <https://dle.rae.es>
- Sawyer, S. & Azzopardi, P. & Wickremarathne, D. & Patton, G. (2018). The age of adolescence. *The Lancet Child & Adolescent Health*. 2. 10.1016/S2352-4642(18)30022-1.
- Superintendencia Nacional de Educación Superior Universitaria (2021). III Informe bienal sobre la realidad universitaria en el Perú.  
<https://cdn.www.gob.pe/uploads/document/file/3018068/III%20Informe%20Bienal.pdf?v=1649883911>
- Susskind, R. E. (2008). *The End of Lawyers?: Rethinking the Nature of Legal Services*. Oxford University Press.

# Desafíos en la educación de las facultades de Derecho desde los paradigmas de educación y la disrupción tecnológica

J.E. Valderrama Velandia. Universidad Santo Tomás Seccional Tunja. Colombia

**Resumen--** Este trabajo se desarrolló con un método analítico descriptivo, con el cual se aborda las tendencias que marca el uso de la inteligencia artificial en la disrupción tecnológica que afrontan las universidades en la formación de educandos. Particularmente en la formación de abogados y abogadas, se analizan las posturas que están demarcando las tendencias en la formación de los estudiantes, y se delinear algunas propuestas para ajustar los currículos y competencias pedagógicas docentes en la enseñanza y orientación de la formación jurídica. Para este propósito, se postula reorientar la teoría jurídica a nuevas propuestas que den orientaciones y postulen soluciones que engloben la vertiginosa transformación social.

**Abstract--** This work was developed with a descriptive analytical method, which addresses the trends that mark the use of artificial intelligence in the technological disruption faced by universities in the training of students. Particularly in the training of lawyers, we analyze the positions that are demarcating the trends in the training of students, and outline some proposals to adjust the curricula and pedagogical teaching skills in the teaching and guidance of legal education. For this purpose, it is postulated to reorient legal theory to new proposals that provide guidance and postulate solutions that encompass the dizzying social transformation.

**Index Terms—**Curriculum, disrupción tecnológica, enseñanza del derecho, inteligencia artificial, pedagogía, teoría jurídica, trialismo jurídico

## NOMENCLATURE

Inteligencia artificial, pedagogía, enseñanza de derecho, disrupción tecnológica.

## I. INTRODUCCIÓN

La disrupción tecnológica que trae consigo la implementación y uso de la Inteligencia artificial, junto a los propósitos se positivos o negativos que se le ha pretendido endilgar, sea por el uso apropiada como herramienta tecnológica, o como instrumento de interacción sin ningún tipo de responsabilidad, como instrumento de mercado y negocios, abre el debate en el mundo laboral, académico y económico sobre el rol desempeñan profesores, formadores, instituciones educativas,

incluso las mismas virtudes sociales con el uso de la tecnología. La pedagogía y postulando paradigmáticos de la enseñanza se encuentra en una encrucijada que desde ha planteado la extinción de puestos de trabajo, profesiones, incluso, valores sociales y culturales.

Esta ponencia quiere retomar algunos conceptos que, a pesar de tradicionales, son de relevancia para las comunidades educativas, paradigmas que pueden ser útiles en estos momentos de vertiginosos avances, proponiendo enseguida, algunas pautas que sean útiles para afrontar los desafíos que imponen las herramientas de inteligencia artificial en la enseñanza del derecho.

Para esto, se propone la siguiente pregunta ¿Cómo se adapta la pedagogía de la enseñanza del Derecho en las universidades ante la disrupción tecnológica global? Para dar respuesta a esta pregunta, seguiremos un método analítico descriptivo, con el cual, se construirá un referente conceptual necesario que oriente las nuevas tecnologías en la orientación de las teorías jurídicas. Seguido de una propuesta para fortalecer el paradigma con el cual se orienta la enseñanza jurídica en el contexto colombiano, para finalmente proponer algunos lineamientos que puedan ser adaptadas a los currículos en las facultades de Derecho latinoamericanas.

Esta ponencia se centrará en el vector de la tecnología de la inteligencia artificial, por la disrupción que ha creado en el entorno universitario e investigativo, que con un entendimiento multidimensional e interdisciplinar tiene beneficios interesantes como herramienta universitaria.

## II. EL CONTEXTO ACTUAL PARA LA REFLEXIÓN

La preparación y educación de estudiantes de derecho como futuros profesionales debe replantearse en atención a las demandas de la sociedad, el contexto geopolítico-social en que se desenvuelven, como a las realidades políticas, sociales, económicos, axiológicas y tecnológicas de cada país, lo que demanda la articulación e integración de saberes jurídicos con los saberes no jurídicos [1].

La preocupación que surge en la actualidad, son la irrupción de tecnologías de las comunicaciones, en donde la información se genera de formas instantáneas, muchas de las veces sin control, o conllevan un riesgo importante para los involucrados.

El actual cuadro social que se ha generado por la revolución digital de la Web y la expansión de numerosos tipos de redes sociales o comunidades virtuales, revela características especiales en las formas para informarse sobre noticias, recibir información, establecer contactos y ejecutar actividades de colaboración profesional, y hábitos nuevos en actividades cotidianas y formas de intercomunicación, como chatear y compartir aficiones, hobbies, fotos e interacciones sociales, en donde el entorno convivencia cambia radicalmente por las redes e internet, que cuentan con una serie de herramientas tecnológicas muy sencillas de utilizar y permiten la creación de comunidades de personas entre las que se establece un intercambio dinámico y comunicativo. Con uso de las redes, la metodología de uso se basa en las teorías constructivistas, fundamentadas en la teoría interaccionista de Vigotsky, que expone en cuanto al desarrollo cognitivo, el aprendizaje es un fenómeno social y colaborativo que se obtiene mejor con la interacción social [2].

La evolución del uso la tecnología en las aulas de clase como en el mundo laboral, ha llevado a simplificar algunas actividades, pero al mismo tiempo, exponer a los estudiantes como a los profesionales a otras dinámicas que reclaman eficiencia y resultados cuantificables.

Así, otro paso en la disrupción que la tecnología trae consigo es la digitalización. La digitalización, en su sentido amplio, es la reorganización de estructuras y relaciones sociales, culturales y económicas ocasionada por la generalización de las tecnologías digitales de la información y la comunicación, en ámbitos de la actividad humana y de la sociedad actual, transformaciones que hace necesario adquirir conciencia de la impresionante cantidad de cambios que supone la introducción de las tecnologías digitales en la universidad y la actividad de las personas en diferentes contextos. Así, reconocer las relaciones entre sujetos y objetos y las perturbaciones que tiene lugar en la universidad como realidad compleja cuyo impacto de la tecnología debe analizarse conjuntamente con los principios, procesos y parámetros de diseño, implementación, despliegue y uso de la tecnología con las decisiones humanas, orientado por un análisis crítico de la tecnología educativa en la universidad que exige no descontextualizarla del trasfondo de valores,

estructuras y actores que influyen en la toma de decisiones y el gobierno de nuestra sociedad [3].

Hoy en día, es la inteligencia artificial y su irrupción en la vida cotidiana de las personas están disponiendo de vertientes para la reflexión continua de los riesgos que se pueden asumir, o de las tendencias que se impondrán en ámbitos como el consumo, la educación y la fuerza laboral.

En este punto, se hace necesario acercarse a la noción de las tecnologías disruptivas, al menos, en un ejercicio comparativo. Las tecnologías disruptivas desafían y cambian fundamentalmente las estructuras o funcionamientos empresariales; mientras que las tecnologías sostenibles apoyan y mejoran los medios en que operan las empresas, como los programas de contabilidad informatizados. Con ello, las tecnologías disruptivas, en un primer momento pueden ser subestimadas por la superficialidad o pocas probabilidades de adopción, y enseguida, provocan cambios profundos en sectores en los cuales se aplican [4]

Entonces puede plantearse que la universidad y la pedagogía deben recorrer un camino vertiginoso, en el cual, la velocidad está imponiéndose por los avances tecnológicos y demandas del mercado, sin perder de vista que la formación profesional es elemental para las sociedades.

## III. NOCIOS INDISPENSABLES PARA LA ENSEÑANZA DEL DERECHO Y LA INTELIGENCIA ARTIFICIAL

La irrupción de la inteligencia artificial sitúa en el debate las nociones hasta el momento aprendidas, las técnicas adquiridas en los espacios académicos y pedagógicos que docentes y estudiantes compartían, y las pautas de enseñanza y aprendizaje de las ciencias sociales.

### A. Tecnología de las comunicaciones

Las tecnologías de la comunicaciones nacen de la innovación tecnológica, permitiendo la creación de nuevos entornos comunicativos y expresivos que abren la posibilidad de desarrollar nuevas experiencias formativas, expresivas y educativas, por lo cual, las TICS son un conjunto de procesos y productos derivados de las nuevas herramientas en hardware y software, cuyos soportes de la información y canales de comunicación, relacionada con el almacenamiento, procesamiento y transmisión digitalizados de la información son rasgos distintivos de estas tecnologías junto con la inmaterialidad, interactividad, instantaneidad, innovación, con elevados parámetros de calidad de imagen y sonido, digitalización [5]. En la actualidad, las tradicionales modalidades de enseñanzas presencial y a distancia, se suma la enseñanza en línea, que usa redes telemáticas a las que se encuentran conectados profesorado y alumnado para conducir las actividades de enseñanza-aprendizaje y ofrece en tiempo real servicios administrativos [6].



El mundo globalizado demanda nuevos saberes, y con la reciente digitalización, y la popularización del computador y el Internet, el modelo de distribución de la información ha cambiado, dado lugar a la Sociedad del Conocimiento, en el cual, las ideas y sus aplicaciones alcanzan más valor, junto con las interconexiones entre lugares, personas, economías y disciplinas. Adicionalmente, la innovación involucra la generación de ideas para mejorar procesos educativos, en los cuales se comparte tecnología y desarrollo de teorías [7].

Las nuevas tecnologías han causado profundas mutaciones en el flujo de información y su distribución, y a su vez, el uso de TIC contribuye a la formación de educandos y docentes, porque sólo contribuyen a la creación y difusión de los conocimientos, sino que además son importantes para preservarlos [8].

### *B. La inteligencia Artificial*

El Consejo Europeo propone como definición de la Inteligencia Artificial al uso de la tecnología digital para crear sistemas que puedan realizar tareas que por lo general se considera que requieren inteligencia humana, con la capacidad de contribuir a una economía más innovadora, eficiente, sostenible y competitiva, mejorando al mismo tiempo la seguridad, la educación y la atención sanitaria de los ciudadanos [9].

Iniciativas de orden comunitario como el Reglamento de Inteligencia Artificial, trabajado en el seno del Consejo Europeo de la Unión Europea, del 21 de abril de 2021, han contribuido a delimitar el concepto de la Inteligencia Artificial con criterios claros para distinguirlos de otros sistemas de software clásicos, para lo cual, comprenden como Inteligencia artificial a los sistemas desarrollados a través de estrategias de aprendizaje automático y estrategias basadas en la lógica y el conocimiento, siendo relevante en lo que a prácticas prohibidas, se sitúa a los agentes privados la prohibición de utilizar la Inteligencia Artificial con fines de puntuación ciudadana. Además, aprovechar las vulnerabilidades de grupos específicos de personas por su situación social o económica y en lo relativo al uso de sistemas de identificación biométrica en tiempo real en espacios de acceso público [10].

El 13 de marzo de 2024, en Estrasburgo, el Parlamento Europeo aprobó la Resolución legislativa que reglamenta el uso de la Inteligencia Artificial en el marco europeo, en los países que integran la unión, donde el Consejo europeo en el considerando 4 asumió la AI como el conjunto de tecnologías de vertiginosa evolución para contribuir en ayudas económicas, sociales, medioambientales, sanitarias, agrarias, educativas, culturales, deportivas, en sectores de justicia, servicios públicos, transporte, lo que redundará en proveer ventajas competitivas esenciales para facilitar la obtención de resultados positivos desde como optimizar las operaciones y la asignación de los recursos, y personalizar las soluciones digitales que se encuentran a disposición de la población y las organizaciones.

Esto abre un campo de aplicaciones en las empresas y en la educación, relacionadas con la adaptación de los procesos empresariales, académicos y organizacionales, acondicionados al usuario, como son el estudiante de derecho, lo que conduce a un mundo compartido por seres humanos y bots que tiene particular impacto en el futuro de la educación, cambios que llevan a nuevas formas de trabajo, tareas a realizar, habilidades demandadas, como cambios culturales en los actores laborales, que demanda aprendizaje, adaptación, capacitación positiva en los actores del proceso de transformación digital [11].

### *C. Problematicación en la enseñanza del Derecho*

A fin de considerar las anteriores nociones de la tecnología y la inteligencia artificial, su uso sea como herramienta para los docentes y la investigación, o como conjunto de datos que sustituye las actividades de docencia que puede impartir un experto en Derecho, son las vertientes que sustentan la pregunta propuesta inicialmente, porque la pedagogía de la enseñanza del derecho en una sociedad del conocimiento digitalizada, está volcada a innovaciones que desplacen o por lo menos sustituyan las bases clásicas de las relaciones estudiante-docente-universidad.

La educación virtual y la aplicación del derecho, reconoce que la presencia de la tecnología suscita la necesidad de revalorizar la docencia, lo que conlleva a centrar su atención en la relación enseñanza-aprendizaje, con lo cual tecnología y derecho, tiene una correspondencia entre los retos del Derecho para concebir la nueva percepción de la realidad a través de los cambios sociales y el estudio tradicional de las figuras jurídicas, y las tecnologías disruptivas emergentes, que desde los intereses privados llegan a tener pretensiones democráticas, como verdaderas democratizadoras del derecho y permitir a los ciudadanos, en principio, acceder a consejos y orientaciones del mundo jurídico, superando dificultades como los honorarios de un buen abogado, incluso, empleando un lenguaje más amigable y sencillo [12].

En la resolución de problemas específicos, la aplicación de la inteligencia artificial ha tenido éxito, y se continúa trabajando para imitar, e incluso, superar, la actuación del ser humano en su proceso de razonamiento o adaptación a macro problemas, es decir, el planteamiento de problemas y circunstancias de complejidad. La evolución de la inteligencia artificial se caracteriza por un aprendizaje continuo a través de la red de internet [13].

Las orillas en las cuales se sitúan contradictores y defensores del uso de la tecnología en las aulas de clase, son marcadas por las tendencias tradicionales de la enseñanza axiológica y la presencia de un experto, como por las tendencias del mercado, en obtener los mayores rendimientos con los mínimos costos. Se enfrenta entonces debates de varias vertientes y corrientes, a los cuales, las universidades y facultades están llamadas a sortear y visualizar en un mediano y largo plazo.

La pedagogía en la enseñanza del Derecho se ha venido transformando constantemente, dando inicio por la enseñanza magistral, en la cual la información se transmitía pasivamente al estudiante, sin permitirse la innovación o aporte propio desde sus vivencias, siendo relevante la exposición dada por quien detentaba la cátedra, con lo cual, el conductismo prevaleció gran parte del siglo XX en las aulas de clase. Con el surgimiento del constructivismo y la participación activa del estudiante, el rol docente se encaminó a la orientación y conducción de información y valoración de la misma.

La disrupción tecnológica por lo menos supone la adaptación de múltiples datos, cantidad de información, y transformaciones sociales que deben considerarse en la orientación teórica del mundo del derecho.

#### IV. APORTES PARA UN PARADIGMA ACTUALIZADO EN LA ENSEÑANZA DEL DERECHO

Con el constructivismo, llegó la mediación de la dialéctica para equilibrar proporcionalmente las pedagogías empleadas por los docentes. Sin embargo, en la actualidad se está recuperando la idea pedagógica de formación en el ethos, la frónesis o juicio prudencial tanto en lo teórico como en el campo práctico, de tal forma que el individuo pueda formarse en el criterio como adquiriera las virtudes necesarias para la vida en sociedad, y con ello, la pedagogía está encaminada a una educación analógica estructurada en la moderación y la proporción de los saberes y las virtudes [14].

La tradición jurídica en las universidades colombianas esta ceñida a la enseñanza positivista, en la cual, la interpretación de la ley, el análisis en la producción legislativa, con la visión a su eficiencia y validez, convirtieron a las facultades de derecho en fríos salones, que en la mayoría de ocasiones se alejan de la realidad social, y otras tantas, están desactualizadas.

Sin embargo, los avatares del tiempo, como lo fueron las medidas decretadas para afrontar las exigencias de la pandemia en el año 2020, impulsó exponencialmente el uso de la tecnología en la mayoría de los ámbitos de las vidas de las personas. Escenarios académicos, profesionales, negociales y hasta familiares se vieron involucrados en el avance al uso de tecnologías de las comunicaciones, y la innovación.

Las Tecnologías de la Información y la Comunicación (TIC) se han incorporado en todos los campos de la sociedad, desde el económico al educativo, dando paso a la llamada Sociedad de la Información y del Conocimiento, con un conjunto de revoluciones en ámbitos jurídicos, políticos, educativos y sociales, lo cual ha construido un ecosistema de tecnologías para la creación social del conocimiento, que incorpora tres características esenciales, tecnología, conocimiento y usuarios [15].

Con la transformación digital, comprendido como la integración de la tecnología en la organización para encontrar las mejoras, con la integración de herramientas y recursos

digitales en los procesos de aprendizaje para optimizar la docencia y la investigación en la educación superior, que aún hoy en día, en entornos físicos al aprendizaje digital, se dirige en distintas áreas que necesitan atención, como lo son desarrollo docente, cambio organizacional, prácticas innovadoras y nuevos modelos institucionales, efectividad de las actividades de enseñanza y aprendizaje, experiencia estudiantil, estrategias y modelos de financiamiento [16]

Por ello, el conocimiento debe concebirse no un tema de cantidades sino del significado que se le otorga, superando la tradicional noción del conocimiento como algo objetivo, estable, producido por expertos, que se puede transmitir a algo subjetivo, dinámico y producido de forma colaborativa, por cuanto, el conocimiento no es una verdad objetiva sino variable y verificable. Con la conectividad en la sociedad actual, se ha transformado el sentido y la producción del conocimiento, revaluando los espacios y los tiempos del aprendizaje, rompiendo la organización social del siglo XX. Las tecnologías móviles permiten a los estudiantes operar a través de diferentes contextos, con el uso de herramientas de las tecnologías, plantear temas en los espacios físicos de una institución, y problematizar el tema con recolección de datos de forma libre, apoyados en programas o software generar nuevos conocimientos e intercambiar resultados en o en un entorno virtual [17].

Los modelos educativos de orientación inclusiva, han surgido como respuesta a los modelos tradicionales basados en el paradigma integrador los cuales han revelado insuficiencias tanto para garantizar la equidad y la justicia social, como para dar respuesta a las necesidades y retos asociados a las desigualdades tradicionales y emergentes de las sociedades contemporáneas. Ahora bien, la Universidad ha suscrito los principios de los modelos inclusivos que garantizan la equidad en la participación, ello no se ha traducido aún en una transformación efectiva, siendo un ejemplo de ello, garantizar este acceso universal y desde el principio de equidad, con políticas de acción afirmativa orientadas a facilitar las transiciones escuela-universidad de aquellos estudiantes que se encuentran en situación de desventaja, lo que ha llevado a este sector de la comunidad académica sea neutralizado bajo la óptica de políticas neoliberales e imperativos económicos. Traducidos al uso de las herramientas en las aulas, trae consigo una amplia brecha de desigualdad entre el estudiantado en desventaja social y económica a causa del acceso a dichas herramientas tecnológicas, ya que, si no todo el alumnado posee los recursos necesarios para el uso de las TIC tal y como se plantea en las aulas, existirá un grupo de estudiantes que se pueden quedar atrás [18].

Sin embargo, aparece el reto que la era digital arroja en la universidad y la preparación del futuro abogado o abogada, expresado en el detrimento de los procesos reflexivos, seguida de la temible escasez de teorización, imprescindible para el avance de la ciencia, sea por la falta de tiempo, de interés o de rentabilidad a la hora de encumbrar publicaciones o financiación para proyectos de investigación, en donde por ejemplo, con el uso de Big Data, cuyos resultados de análisis de datos contando con redes de ordenadores en todo el mundo

amenaza con acabar la teorización en las ciencias humanas, pues bastará que el software encuentre patrones entre los datos para, así, obtener el conocimiento [19].

La problematización de las fuentes desde la cuales se plantean las relaciones humanas y máquinas, surge de la combinación de cuestiones que Suchacka, Muster y Wojewoda sintetizan así “1) social and ethical aspects of the human-machine relationship – with special emphasis on the dimension of pragmatism, trust and fascination with new technologies and the principles of robot ethics, 2) the effects of automation processes, creative capabilities of human being and having appropriate competences, 3) research needs emerging as conclusions from the previously conducted considerations on the still undeveloped research fields related to AI.” [20, p. 432-433].

En la sociedad, se ha planteado el debate relacionado con la tecnología y la técnica con su correlación en la comunidad, especialmente cuando el escenario tecnológico y su propio discurso fascina, asociándose al determinismo tecnológico autores como Harold Innis, Marshal McLuhan y la escuela canadiense al considerar las tecnologías de los medios de comunicación como determinantes de formas de percepción y sensibilidad en la historia humana [21], a tal punto que se ha planteado cambios en las pautas de las actividades humanas de índole laboral, productivo, y hoy en día educativo están en la lectura y expectativa, como expresión de la influencia social de la tecnología [22].

Sin embargo, a esta postura también sobresalen quienes sostienen que el determinismo tecnológico no es suficiente para dar alcance y explicación a los fenómenos de las tecnologías de la información y las comunicaciones con las relaciones humanas [5]. Por cuanto la toma de decisiones, si bien estará asociada al hombre, reconoce que la tecnología digital son condiciones ineludibles para los beneficios de la sociedad de la información.

Esto conlleva a plantear en los entornos universitarios, campos que concilien los avances de las tecnologías, la formación de profesionales con competencias y aptitudes críticas y firmes antes las expectativas y retos que La tecnología generara en la sociedad.

## V. ALGUNAS CONSIDERACIONES EN LA UNIVERSIDAD Y LA INCORPORACIÓN DE LA INTELIGENCIA ARTIFICIAL

En el ecosistema digital, las universidades juegan un papel fundamental, como centros generadores de conocimiento a partir del impulso de la investigación basados en el método científico, como impulsando las tendencias innovadoras en la industria y las aplicaciones sociales de la tecnología.

Por lo tanto, la reconstrucción curricular de los planes de formación y educación en Derecho deben superar la etapa decimonónica, basada en procesos conductivistas, y que recientemente bajo el halo constructivista, permanecía con pasividad a la actividad e iniciativa del estudiante, para aplicar

métodos prudenciales en el uso de herramientas tecnológicas con la interacción humano-máquina.

El aporte que la teoría jurídica puede encontrar, logra descifrarse desde La Teoría trialista, reclutada en la concepción tridimensional del Derecho, según la cual este consta de hechos, normas y valores, la cual se desarrolló desde el integrativismo que comprende dentro del fenómeno jurídico las dimensiones sociológica, nomológica y axiológica. Con la Inteligencia Artificial aplicada en las redes sociales, se acentúa la división entre derecho consuetudinario y derecho repentino aumentado por la aceleración tecnológica e induciendo y auxiliando a la adopción de toma de decisiones a un ritmo vertiginoso, el Trialismo, por medio del reconocimiento de las adjudicaciones descriptas, con la comprensión del proceso de toma de decisión, y del descubrimiento de las categorías como bioética, cibernética, inteligencia artificial y nuevas tecnologías, pretende brindar un complejo realista del fenómeno jurídico y su actualización permanente, para superar la paquidérmica acción del derecho superado por la realidad[23].

Piénsese en las dimensiones de transformación en la teoría de los derechos con la perspectiva de cambios a la luz de la inclusión de tecnologías de la comunicación y la información, siendo adecuado pensar en marcos normativos menos rígidos y que permitan un campo explicativo de los cambios de los derechos tradicionalmente liberales en clave de realidad tecnológica. Con ello, la teoría de los derechos contemporánea cuenta con una clara influencia analítica, lo que implica que los análisis de derechos se encuentran en la comprensión de sus usos y sus contextos de aplicación y no en el descubrimiento de su esencia [20]

### A. Actualización curricular transversal

Las tecnologías de la información están logrando generar, procesar, almacenar y transmitir datos y valores a velocidades inimaginables con lo cual, se van produciendo profundos cambios en la sociedad, las fuentes de trabajo, las formas de producción y consumo, inclusive como se aprende y genera conocimiento, con ello, son las nuevas dinámicas sociales, políticas, culturales, económicas y de apropiación del conocimiento, con lo cual, la incorporación de la inteligencia en los servicios digitales rediseñan procesos en forma innovadora, de tal manera que la economía digital se potencia en el entorno internacional porque las fronteras se hacen difusas y se minimizan las limitaciones para una sociedad global y de la inmediatez [20].

Entonces, las carreras de derecho deben pensarse en profesionales que adquieran competencias y habilidades para la resolución de conflictos, incorporando las tecnologías, en donde las universidades tendrán que dinamizar su transversalidad, junto con escuelas o facultades de ingeniería, programación o software, que a su vez se retroalimenten de las novedades jurídicas.

Con el desarrollo de las tecnologías modernas la esfera económica y social aprovecha las nuevas aplicaciones tecnológicas, afianzada por la presunción optimista del beneficio económico como principal motivación de los empresarios, enfrentados a los retos relacionados con la creación de prototipos de soluciones en cooperación con los científicos. Entonces, las ciencias sociales necesitan tanto la investigación sobre las relaciones hombre-máquina, y a su vez, reflexionarse en las teorías centradas en los aspectos sociales y éticos, donde los investigadores sociales deberán prestar atención a las implicaciones sociales de las consecuencias de aplicar los logros desarrollados por ingenieros y programadores, por la sensibilidad y preparación profesional con la que cambia el mundo y el estilo de vida de las personas [24] y los riesgos asociados a los desarrollos tecnológicos en ámbitos como la familia, las relaciones societarias, financieras, culturales y sociales.

De los efectos que trajo la pandemia por COVID-19, fue el crecimiento exponencial de usuarios en internet, en donde las instituciones de educación recurrieron al uso de correos y plataformas para garantizar el acceso a la educación. Sin embargo, el reconocimiento del acceso al servicio como Derecho Humano, se remonta a 2011, en que la Asamblea general de la Organización de las Naciones Unidas, declaró el acceso a la internet como derecho humano. Esto plantea entonces del reconocimiento no sólo del acceso a la red mundial sino de ciberderechos humanos que garanticen el desarrollo equilibrado, que en el espacio global y de la Sociedad de la información es menester observar el conjunto interdependiente de infraestructuras de las Tecnologías de Información y Comunicación [25].

#### *B. Adaptación Microcurricular, mesocurricular y macro curricular, y sensibilización del uso tecnológico*

Ha hecho carrera entre las Instituciones de Educación superior, Universidades y Centros de Investigación, la creación administrativa de currículos de acuerdo con las prerrogativas administrativas sean regionales o nacionales, como en el caso colombiano bajo los parámetros de la autonomía universitaria y los lineamientos del Ministerio de Educación Nacional, con la flaqueza evidenciada en numerosas materias, temas, asignaturas que están fuera los planes de estudio, o no son incorporadas por las decisiones organizaciones.

La transformación digital de una organización requiere incorporar tecnologías, crear o modificar procesos y disponer de las personas con las capacidades y habilidades adecuadas para dichos procesos y tecnologías. Es por ello que los mayores progresos han ocurrido en compañías que son nativas digitales, en contraste con las organizaciones más maduras. Modificar procesos, personas y tecnologías es muy difícil cuando están muy consolidadas en su cultura organizacional [26].

Con la incorporación de las TICs, las posibilidades educativas no se limitan únicamente a las ofertadas en un

entorno cercano, sino que se pueden elegir cursos y propuestas de formación impartidas remotamente, con un proceso de enseñanza-aprendizaje por medio de las TICs habilita la posibilidad de adaptación de la información a las necesidades y características de los usuarios, como disponer de nuevas herramientas para el proceso de la información y la comunicación, más recursos educativos interactivos y más información, pueden desarrollarse nuevas metodologías didácticas de mayor eficacia formativa. Además, ofrecen una mayor facilidad de desarrollo de habilidades de expresión escrita, gráfica y audiovisual, eliminando las barreras espacio-temporales [4].

De tal manera que las competencias de los abogados sean orientadas a la protección de datos, uso adecuado de herramientas tecnológicas para conservación de información sensible, como de evaluación de riesgos ante las vulnerabilidades que tiene la red.

La incompetencia inconsciente, configurada como las múltiples conductas inseguras en las cuales puede incurrir un abogado, cuando a través de canales de mensajes de datos y el manejo de nuevas tecnologías aparea consecuencias negativas ante el incumplimiento doloso por la deficiente o negligente conducta en el manejo de datos. Si bien la normatividad en cuanto a la protección de datos es abundante, puede plantearse de cara a las conductas disciplinarias obligaciones relativas en cuanto a la privacidad de la información [27].

Entonces, el fomento de currículos en los cuales, la participación activa y positiva del docente, junto con las tendencias del mercado y la educación, conlleva a crear rutas de colaboración interdisciplinaria entre unidades académicas de las universidades, para potenciar el uso de las nuevas tecnologías digitales.

Esta sensibilización se observa con recientes acontecimientos en los cuales la Rama Judicial de Colombia sufrió ataques cibernéticos originados por un ransomware que desde el 12 de septiembre de 2023 afectó los servicios informáticos y digitales para la Rama Judicial. La empresa IFX Networks Colombia SAS, proveedora de los servicios, debió desplegar un sinnúmero de actividades para recuperar la información [28], a fin de restablecer el servicio, como a su vez, devolver la credibilidad y confianza en la información almacenada.

#### *C. Fomento de la crítica analítica y teorización del docente en la disrupción tecnológica*

No es un secreto entonces, que el uso de la tecnología impone nuevas competencias para ser desarrollados por los docentes, como analíticas de datos, informática jurídica moderna, uso de inteligencia artificial para generar contenidos, entre otras tecnologías, las cuales son de libre acceso a través de Internet. A esto debe sumarse que, en toda aula de clase, incluso con el esfuerzo de las propias instituciones, las conexiones wifi e inalámbricas, como el uso de pantallas inteligentes y bases de datos, en uso crítico y analítico debe fomentarse en todo momento.

Por eso, competencias que aparentemente son de la órbita de las ingenierías o de la programación, como lo son el análisis de datos, aplicación de herramientas de las nuevas tecnologías, deben ser mejoradas en la pedagogía orientada por los educadores en Derecho, incluso, pensándose en mejorar la formación de docentes y no docentes, como reflejo de la calidad en la educación.

Aun así, el uso de la tecnología no es positiva en todos los eventos. Considérese la noción de neoliberalización tecnologizada de la universidad, que ha planteado hipotéticamente la multiplicación injustificadamente de la cantidad de trabajo, la burocratización y el control, extinguiendo recursos y tiempo para el pensamiento crítico y el cuestionamiento del statu quo, que fueron objetivos de la educación superior.

Así, considerando los beneficios que pueda brindar la inteligencia artificial brindar, no se subestima los riesgos potenciales para el disfrute de los derechos humanos, entre estos, el funcionamiento de la democracia, el acatamiento del Estado de derecho, para lo cual, un enfoque transversal propicie la adopción de principios generales que se compaginen con la innovación para que en un marco jurídico vinculante se asocien diseños y normas aplicables a las herramientas de inteligencia artificial [29]

El uso de la tecnología ha permitido mayores niveles de personalización, participación y democratización y una auténtica apertura de la institución a la sociedad, que junto con los investigadores, los docentes, los estudiantes, y el personal de la institución estén mejor conectados, y logren disfruten de un mayor potencial para crear y difundir un conocimiento más amplio, variado y complejo [3], pero que no debe dejar de lado, la reflexión del objeto que el derecho se ha propuesto estudiar, la conducta humana, que hoy se involucra con la tecnología.

Entonces, al plantearse la siguiente pregunta ¿Cómo puede ajustarse el uso del lenguaje a la disrupción tecnológica y la enseñanza del derecho?, la hipótesis que se plantea es que, a partir de la adaptación, proceso pasivo en el cual se espera la aparición de normatividad específica para el desarrollo de procesos de aprendizajes en el Derecho, es en escenario desalentador ante la situación legal, siendo paquidémica y retrasada. Más bien, la incorporación puede traer diferencias conceptuales, teóricas o incluso filosóficas, con lo cual, queda la integración de la disrupción tecnológica, es amplia lingüística y conceptualmente, enriquece la transversalidad, con lo cual, las ciencias sociales y las ingenierías se complementan en sus campos.

Finalmente, la producción normativa relacionada con la inteligencia artificial, está planteando entre sus retos los riesgos en las infraestructuras críticas, como lo son la educación y la formación profesional, la formación de mano de obra y generación de empleo, los servicios públicos y privados esenciales, como sanitarios, judiciales o bancarios, en sistemas de aplicación de la ley, migración y gestión de

fronteras como la impartición de justicia y procesos democráticos. Así, la evaluación para reducir dichos riesgos, requieren despliegue de herramientas y usos para mantener registros transparentes y precisos de información, como la garantía de supervisión humana, de tal forma que los ciudadanos tengan derecho a presentar quejas y a recibir explicaciones de las situaciones que afecten sus derechos cuando se involucren sistemas de IA de alto riesgo [30].

## VI. CONCLUSIONES

El impulso que recientemente han tenido las tecnologías de las comunicaciones y la información, plantean interesantes retos a las universidades, siendo centros de investigación y generación de conocimientos, como a su vez, formadoras de profesionales que deberán contar con suficientes habilidades y competencias para encarar los desafíos futuros.

Precisamente en cuanto a la formación de los abogados, las exigencias con cada vez de mayor calado, teniendo en cuenta los intereses que se disponen en los escenarios judiciales, como al interior de las propias firmas o estudios de abogacía. La interacción cada vez más profunda entre las competencias en el uso de la tecnología como la protección de los datos, la influencia en las decisiones, como en el desarrollo de los casos y el litigio, son campos en los cuales la preparación tanto técnica como humana son imprescindibles.

Hoy en día está de nuevo debates de antaño, con diferentes posturas filosóficas que buscan conciliar entre los avances tecnológicos y las dimensiones humanas. Esto vienen a confluir caminos en las universidades y centros de investigación, donde la imposición empresarial y negocial requieren avanzar a pasos gigantes para no caer en la obsolescencia contractual o negocial, y por otro lado, la creación y sustentación crítica de contenidos para la interiorización en las relaciones humanas y los riesgos que se afrontan.

De las categorías que se estudian, la disrupción tecnológica halla en el desarrollo y aplicación de la inteligencia artificial su mejor muestra. Si bien, la inteligencia artificial no es un descubrimiento reciente, su aplicación en diferentes ámbitos de la vida social, económica, política y educativa, está planteando debates de relevancia inusitada, incluso, llegando a regularse desde marzo de 2024 por el Parlamento Europeo, planteando los altos riesgos que pueden llegar a involucrarse en cuanto a la determinación de la voluntad de las personas, el Estado y las formas de participación democrática, como a su vez en la educación, administración de justicia, aplicaciones en la producción de alimentos, y en fin, cualquier campo de la vida.

Por ello, la comunicación e correlación trasversal en la formación de los futuros profesionales, sean abogados, ingenieros, médicos, economistas o cualquier área del conocimiento, deben reconocer los beneficios de la aplicación de inteligencias artificiales en los campos de conocimiento.

## VII. REFERENCIAS

- [1] C.L. Serje Jiménez. (2023, Diciembre). Los ODS y los abogados desde las facultades y programas de Derecho. [On Line]. Ámbito Jurídico. Bogotá D.C. Col. Disponible en [https://www.ambitojuridico.com/noticias/academia/los-ods-y-los-abogados-desde-las-facultades-y-programas-de-derecho?fbclid=IwAR2GuLLVjtJH4StIdghDxXvKX6WRzITrFX22u0ZCCCr\\_F18b3k\\_ENZ0weaM](https://www.ambitojuridico.com/noticias/academia/los-ods-y-los-abogados-desde-las-facultades-y-programas-de-derecho?fbclid=IwAR2GuLLVjtJH4StIdghDxXvKX6WRzITrFX22u0ZCCCr_F18b3k_ENZ0weaM).
- [2] R. Serrano Morales, C., Y. Silva Del Rosario, Redes sociales de Internet en la carrera Derecho, Universidad de Las Tunas. Opuntia Brava, [s. l.], v. 13, n. 3, p. 241–250, 2021. Disponible en: <https://search-ebscohost-com.crai-ustadigital.usantotomas.edu.co/login.aspx?direct=true&db=fap&AN=153905703&lang=es&site=eds-live&scope=site>. Acceso em: 2 fev. 2024.
- [3] J. Adell Segura, L. Castañeda Quintero, and F. Esteve Mon, “¿Hacia la Ubersidad? Conflictos y contradicciones de la universidad digital,” RIED. Revista Iberoamericana de Educación a Distancia, vol. 21, no. 2, p. 51, Apr. 2018, doi: <https://doi.org/10.5944/ried.21.2.20669>
- [4] R. Susskind. *El abogado del mañana Una introducción a tu futuro*. 1ra Edición en castellano. Las Rosas (Madrid – España): Wolters Kluwer, 2020. Pp. 77-79
- [5] J.M Sancho Gil, A. Ornellas, J. Arrazola Carballo. “La situación cambiante de la universidad en la era digital | RIED-Revista Iberoamericana de Educación a Distancia.” Vol. 21 Núm. 2, pp. 31-49. Jul, 2018. Acceso: 15 Mar. 2024 [Online]. Available: <https://revistas.uned.es/index.php/ried/article/view/20673>
- [6] C. Ferro Soto, A. I. Martínez Senra, y M. C. Otero Neira, «Ventajas del uso de las TICs en el proceso de enseñanza-aprendizaje desde la óptica de los docentes universitarios españoles», *Educat*, n.º 29, p. a119, jul. 2009. Disponible en <https://www.edutec.es/revista/index.php/edutec-e/article/view/451>
- [7] *Ministerio de Educación Nacional. Competencias TICS para el Desarrollo Profesional Docente*, 1ra ed., Bogotá D.C., Colombia, 2013., Disponible en: [https://www.mineduacion.gov.co/1759/articles-339097\\_archivo\\_pdf\\_competencias\\_tic.pdf](https://www.mineduacion.gov.co/1759/articles-339097_archivo_pdf_competencias_tic.pdf)
- [8] A. RONI. Hacia sociedades del conocimiento integradoras. El Correo de la UNESCO, 8, p. 10-11, illus.2007. Disponible en: [https://unesdoc.unesco.org/ark:/48223/pf0000189594\\_spa](https://unesdoc.unesco.org/ark:/48223/pf0000189594_spa)
- [9] CONSEJO EUROPEO Consejo Unión Europea. (2023, Enero). Inteligencia artificial. [On line]. <https://www.consilium.europa.eu/es/policies/artificial-intelligence/>
- [10] Comité de Representantes Permanentes. (2022, nov.). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión - Orientación general. [On line]. Disponible en <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/es/pdf>
- [11] A. E. De Giusti, “Transformación digital en educación superior: posibilidades y desafíos,” *TE & ET*, vol. no. 35, Sep. 2023, Available: <https://sedici.unlp.edu.ar/handle/10915/158703>. [Accessed: Feb. 03, 2024]
- [12] J. P. Pantoja Tecnologías disruptivas y derecho en Colombia : la nueva forma de ejercer la profesión. 2017. [online]. Disponible en: <http://hdl.handle.net/10554/44367>.
- [13] G. A. Quezada Castro, M. del P. Castro Arellano, and M. del P. Quezada Castro, “Inteligencia artificial y enseñanza del derecho: su incorporación durante la pandemia de la Covid-19,” *Revista Venezolana de Gerencia: RVG*, vol. 27, no. Extra 8, pp. 750–764, 2022, Available: <https://dialnet.unirioja.es/servlet/articulo?codigo=8890792>. [Accessed: Feb. 03, 2024]
- [14] M. Beuchot. *Hechos e interpretaciones hacia una hermenéutica analógica*. México. Fondo de Cultura Económica. 2016
- [15] F. M. Esteve Mon and M. Gisbert Cervera, “El nuevo paradigma de aprendizaje y nuevas tecnologías,” *REDU. Revista de Docencia Universitaria*, vol. 9, no. 3, p. 55, Dec. 2011, doi: <https://doi.org/10.4995/redu.2011.6149>
- [16] J. S. Ibáñez and V. I. M. Juarros, “Las diferentes concepciones de la universidad digital en Iberoamérica,” *RIED. Revista Iberoamericana de Educación a Distancia*, vol. 21, no. 2, 2018, Available: <https://www.redalyc.org/journal/3314/331455826007/html/>
- [17] B. Gros, “La caída de los muros del conocimiento en la sociedad digital y las pedagogías emergentes,” *Education in the Knowledge Society*, vol. 16, no. 1, pp. 58–68, 2015, Available: <https://www.redalyc.org/articulo.oa?id=535554757005>. [Accessed: Feb. 03, 2024]
- [18] M. Crespo and M. Aranzazu, “Participación estudiantil e inclusión digital en la universidad. Un estudio en contextos iberoamericanos,” vol. 20, no. 1, pp. 10–38, Jun. 2022, doi: <https://doi.org/10.14516/fde.957>
- [19] J. Adell Segura, L. Castañeda Quintero, and F. Esteve Mon, “¿Hacia la Ubersidad? Conflictos y contradicciones de la universidad digital,” RIED. Revista Iberoamericana de Educación a Distancia, vol. 21, no. 2, p. 51, Apr. 2018, doi: <https://doi.org/10.5944/ried.21.2.20669>
- [20] M. Suchacka, R. Muster, and M. Wojewoda, “Human and machine creativity: social and ethical aspects of the development of artificial intelligence,” *CS*, vol. 14, no. 2, pp. 430–443, Nov. 2021
- [21] L.A. Chavarro. “Discussion about Technological Determinism: From Impact to Mutual Influence | Sistemas y Telemática.” Vol. 2 No. 4, pp. 121–143. Jul, 2006. Acceso Mar, 2015, 2024 [Online]. Available: <https://doi.org/10.18046/syt.v2i4.938>
- [22] R. Heilbroner. *¿Son las máquinas el motor de la historia? Historia y determinismo tecnológico*. Madrid, Editorial Alianza, 1996.
- [23] M. Mascitti, “El Trialismo como un medio para promover la justicia dentro de la complejidad de la nueva era,” *Anales de la Cátedra Francisco Suárez*, vol. 56, pp. 123–154, Jan. 2022, doi: <https://doi.org/10.30827/acfs.v56i.18498>
- [24] J. Becerra, L. Cotino Hueso, C.B. García Vargas, M.E. Sánchez Acevedo, J. Torres Ávila, *La responsabilidad del Estado por la utilización de tecnologías de la información y la Comunicación*. Primera Edición. Lugar de publicación: Bogotá D.C: Colombia, 2015.
- [25] E. Chinkes and D. Julien, “Las instituciones de educación superior y su rol en la era digital. La transformación digital de la universidad: ¿transformadas o transformadoras?,” *Ciencia y Educación*, vol. 3, no. 1, pp. 21–33, Jun. 2019, doi: <https://doi.org/10.22206/cyed.2019.v3i1.pp21-33>
- [26] J. E. Gutiérrez Otiniano, “Proceso judicial y complementariedad paradigmática. Estudio de casos,” *Revista vasca de derecho procesal y arbitraje = Zuzenbide prozesala ta arbitraia euskal aldizkaria*, vol. 35, no. 2, pp. 139–153, 2023, Available: <https://dialnet.unirioja.es/servlet/articulo?codigo=8983404>. [Accessed: Feb. 04, 2024]
- [27] J.J. Cano, P. Gutiérrez, D. J. V. Blanco. “La Imposición de cibercompetencias en el ejercicio de la abogacía por cuenta de la protección de datos personales”. En *Derecho de las tecnologías y las tecnologías para el derecho*. Bogotá D.C: Ediciones Uniandes, 2022, cap. I, pp. 1-64.
- [28] Consejo Superior de la Judicatura. Acuerdo PSCJA23-12089 “Por el cual se suspenden términos judiciales en el territorio nacional”. Bogotá D.C. 2023. [En línea]. Available: <https://escuelajudicial.ramajudicial.gov.co/sites/default/files/PCSJA23-12089.pdf>
- [29] C.E. Consejo de Europa. “El Consejo de Europa y la inteligencia Artificial”. Enfoque Temático. 2023. Available: <https://edoc.coe.int/en/artificial-intelligence/11755-el-consejo-de-europa-y-la-inteligencia-artificial.html>
- [30] Y. Yakimova, J. Ojamo. Artificial Intelligence Act: MEPs adopt landmark law | News | European Parliament.”. Mar. 13, 2024. [Online]. Available: <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law>

## VIII. BIOGRAPHIES



**Jose Eduardo Valderrama Velandia.** Nace el 09 de Agosto de 1988. Abogado de la universidad Antonio Nariño. Graduado y titulado de la Maestría en Derecho con énfasis den Derecho Mercantil y de los Negocios Internacionales de la Universidad Sergio Arboleda, y Master Universitario de la Universidad de la Rioja en Derecho de la Propiedad Intelectual y de las Nuevas Tecnologías. Candidato a Doctor en Derecho Público por la Universidad Santo Tomás Seccional Tunja, en donde es coordinador del Módulo de Derecho Privado y docente de Pregrado y posgrado.

Ha sido docente catedrático y director de Programas de Derecho en Colombia. Conjuez del Tribunal Administrativo del Distrito Judicial de Tunja (Boyacá-Colombia)

# Engenharia da Paz na Era da Quarta Revolução Industrial: Moldando uma Nova Mentalidade no Ensino da Engenharia

1<sup>st</sup> Tania C. D. Bueno  
Instituto i3G  
Florianópolis, Brazil  
tania.bueno@institutoi3g.org

2<sup>nd</sup> Ramiro Jordan  
ISTEC, Inc. e University of New  
Mexico, USA  
rjordan@unm.edu

**Resumo**— Os sistemas de ensino de engenharia em todo o mundo estão atualmente numa fase de transformação, marcada por uma incerteza considerável decorrente da rápida ascensão da superinteligência computacional e enfrentando a destruição dos nossos habitats naturais e a escassez de recursos, violações da privacidade, iniquidade e desigualdade social, e conflitos crescentes. Em meio ao cenário transformador da Quarta Revolução Industrial, a Engenharia da Paz surge como uma nova mentalidade e um catalisador educacional que nos inspira a construir um ambiente além da sobrevivência, entrelaçando perfeitamente tecnologia, consciência social e inteligência emocional para promover a paz, a harmonia e o desenvolvimento sustentável. dentro das sociedades. A sinergia alcançada através da fusão de tecnologia, princípios de justiça social e inteligência emocional não só prepara os indivíduos para os desafios da nossa época tecnológica em evolução, mas também transmite uma perspectiva abrangente e inclusiva que transcende as fronteiras disciplinares. Esta mudança paradigmática não só reconhece as disrupções atuais, mas também antecipa as implicações futuras destas tecnologias disruptivas, garantindo que os engenheiros e todas as disciplinas não são apenas adaptáveis, mas também bem preparadas para responder às exigências desta era dinâmica. A Engenharia da Paz (PENG) defende a quebra dos silos acadêmicos existentes e o desenvolvimento de uma abordagem holística para trazer novas soluções para enfrentar os desafios globais. Este trabalho enfatiza a importância de compreender as nuances da paz e sistematiza três aspectos da educação PENG: o social, o tecnológico e o emocional. Ao assimilar técnicas e metodologias como Engenharia da Mente, Design Eticamente Alinhado (EAD) e Mindfulness, permite-se construir uma visão holística de paz. Esta visão representa um desafio complexo para a educação em engenharia, intrinsecamente entrelaçada na estrutura da dinâmica humana e social. A exploração e discussão abrangente deste conceito revela-se mais eficaz quando contextualizado nas esferas filosófica, sociológica e psicológica. Compreender a paz dentro deste quadro interdisciplinar aumenta a eficácia da abordagem desta questão intrincada e transformadora na educação em engenharia. O PENG considera em profundidade as consequências pretendidas e não intencionais, e dados confiáveis verificáveis que se traduzem em Conhecimento Acionável para a concepção de novas soluções e combate à desinformação.

**Termos de Indexação**— Engenharia da Paz, Ensino da Engenharia, Quarta Revolução Industrial, Mindfulness, Design Eticamente Alinhado, Engenharia da Mente, Dados confiáveis verificáveis, Conhecimento acionável.

## I. INTRODUÇÃO

O aumento da globalização impôs um modelo comportamental padronizado globalmente, arriscando a erosão dos valores fundamentais [1]. Esta mudança é particularmente visível no cenário em evolução do ensino de

engenharia, marcado por incertezas decorrentes de rápidos avanços tecnológicos, desafios ambientais, violações de privacidade, desigualdades e desigualdades sociais e conflitos crescentes. Os apelos à reforma dos currículos de engenharia estão a intensificar-se, defendendo uma abordagem multidisciplinar que integre pedagogias baseadas em evidências e mecanismos de aprendizagem orientados para resultados [2]. À medida que as instituições de engenharia se esforçam para se adaptar, seu foco principal é a criação de experiências de aprendizagem de qualidade que capacitem os alunos a cultivar habilidades essenciais, como pensamento crítico, resolução de problemas, aprendizagem ao longo da vida e trabalho em equipe eficaz [3]. Apesar do aumento da informação, nomeadamente facilitado pela Internet e pelos telefones celulares, não se seguiu necessariamente um aumento da sabedoria. Em vez disso, as ansiedades coletivas aumentaram, particularmente evidentes entre a população mais jovem, representando uma preocupação premente para a saúde global. O rescaldo da pandemia sublinhou esta questão, revelando uma sociedade não só fisicamente doente, mas também lutando com uma capacidade diminuída de criatividade [4]. Isto levanta uma questão crucial: em que trajetória estamos? Embora a tecnologia deva atuar como um catalisador para o avanço humano, paradoxalmente parece estar a distanciar-nos dos nossos valores fundamentais e queridos. O imperativo agora reside em recalibrar a nossa relação com a tecnologia e o planeta para garantir que ela sirva como um aliado no nosso crescimento coletivo, em vez de uma força que nos distancia da essência da nossa humanidade, esta foi a conclusão do Fórum Económico Mundial - WEF, no seu relatório de riscos globais [4]. Esta evolução responde não só às tendências em mudança nos requisitos da indústria, mas também às crescentes preocupações relativas ao desenvolvimento sustentável e às alterações climáticas. Portanto, premissas importantes para a Engenharia da Paz são “Um planeta, um ambiente, uma chance”, Dados confiáveis verificáveis e Conhecimento acionável [5]. Neste contexto, o conceito de Engenharia da Paz (PENG) surge como um princípio orientador, defendendo uma abordagem holística que não apenas aborde a proficiência técnica, mas também enfatize a promoção de uma relação harmoniosa entre tecnologia, sociedade e meio ambiente [6][7][8][9]. Apresentar estes conceitos aos estudantes de engenharia, entrelaçando a justiça aos efeitos da tecnologia, muda-nos de uma configuração sócio tecnológica centrada na guerra para uma agenda global de engenharia da paz. Esta mudança transformadora visa nutrir engenheiros educados para remodelar o seu mundo para a paz e a justiça [3]. A PENG está mudando a mentalidade de todas as disciplinas e criando e verificando dados confiáveis para P&D, atividades



empreendedoras, design, política, finanças, saúde e muitos outros campos. As convulsões globais exigem uma mudança de paradigma, uma nova mentalidade, na engenharia e no ensino de outras disciplinas. Em meio às incertezas da Quarta Revolução Industrial, o PENG surge como um catalisador para promover a harmonia. Este trabalho apresenta uma nova abordagem para o desenvolvimento da Engenharia da Paz, enfatizando uma compreensão abrangente da paz. A paz, como uma questão complexa profundamente enraizada nas dinâmicas humanas, ambientais e sociais, ganha eficácia através da exploração em contextos filosóficos, sociológicos e psicológicos. A fusão da tecnologia, dos princípios de justiça social e da inteligência emocional não só prepara os indivíduos para os desafios da época tecnológica, mas também transmite uma perspectiva holística que transcende as fronteiras disciplinares. Esta mudança paradigmática não só reconhece as inovações, mas antecipa as implicações futuras de tecnologias como a inteligência artificial, a blockchain e a computação quântica, garantindo que os engenheiros não sejam apenas adaptáveis, mas também bem preparados para as exigências desta era dinâmica.

## II. ENGENHARIA DA PAZ COMO UM NOVO MINDSET

Valores como a sustentabilidade ambiental e a responsabilidade social tornam-se cada vez mais cruciais no contexto da Quarta Revolução Industrial. Ao enquadrá-lo como uma revolução de valores, há um apelo à integração de práticas sustentáveis nos avanços tecnológicos, garantindo que o progresso não seja apenas eficiente, mas também ambiental e socialmente responsável. O PENG complementa esta procura, promovendo uma compreensão abrangente da interligação entre as soluções de engenharia e os seus impactos sociais mais amplos, incluindo políticas e finanças.

O panorama da formação profissional académica está a sofrer uma profunda transformação, procurando alinhar-se com as necessidades dinâmicas de aprendizagem dos estudantes da era moderna. A engenharia da paz, como parte integrante desta transformação, reconhece a importância de nutrir uma mentalidade que vai além da especialização técnica, colocando ênfase em considerações éticas, sensibilidade cultural e um compromisso com a responsabilidade social [6].

Os desafios éticos no âmbito da engenharia surgem de várias fontes, incluindo pressões comerciais, prazos rigorosos, falta de sensibilização e uma preferência por ganhos a curto prazo em detrimento da sustentabilidade a longo prazo. Em resposta, o conceito de PENG surge como uma solução robusta para abordar riscos multifacetados, com o objetivo de infundir valores humanos na engenharia e em outras disciplinas dos profissionais.

A Engenharia da Paz capacita os alunos com a capacidade de navegar pelas intrincadas dinâmicas sociais e políticas. Nosso estudo apresenta uma estrutura capacitadora que desenvolve habilidades sociais, tecnológicas e emocionais, promovendo a percepção do problema, a qualidade e a criatividade. Esta abordagem envolve ativamente as partes interessadas e promove a colaboração interdisciplinar para adotar uma perspectiva holística de engenharia que reconhece a importância dos valores humanos.

A nascente comunidade de engenharia da paz precisa de

construir o ecossistema para garantir o seu sucesso a longo prazo. Os parceiros académicos e institucionais podem fornecer as informações necessárias para se envolver neste trabalho transformador.

Desde 2018, a Universidade do Novo México, os Laboratórios Nacionais Sandia, o Consórcio de Engenharia da Paz (PEC) e o Bioma Engenharia da Paz têm colaborado para apresentar a Engenharia da Paz a um público mais amplo. O Consórcio de Engenharia da Paz [7], dedicado ao avanço do conhecimento, das ferramentas e do talento, serve como uma estrutura valiosa para instituições que procuram conceber e implementar os seus próprios programas de Engenharia da Paz. Para avançar a Engenharia da Paz na Educação em Engenharia, são propostas duas abordagens principais:

1. Expandir e melhorar os currículos: As instituições educacionais devem ampliar os currículos existentes para formar engenheiros proficientes não apenas em habilidades técnicas, mas também bem versados em disciplinas relevantes, como campos STEM, ciências sociais, artes e disciplinas aplicadas como diplomacia, saúde, direito e negócios. Esta educação abrangente promove engenheiros que não são apenas tecnicamente proficientes, mas também cidadãos globais compassivos e socialmente responsáveis.

2. Estabelecer um Corpo de Conhecimento em Engenharia da Paz (BoK): Desenvolver um BoK básico para a educação e prática da Engenharia da Paz, servindo como um guia para as instituições criarem programas de Engenharia da Paz. Colabore com organizações como a ABET para credenciar esses programas, garantindo conteúdo transformador que enfatize a ética, a consciência social e as considerações ambientais. Este BoK permite que os engenheiros compreendam as consequências intencionais e não intencionais de suas soluções.

Existem instituições e centros de investigação que representam uma gama de abordagens à Engenharia da Paz, combinando conhecimentos de engenharia com outras disciplinas para enfrentar desafios complexos relacionados com a paz, conflitos e desenvolvimento. É importante observar que o campo está evoluindo rapidamente e novas iniciativas estão surgindo. O surgimento da engenharia da paz como um campo e uma mentalidade distintos é uma resposta ao reconhecimento de que os princípios, tecnologias e práticas de engenharia podem contribuir significativamente para os esforços de construção da paz e para abordar as causas profundas dos conflitos. Embora não exista um evento específico que tenha marcado o início da Engenharia da Paz, o seu desenvolvimento remonta a vários fatores históricos e à crescente consciência do papel da engenharia na promoção da paz e do desenvolvimento sustentável.

No geral, o surgimento da engenharia da paz reflete uma mudança de paradigma no pensamento da engenharia, reconhecendo o potencial da engenharia para ir além do desenvolvimento tradicional de infraestruturas e abordar os fatores sociais, económicos e ambientais subjacentes que contribuem para os conflitos. Ao alavancar a experiência e a tecnologia em engenharia, a engenharia da paz visa contribuir para o desenvolvimento sustentável, a resolução de conflitos

e a promoção da paz e da justiça social a nível mundial. O campo emergente da engenharia da paz e do trabalho para definir as habilidades desejadas, as melhores práticas e as questões de pesquisa necessárias para o futuro engenheiro global.

Os participantes trabalharam para definir o ecossistema de engenharia da paz, para identificar oportunidades de crescimento e para compreender os padrões de dados da paz [7]. A Engenharia da Paz é um campo relativamente novo e emergente que se concentra na aplicação de princípios e metodologias de engenharia para promover a construção da paz, a resolução de conflitos e o desenvolvimento sustentável. Embora o campo da engenharia da paz ainda não esteja difundido, existem algumas universidades e instituições que começaram a oferecer programas ou iniciativas relacionadas com a engenharia da paz. Abaixo está uma lista de algumas instituições acadêmicas que criaram um programa de Engenharia da Paz:

- Universidade Drexel (Filadélfia, EUA).
- Universidade Villanova (Villanova, EUA).
- Universidade de San Diego (San Diego, EUA).
- Universidade de Saint Thomas (St. Paul Minnesota, EUA)
- Universidade de Coventry (Coventry, Reino Unido).
- Universidade do Novo México (Albuquerque, EUA)

O Consórcio de Engenharia da Paz é composto por muitas instituições acadêmicas em todo o mundo, pela indústria e pelos Laboratórios Nacionais dos EUA. O Consórcio procura parceiros para participar e fazer a diferença globalmente.

#### A. *Estudo de Caso: Peace Engineering Minor na Universidade do Novo México*

De 12 a 26 de novembro de 2018, a Escola de Engenharia da Universidade do Novo México (UNM-SoE), em colaboração com o Consórcio Ibero-Americano de Ciência e Tecnologia (ISTEC), o Global Engineering Deans Council (GEDC) e, o A Federação Internacional de Sociedades de Educação em Engenharia (IFEES) organizou a Primeira Conferência Global de Engenharia para a Paz (WEEF-GEDC 2018). Naquela época, a Engenharia da Paz era definida como a aplicação intencional de princípios de ciência, tecnologia, cultura e engenharia em nível de sistema para promover e apoiar diretamente as condições para a paz. Seu trabalho é direcionado diretamente para um mundo onde a prosperidade, a sustentabilidade, a equidade social, o empreendedorismo, a transparência, a voz e o envolvimento da comunidade, a ética, a equidade e uma cultura de qualidade prosperem [5].

Como resultado da conferência WEEF-GEDC 2018, a UNM-SoE criou um Minor de Engenharia da Paz aberto não apenas para as áreas de Engenharia, mas para todas as disciplinas. O PENG é transdisciplinar, elimina silos acadêmicos e inclui tópicos relevantes em diferentes disciplinas. Engenharia da Paz é a aplicação dos princípios da Ciência, Tecnologia, Engenharia, Artes e Matemática (STEAM), práticas sustentáveis, sensibilidade cultural e inovação para promover e apoiar a paz, e seu perfil está aumentando entre instituições em todo o mundo [9].

#### B. *Objetivos e Metas do Programa Minor*

O objetivo do Minor é formar profissionais “inteligentes nas ruas” de todas as disciplinas que possam se adaptar e girar rapidamente com base no contexto em que estão inseridos. Ou seja, queremos educar cidadãos globais “inteligentes nas ruas”. Os alunos devem estar abertos para aprender e adotar as competências digitais em constante mudança (ex. análise de dados), devem ser resilientes, engenhosos, éticos, diplomatas e ter o talento básico em políticas, finanças e gestão de projetos. Muito importantes são o pensamento sistêmico e a capacidade de comunicação social para funcionar em todas as disciplinas e culturas. Uma conscientização e uma ferramenta são dados confiáveis e verificáveis. Dados confiáveis são essenciais na tomada de decisões [5][10] que podem ter resultados negativos ou positivos. Muitas decisões impactantes estão sendo tomadas na ausência de ciência; assim, a replicabilidade não é possível, na ciência a observação dos dados/resultados é quem decide.

O Peace Engineering Minor tem 15 horas de crédito. É composto por dois cursos obrigatórios de 3 horas de crédito: ENG 220 - Engenharia, Negócios, Sustentabilidade, Ética, Sociedade e Justiça, Equidade, Diversidade, Acessibilidade, Inclusão (JEDAI) e ENG 320 - Design Thinking, Métricas, Analytics, IA, ML, dados confiáveis e JEDAI. As 9 horas restantes são eletivas de qualquer disciplina que devem ser pré-aprovadas pelo corpo docente de Engenharia da Paz e pelo Consórcio de Engenharia da Paz. Também deve estar em conformidade com as diretrizes da ABET. Estamos abertos a expandir a oferta de cursos para menores. O PENG Minor também está colaborando com membros do Peace Engineering Consortium (PEC) para conteúdo, apresentações, palestras convidadas, discussões e compartilhamento de projetos. Os cursos utilizam um formato de ensino em equipe para promover a compreensão dos alunos sobre a interação da prática da engenharia com os negócios e a sociedade. Os alunos aprendem sobre inovação, empreendedorismo, padrões globais e ética profissional. Redações comerciais e técnicas são incorporadas ao longo do curso. O curso convida pessoas de comunidades profissionais e globais afins para apresentar palestras e liderar discussões. Os objetivos do curso incluem apresentar aos alunos o amplo contexto de todas as práticas disciplinares, tanto nacional como internacionalmente, promovendo habilidades e atitudes necessárias para o sucesso no local de trabalho moderno, compreendendo as questões éticas que os engenheiros praticantes podem enfrentar e melhorando as habilidades de comunicação técnica.

Os possíveis tópicos abordados são os Grandes Desafios da Academia Nacional de Engenharia para o Século 21, os 17 Objetivos de Desenvolvimento Sustentável (ODS) das Nações Unidas, o empreendedorismo, a inovação na prática da engenharia, o pensamento de design e o trabalho em equipe no local de trabalho da engenharia moderna, padrões internacionais de engenharia, consciência global - ness, Indústria 4.0, ética, transparência, justiça social, dados confiáveis e comunicação de engenharia com uma comunidade não técnica.

No semestre de agosto de 2022, outono de 2022, o número de alunos do curso ENG 220 teve que ser limitado a 50 alunos devido ao crescente interesse pelo curso. Os alunos trabalharam em equipes com foco em alguns ODS da ONU. O projeto final do curso foi um Painel de Engenharia da Paz online para o Estado do Novo México. O objetivo do painel é fornecer dados confiáveis verificáveis e informar de maneira simples ao cidadão médio do Estado do Novo México. Os temas para o dashboard selecionados foram Água, Qualidade do Ar, Saúde e Finanças no Médio Rio Grande. Colete dados confiáveis verificáveis, processe-os e apresente as informações ao cidadão comum para que ele tome sua própria decisão. O objetivo não é influenciar, mas sim desmistificar as estatísticas, as competências digitais necessárias para obter os dados e visualizá-los, para ensinar o cidadão a tomar a sua própria decisão sobre estas questões. Ou seja, a cidade, o condado, o estado e o governo federal dos EUA estão fazendo o que falam para todos os cidadãos do Novo México. Ou seja, se os recursos dedicados a essas questões estão sendo bem investidos e produzindo os resultados corretos, há transparência [11].

O PENG Minor está quebrando os silos que existem na academia e afeta um número maior de futuros cidadãos globais de diferentes disciplinas. Os membros do Peace Engineering Consortium ajudam a facilitar palestras, palestras, workshops e capacitar os alunos com diferentes perspectivas e consciência do contexto. Além disso, alterações ou revisões curriculares são trazidas pelo Consórcio de Engenharia da Paz; temos um processo de revisão por pares em vigor. Claramente, o aumento do número de alunos matriculados nos três primeiros semestres deste programa demonstra que o PENG Minor é um sucesso.

### III. ESTRATÉGIAS PARA ENSINAR ENGENHARIA DA PAZ

Neste empreendimento, expomos a sinergia de três paradigmas, formando uma estratégia robusta em três frentes, preparada para remodelar o cenário educacional para engenheiros e profissionais em diversos domínios.

Para forjar um engenheiro da paz, o imperativo reside no cultivo de competências num espectro triplo – abrangendo competências sociais, tecnológicas e emocionais. No domínio das competências sociais, a capacidade de negociar, mediar e reconciliar ocupa um lugar central, servindo como uma abordagem preventiva e focada na resolução de conflitos. Uma compreensão ética da diversidade social e ambiental é considerada essencial, promovendo uma cultura de paz baseada em princípios de justiça social. Pilares como a tolerância, o respeito pela diversidade, a igualdade de gênero, a não violência, a equidade e a participação dos cidadãos devem sustentar todos os projetos criativos idealizados pelos estudantes.

Voltando-se para as competências tecnológicas, o PENG procura construir comunidades resilientes e promover a compreensão intercultural através da tecnologia. Em resposta aos riscos contemporâneos como a inteligência artificial, os avanços tecnológicos, a guerra biológica, a extinção de espécies, as alterações climáticas e as crises de saúde globais, a Engenharia da Paz surge como uma resposta robusta. O

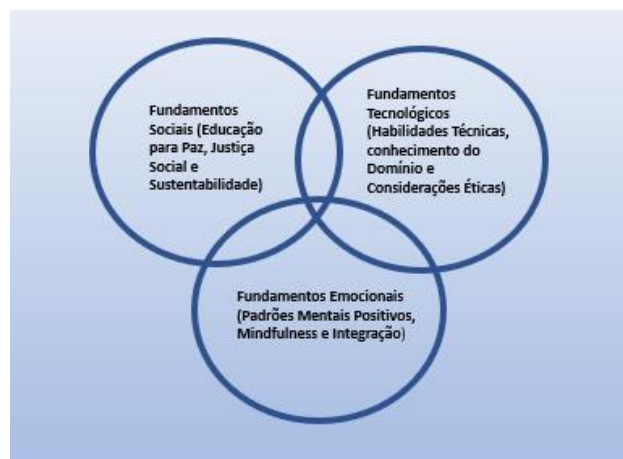


Fig. 1. Fundamentos tridimensionais da Engenharia da Paz.

objetivo é infundir valores humanos na engenharia e em outras práticas profissionais, capacitando os profissionais a contribuir não apenas com soluções técnicas avançadas, mas também com soluções alinhadas ao bem-estar global.

A terceira faceta deste quadro é emocional, com a Engenharia da Paz a abraçar uma mentalidade positiva aplicável ao ensino (ver seção IV), ao processo criativo e à execução de projetos. Este padrão mental positivo, alcançável através de diversas técnicas, visa a harmonia entre a coerência do coração e um estado mental definido como Paz.

Uma mentalidade positiva e otimista abre os alunos a novas ideias, promovendo um ambiente propício à inspiração, criatividade e inovação. As práticas de respiração consciente são frequentemente utilizadas para cultivar a calma e a clareza mental, permitindo uma melhor concentração no momento presente e criando um terreno fértil para o pensamento criativo e a inspiração. Neste ambiente mental descontraído e aberto, a inspiração floresce, ampliando as possibilidades de contribuições significativas para a promoção da paz e do bem-estar global.

No domínio da educação, a base da Engenharia da Paz assume a forma de uma tríade dinâmica, encapsulando três dimensões indispensáveis que vão além dos paradigmas tradicionais, oferecendo uma abordagem abrangente e transformadora. Uma frase de efeito para a Engenharia da Paz é “Um planeta, um ambiente, uma chance”, dados confiáveis verificáveis e conhecimento acionável que desafiam a rota tradicional e estabelecida pela qual os indivíduos entram e progredem nas carreiras de engenharia [5]. É imperativo recalibrarmos a nossa abordagem para responder às exigências de um cenário contemporâneo caracterizado pela transformação digital, diversidade, globalização e mudanças rápidas.

A abordagem educacional à Engenharia da Paz compreende três dimensões fundamentais (ver figura 1, acima):

1. **Fundamentos Sociais** (Educação para a Paz, Justiça e Sustentabilidade): Fundamental entre estas, está intrinsecamente tecida com princípios de justiça social e ética, promovendo abordagens colaborativas, inclusivas e sustentáveis para harmonizar a dinâmica social e dissuadir proativamente os conflitos.

**2. Fundamentos Tecnológicos** (Habilidades Técnicas, Conhecimento de Domínio e Considerações Éticas): Especialmente pertinente no cenário tecnológico contemporâneo, o ensino de engenharia desempenha um papel fundamental ao incutir uma consciência das implicações éticas da tecnologia, combatendo a potencial desumanização associada à automação total, artificial inteligência, blockchain e computação quântica. É extremamente importante e vital que todas as profissões e profissionais desafiem a desinformação através da utilização e proteção de Dados Confiáveis e Verificáveis. Esta declaração apela a uma nova abordagem à resolução de problemas: uma que enfatize a colaboração e a integração de conhecimentos transdisciplinares e programas educativos. Defende a aplicação simultânea de soluções tecnológicas juntamente com o reforço da ética, da política e da consideração pelos sistemas vivos. A Engenharia da Paz aproveita e atua com base em dados confiáveis e verificados para orientar suas ações.

**3. Fundamentos Emocionais** (Padrões Mentais Positivos, Mindfulness e Integração): Esta base torna-se uma consideração vital, incentivando os estudantes de engenharia a desenvolver um profundo respeito pelas intrincadas consequências de suas ações através da observação passiva e da não intervenção. Esta abordagem consciente serve como um catalisador para mitigar os impactos económicos, sociais e ambientais, enfatizando a responsabilidade dos futuros engenheiros na elaboração de soluções que reflitam uma compreensão mais profunda da interligação entre a humanidade e o mundo natural.

Ensinar engenharia para a paz a estudantes de engenharia pode ser uma tarefa desafiadora, mas é crucial enfatizar que existem várias abordagens eficazes que podem ser adotadas. Aqui estão algumas sugestões:

- Introduzir o conceito de Engenharia da Paz no início do curso: É essencial que os alunos compreendam que a engenharia não se limita à concepção de estruturas físicas, mas também pode contribuir para a resolução de conflitos e a promoção da paz. Os professores podem introduzir este conceito nas aulas iniciais do curso para incutir uma perspectiva válida da engenharia.

- Incluir Engenharia para a Paz no currículo de engenharia: Os professores podem incorporar cursos dedicados que cubram tópicos de Engenharia para a Paz, como conflitos armados, direitos humanos, justiça social, sustentabilidade e desenvolvimento humano. Isso proporcionará aos alunos uma compreensão estruturada e aprofundada do assunto.

- Promover atividades extracurriculares relacionadas com a engenharia da paz: Incentivar os alunos a participarem em atividades extracurriculares, tais como grupos de estudo ou projetos relacionados com a engenharia da paz, pode melhorar as suas competências na resolução de conflitos, negociação e comunicação. Também lhes permite aplicar conceitos teóricos em cenários práticos.

- Promover a investigação sobre Engenharia da Paz: Os professores podem inspirar os alunos a realizar pesquisas sobre engenharia da paz e a escrever trabalhos académicos

sobre o assunto. Isso promove o pensamento crítico, incentiva o pensamento independente e aprofunda a compreensão do tema.

- Convide especialistas para palestras e aulas: Trazer especialistas que estejam ativamente envolvidos no campo da engenharia da paz para ministrar palestras ou ministrar aulas pode fornecer aos alunos insights valiosos e perspectivas do mundo real. Isso os expõe a aplicações práticas da engenharia da paz e a potenciais oportunidades de carreira.

A evolução do ensino de engenharia através da Engenharia da Paz encapsula uma fusão harmoniosa de tecnologia, consciência social e inteligência emocional. Esta abordagem visionária não só prepara os estudantes para os desafios de um mundo em rápida mudança, mas também cultiva uma nova geração de engenheiros que não são apenas proficientes nos seus domínios técnicos, mas também são conscientes, socialmente conscientes e capazes de contribuir significativamente para a melhoria da sociedade. Isto também é válido para quaisquer disciplinas existentes e novas a serem criadas para enfrentar os desafios globais.

#### IV. INTEGRANDO MINDFULNESS, ENGENHARIA DA MENTE E EAD AO FRAMEWORK

Segundo a OCDE [13], as futuras escolas e currículos devem desenvolver competências para a vida, cultivar competências como autoconsciência, autorregulação, resiliência, tomada de perspectiva, empatia, gratidão, atenção plena e liderança. Entre as inúmeras estratégias exploradas, a incorporação de práticas de meditação e atenção plena emergiu como um farol de esperança para muitos que procuram uma abordagem holística ao bem-estar mental. A análise da teoria e da literatura indica que a atenção plena é promissora na promoção de várias vantagens em diversas populações. Esses benefícios abrangem o desenvolvimento de competências intrapessoais e interpessoais, como o aumento da autorregulação, da resiliência, do bem-estar e da empatia. O panorama da investigação na era pós-pandemia testemunhou um aumento de projetos dedicados a compreender e abordar o impacto psicológico destes tempos sem precedentes. A mudança abrupta para o trabalho remoto e a implementação de modalidades de aprendizagem virtual alteraram significativamente a dinâmica de como as pessoas se envolvem no trabalho e nos estudos. Estas mudanças trouxeram uma série de desafios, incluindo níveis elevados de stress, fronteiras confusas entre a vida pessoal e profissional e a necessidade de estratégias inovadoras para melhorar o bem-estar mental.

No contexto do PENG, as considerações éticas são fundamentais. O uso responsável e sustentável de conhecimentos e habilidades de engenharia é parte integrante da disciplina. Tópicos como ética profissional, práticas de engenharia responsáveis e sensibilidade cultural são cruciais para os alunos, garantindo uma compreensão das dimensões éticas e promovendo uma perspectiva holística de engenharia que reconhece a importância dos valores humanos no seu trabalho na Engenharia da Paz.

A falta de atenção a este tópico pode resultar em consequências não intencionais que afetam negativamente os valores humanos, como:

- Negligência das comunidades, tais como danos ambientais, deslocamento de comunidades ou perda de meios de subsistência.

- Questões éticas como violações de privacidade, preconceitos ou efeitos discriminatórios, se não considerarem valores humanos como justiça, equidade e inclusão.

- Negligência das questões de segurança, que podem levar a perigos, acidentes ou outros riscos para a saúde e o bem-estar humanos.

- Falta de empatia com o usuário; Inadequação em colocar o usuário no centro; Falha em priorizar a experiência do usuário.

#### A. *Mindfulness*

Anos de pesquisa mostram benefícios da prática regular da atenção plena em diversos setores da sociedade e apesar da extensa investigação que demonstra estas vantagens, permanece uma lacuna notável na exploração dos potenciais intersecções entre Mindfulness e o campo da engenharia [14]. Grandes corporações como Google, Cisco, P&G e Facebook adotam o treinamento de Mindfulness para aumentar a criatividade, a inteligência emocional e o bem-estar entre os funcionários [15]. Adaptando estas práticas às equipes de engenharia, as empresas devem explorar como o Mindfulness melhora o pensamento divergente, crucial no design técnico. Uma abertura consciente, e não apenas de atenção, pode desencadear mentalidades inovadoras. Neste contexto, o reconhecimento da eficácia das pausas cerebrais, também chamados de Brain Breaks, assumiu um novo nível de importância. Pausas cerebrais, pausas curtas ou atividades destinadas a proporcionar alívio mental e aumentar o foco tornaram-se ferramentas essenciais para enfrentar os desafios colocados pelo atual cenário global [1]. As práticas de Mindfulness oferecem um meio poderoso para melhorar a colaboração e a comunicação entre estudantes de engenharia [14]. O envolvimento nestas práticas dota os indivíduos da capacidade de apreciar diversos pontos de vista e facilita a troca eficaz de conhecimentos. Além disso, a atenção plena cultiva foco e concentração aprimorados, permitindo que os alunos se aprofundem em seus estudos e contribuam com mais precisão e perspicácia.

Entretanto, a essência da atenção plena enfrenta o risco de diluição devido à sua excessiva comercialização e mercantilização. Esta tendência surge em parte da percepção da atenção plena como apolítica, levando a uma relutância em aprofundar a investigação moral e considerar impactos sociais mais amplos. Há uma suposição comum de que o comportamento ético emergirá naturalmente da prática ou através da incorporação da bondade e da compaixão pelos professores, ou talvez através da autodescoberta. No entanto, reduzir a atenção plena a uma mera técnica para vários fins instrumentais simplifica excessivamente o seu potencial, promovendo a crença errada de que transformações éticas significativas surgirão automaticamente ao “prestar atenção ao momento presente” de uma forma “sem julgamento”. Na realidade, um foco excessivo na “consciência sem julgamento” pode prejudicar, em vez de aumentar, a inteligência moral. A verdadeira atenção plena envolve reflexão crítica e envolvimento ativo com considerações

éticas, em vez de aceitação passiva ou evitação de julgamento.

Esta noção está alinhada com o conceito de Engenharia da Paz (PENG), que necessita de uma abordagem multidimensional que abranja aspectos técnicos juntamente com dimensões sociais, culturais, éticas e ambientais mais amplas do bem-estar humano. A Engenharia da Paz representa uma mudança de paradigma onde os aspectos emocionais e espirituais são integrantes do processo de aprendizagem. Incorpora uma mentalidade positiva aplicável no ensino, nos processos criativos e na execução de projetos, promovendo a transformação nas mentes e nos corpos de alunos, professores e profissionais. Abraçar este padrão mental positivo envolve o emprego de várias técnicas para harmonizar a coerência do coração com um padrão mental definido pela Paz.

#### B. *Engenharia da Mente*

A integração de questões éticas no desenvolvimento de projetos que visam o desenvolvimento da paz por engenheiros pode ser desenvolvida através da metodologia Engenharia da Mente [18] (ver Tabela 1). Onde, a equipe pode identificar os principais conceitos e fontes utilizados na avaliação e seleção de domínios para projetos PENG. Em seguida, a equipe chegou a um acordo quanto aos critérios estratégicos estabelecidos pelas questões de diversidade e sustentabilidade. Os inventários de conteúdo, processos e pessoas foram realizados seguindo as premissas de compartilhamento de conhecimento, visualização e definição de relevância, e seus desenvolvimentos podem ser descritos por um vocabulário controlado. Este quadro deve ser implementado nos próximos projetos de Engenharia da Paz para avaliar a sua eficácia tangível. Aplicações anteriores deste framework foram em projetos de apoio à decisão envolvendo IA. Esses desenvolvimentos demonstraram a capacidade de facilitar a integração duradoura de equipes proficientes e garantir a manutenção contínua e o aprimoramento do conhecimento dentro destes sistemas baseados em conhecimento [17]. Incutir ética na engenharia exige uma abordagem holística que transcenda meros acréscimos ao currículo. Portanto, adotamos a metodologia como parte integrante de nossos estudos. EAD [16] e Engenharia da Mente [18] são implantados em vários desenvolvimentos de IA e aproveitam a sabedoria coletiva de engenheiros e especialistas no assunto.

A metodologia Engenharia da mente é desenvolvida por três premissas: 1. Compartilhamento de Conhecimento; 2. Visualização; 3. Definição de Relevância. Em geral, são feitos quatro tipos de inventários: processos, tecnologia, conteúdo e pessoas. O capital humano, a missão, as metodologias, as tecnologias e os conhecimentos disponíveis na instituição são identificados buscando motivação, flexibilidade, versatilidade, adaptabilidades especializadas e usuários relacionados ao contexto. Desses inventários surge o mapeamento conceitual de processos, tecnologias, conteúdos e pessoas. Os mapas de conteúdo são a base dos engenheiros de ontologias, mas os mapas de processos, tecnologias e pessoas são os que definem a relevância e a coerência das relações ontológicas. Nesta fase é desenvolvido

o vocabulário controlado do domínio da Engenharia da Paz. O vocabulário controlado é separado em domínios (temas e subtemas). As ontologias são organizadas em contextos pertencentes ou não a um domínio ou subdomínio. As definições de domínio estão essencialmente relacionadas com os resultados esperados do sistema. Os domínios formam uma árvore hierárquica, agrupando os assuntos de forma a facilitar a análise das informações da base de conhecimento [17].

### C. *Design Alinhado Eticamente - EAD*

Ethically Aligned Design (EAD) [16] é uma estrutura desenvolvida pelo Instituto de Engenheiros Elétricos e Eletrônicos (IEEE) que visa orientar o desenvolvimento de tecnologias emergentes com foco em considerações éticas. Fornece um conjunto de princípios e diretrizes para garantir que a tecnologia seja concebida, implementada e utilizada de uma forma que se alinhe com os valores humanos, respeite os direitos individuais e promova o bem-estar social. A importância da EAD para os estudantes de engenharia reside no fato de serem eles os futuros criadores e inovadores da tecnologia. Aqui estão alguns motivos pelos quais o EAD é importante para estudantes de engenharia:

- **Responsabilidade Ética:** Os engenheiros têm a responsabilidade de considerar os potenciais impactos sociais, culturais e ambientais dos seus projetos.
- **Design Centrado no Usuário:** A EAD enfatiza a importância de projetar tecnologia tendo os usuários finais em mente. Ao considerar as necessidades, valores e preferências de diferentes grupos de usuários, os estudantes de engenharia podem criar soluções mais inclusivas e fáceis de usar que atendam às diversas necessidades da sociedade.
- **Responsabilidade e Confiança:** O EAD ajuda os estudantes de engenharia a compreender a importância de construir confiança por meio de práticas de design transparentes e responsáveis, garantindo que a tecnologia que eles criam seja confiável, segura e respeite a privacidade.
- **Mitigação de preconceitos e discriminação:** Tecnologias emergentes como a inteligência artificial (IA) têm o potencial de amplificar preconceitos existentes e discriminar determinados grupos. O EAD incentiva os estudantes de engenharia a estarem atentos aos preconceitos durante o processo de design e a desenvolver estratégias para identificar, mitigar e eliminar preconceitos em algoritmos e sistemas.
- **Sustentabilidade a Longo Prazo:** A EAD promove uma visão holística do design tecnológico, considerando a sua sustentabilidade a longo prazo e o impacto ambiental. Os estudantes de engenharia podem aprender a desenvolver soluções que sejam ecologicamente corretas, eficientes em termos energéticos e que promovam práticas sustentáveis.

Ao integrar os princípios da EAD em sua educação e prática, os estudantes de engenharia podem contribuir para o desenvolvimento e implantação responsável da tecnologia, causando um impacto positivo na sociedade e ao mesmo tempo mantendo padrões éticos [17]. Ele os equipa com as ferramentas e a mentalidade necessárias para enfrentar dilemas éticos complexos e projetar soluções que beneficiem indivíduos e comunidades como um todo no contexto da

Engenharia da Paz. Estas premissas aplicadas ao PENG permitirão a integração de questões éticas no desenvolvimento de projetos que visam o desenvolvimento da paz pelos engenheiros (ver Tabela 1, na próxima página).

A equipe consegue identificar os principais conceitos e fontes utilizados na avaliação e seleção de domínios para projetos PENG. Em seguida, a equipe chegou a um acordo quanto aos critérios estratégicos estabelecidos pelas questões de diversidade e sustentabilidade. Os inventários de conteúdo, processos e pessoas foram realizados seguindo as premissas de compartilhamento de conhecimento, visualização e definição de relevância, e seus desenvolvimentos podem ser descritos por um vocabulário controlado.

Este quadro deverá ser implementado nos próximos projetos de Engenharia da Paz para avaliar a sua eficácia tangível. Aplicações anteriores da estrutura Engenharia da Mente em projetos de apoio à decisão envolvendo IA demonstraram sua capacidade de facilitar a integração duradoura de equipes proficientes e garantir a manutenção contínua e o aprimoramento do conhecimento dentro do sistema.

## V. CONCLUSÕES

Desde o início da década de 1980, tem havido uma notável proliferação de organizações dedicadas a aproveitar o poder da engenharia para enfrentar desafios humanitários e de desenvolvimento [19]. Entre essas organizações estão Engineering for Change, Engineers Against Poverty, Engineers for Overseas Development, Humanitarian Engineering, Contextual Engineering, bem como capítulos nacionais de Engineers Without Borders e RedRs. Este aumento na atividade organizacional contribuiu significativamente para a expansão de programas e iniciativas de educação em engenharia humanitária em todo o mundo.

No meio deste cenário dinâmico, a Engenharia da Paz emergiu como um quadro convincente que alarga os princípios fundamentais da engenharia humanitária para abranger não só o alívio do sofrimento e do desenvolvimento, mas também a prevenção e resolução de conflitos e os grandes desafios globais. Enfatiza o papel dos engenheiros na promoção da paz, na promoção da justiça social e na abordagem das causas profundas dos conflitos, como a justiça ambiental. Segundo Trevelyan [20], a perspectiva é que a pesquisa em ciências sociais e humanas tenha o potencial de revelar insights valiosos capazes de orientar intervenções destinadas a mitigar as deficiências nas práticas de engenharia.

A missão da Engenharia da Paz é promover ativamente uma cultura de paz, exigindo que os engenheiros da paz, bem como os cidadãos e profissionais globais de todas as disciplinas, se tornem pensadores e executores globais completos. Eles devem estar conscientes de suas obrigações éticas profissionais e pessoais, compreender seus papéis como engenheiros cidadãos, cientistas, profissionais ou formuladores de políticas na sociedade, e compreender as consequências intencionais e não intencionais de suas decisões relativas à concepção, planejamento, gestão e

TABELA 1:

Fases da Engenharia da Mente e sua aplicação em Projetos de Engenharia da Paz (PENG).

| Fases                                   |                                                          | Definição                                                                                                                                              | Importância PENG                                                                                                                                                                         | Aplicação PENG                                                                                                                                                         |
|-----------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Compartilhamento de conhecimento</b> | Identificação de aspectos emocionais                     | Identifica os conhecimentos de cada integrante da                                                                                                      | Facilita a integração da equipe de trabalho e a introdução de novos integrantes no processo.                                                                                             | Mantém o compartilhamento contínuo de conhecimento                                                                                                                     |
|                                         | Normalização do Vocabulário                              | Descreve o vocabulário usual entre a equipe de engenheiros e os especialistas da área bem como os usuários do projeto.                                 | Melhora a velocidade da tomada de decisão                                                                                                                                                | Quebra a resistência à novas ideias.                                                                                                                                   |
|                                         | Inventário de Processos, Pessoas, Tecnologia e Conteúdo. | Permite conhecer amplamente o contexto do projeto.                                                                                                     | Ajuda na definição de Relevância.                                                                                                                                                        | Diminui a possibilidade de falha na execução do projeto.                                                                                                               |
| <b>Visualização</b>                     |                                                          | Permite definir a similaridade entre os indivíduos da equipe na forma de perceber e abordar o problema.                                                | Permite identificar com melhor clareza os impactos das ações do projeto antes da sua execução definitiva. Melhora a capacidade de imaginação dos integrantes da equipe e gera inovações. | Define a tecnologia a ser empregada com maior clareza, bem como os recursos a serem utilizados.                                                                        |
| <b>Definição de Relevância</b>          |                                                          | É a fase mais importante. Onde o projeto se adequa a realidade, no prazo, no escopo e nos custos. Sem perder a relevância da manifestação do coletivo. | Define a dimensão social do projeto e as ações a serem realizadas para alcançar eficazmente o resultado.                                                                                 | Permite que todos os envolvidos sintam que há uma dimensão social/emocional/tecnológica, onde a ética e a paz estão sendo executadas como finalidade maior do projeto. |

operação de projetos em todos os aspectos. vários contextos socioeconômicos, culturais e políticos. A engenharia da paz caracteriza-se não apenas pelas suas aplicações sociotécnicas, mas também pelo seu ethos e objetivos, formulados com um compromisso com a justiça social.

Globalmente, existem apelos urgentes à ação para abordar e resolver desafios prementes e amplamente reconhecidos à paz e à segurança antes que se transformem em questões mais complexas e dispendiosas a nível ambiental, financeiro e social, atingindo potencialmente um ponto crítico até 2030. A Engenharia da Paz responde a estes exorta, reconhecendo as contribuições significativas que a engenharia, juntamente com as ciências exatas e sociais, bem como outras disciplinas como o direito e as finanças, pode dar para a construção de um mundo mais sustentável, estável, seguro, equitativo e pacífico. Os Engenheiros da Paz aproveitam dados confiáveis verificáveis e utilizam uma abordagem holística de resolução de problemas para enfrentar esses desafios globais.

O estabelecimento de currículos e programas de graduação em Engenharia da Paz é visto como uma estratégia vital para cultivar novos talentos capazes de enfrentar os desafios globais de forma proativa antes da chegada de 2030. Vários programas acadêmicos se cruzam com a Engenharia da Paz, incluindo Engenharia Humanitária, Engenharia para

o Bem, Engenharia Verde e Contextual. Engenharia, entre outros. Portanto, a integração do PENG no currículo transcende meros esforços extracurriculares destinados a resolver conflitos ou a satisfazer necessidades humanitárias, como visto nas iniciativas tradicionais de engenharia humanitária.

"O PENG Minor" [5] é um exemplo de dismantelamento dos silos acadêmicos que tradicionalmente segregam as disciplinas, envolvendo assim um espectro mais amplo de futuros cidadãos globais em vários campos. O Minor em Engenharia da Paz é disciplina eletiva na Universidade do Novo México [21] e parte da grade curricular da Escola de Engenharia, que inclui: Centro de Materiais de Alta Tecnologia, Centro de Materiais Microprojetados, Centro de Educação e Pesquisa em Computação de Alto Desempenho, Instituto de Estudos de Energia Espacial e Nuclear, Aliança para Pesquisa em Transporte, Laboratório de Materiais Avançados, Centro de Engenharia Biomédica, Sistemas Inteligentes Centro de Engenharia, Centro de Treinamento e Tecnologia de Fabricação, Centro de Inovações e Aplicações de Microssistemas Espaciais Configuráveis (COSMIAC) e Centro de Água e Meio Ambiente. O Minor em Engenharia da Paz é um exemplo que deve ser disseminado em outras universidades pelo mundo. Os membros do Peace Engineering Consortium - PEC desempenham um papel

fundamental na facilitação de discussões, ministrando palestras, organizando workshops e proporcionando aos alunos diversas perspectivas e consciência contextual. Além disso, o Consórcio promove mudanças e revisões curriculares no programa. Ele se aprofunda, abrangendo o cultivo das faculdades mentais e emocionais do estudante de engenharia para remodelar seus processos cognitivos e dinâmicas interpessoais dentro do nosso ambiente – “Um Planeta, Um Ambiente, Uma Chance”.

Há muitas mudanças socioeconômicas e ambientais acontecendo neste momento. Neste processo encontramos a destruição dos nossos habitats e recursos naturais. Tal como está hoje, todas as áreas da engenharia terão de enfrentar a escassez e a degradação das suas matérias-primas devido à nossa falta de consciência (ignorância ou evitação) das consequências pretendidas e não intencionais. A engenharia, como área, é frequentemente associada ao conhecimento técnico, à solução de problemas e à busca pela eficiência. Os engenheiros são treinados para dividir problemas complexos em partes gerenciáveis e encontrar soluções por meio de métodos lógicos e científicos. Apesar do enorme crescimento do conhecimento técnico-científico sobre a natureza, inúmeros problemas não foram resolvidos e agora são expostos pela possibilidade de extinção da vida na Terra devido ao uso excessivo deste conhecimento tecnológico pela indústria moderna.

No rescaldo dos conflitos, os engenheiros têm historicamente desempenhado um papel crítico na reconstrução de infraestruturas e na restauração de serviços básicos nas áreas afetadas. O seu trabalho na reconstrução de estradas, pontes, sistemas de abastecimento de água e outras infraestruturas críticas tem sido essencial para criar estabilidade e promover a paz. Os engenheiros estão há muito tempo envolvidos em projetos de desenvolvimento que visam melhorar as condições de vida, reduzir a pobreza, resolver conflitos e abordar a desigualdade social. O campo da engenharia do desenvolvimento tem enfatizado práticas de desenvolvimento sustentável e inclusivas que se alinham com os objetivos de construção da paz.

Os Objetivos de Desenvolvimento Sustentável das Nações Unidas, adotados em 2015[22], destacam a interligação de vários desafios globais, incluindo a pobreza, a desigualdade, a degradação ambiental e os conflitos. Os engenheiros reconheceram a importância da sua experiência para alcançar estes objetivos e começaram a explorar formas de aplicar princípios de engenharia para promover a paz e a sustentabilidade. Com uma compreensão mais profunda dos conflitos e das causas subjacentes, tem havido um reconhecimento crescente de que as abordagens de engenharia podem ser integradas com metodologias de resolução de conflitos. Este reconhecimento abriu caminho para a Engenharia da Paz, que procura utilizar princípios e tecnologias de engenharia para abordar as causas profundas dos conflitos, promover a justiça social e promover a paz sustentável. A busca pelo cultivo de uma cultura de paz está na agenda há muito tempo, conforme reconhecido pela UNESCO [22]. Ao contrário da noção de que a paz é uma mera escolha ou atitude que se pode adotar sem esforço, é, na

verdade, uma habilidade que requer desenvolvimento deliberado. Assim como aprender matemática, a paz é uma proficiência interna, uma forma única de compreender o mundo que necessita de cultivo e compreensão intencionais. “Um planeta, um ambiente, uma chance.”

É importante que a Engenharia da Paz enfrente os desafios sociais, económicos e ambientais, promovendo o desenvolvimento sustentável e construindo sociedades pacíficas e resilientes. Ao abraçar a Engenharia da Paz através da Abordagem Social, Emocional e Tecnológica, não apenas enfrentamos os desafios que ameaçam a nossa civilização, mas também nutrimos as sementes de um futuro próspero e harmonioso para toda a humanidade.

#### AGRADECIMENTOS

Gostaríamos de estender nossos sinceros agradecimentos ao Sr. Hans Hoyer, Secretário da Federação Internacional de Sociedades de Educação em Engenharia (IFEES), por seu inestimável apoio e incentivo em nossa participação no Instituto i3g dentro do Peace Engineering Consortium.

#### REFERENCIAS

- [1] Global Trends - 2040. March 2021. NIC 2021-02339 - ISBN 978-1-929667-33-8. To view digital version: [https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends\\_2040.pdf](https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf)
- [2] National Academy of Engineering. 2009. Developing Metrics for Assessing Engineering Instruction: What Gets Measured Is What Gets Improved. Washington, DC: The National Academies Press. <https://doi.org/10.17226/12636>.
- [3] Tharakan, J. Disrupting Engineering Education: Beyond Peace Engineering to Educating Engineers for justice. *Procedia Computer Science*, Vol. 172, 2020, Pages 765-769, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2020.05.109>.
- [4] The Global Risks Report 2023 18th Edition. World Economic Forum <https://www.weforum.org/publications/global-risks-report-2023/>
- [5] R. Jordan, E. Hamke, M. Yousef, & D. Koechner (2024). Peace Engineering Minor: Actionable Knowledge. Towards a Hybrid, Flexible and Socially Engaged Higher Education, *Proceedings of the 26th International Conference on Interactive Collaborative Learning (ICL2023)*, Volume 2. Springer (pp. 189-199)
- [6] R. Jordan, K. Agi, B. Amadei, T. Casuse, D. Koechner, I. Nair, M. Nelson, M. Olson, M. Quihuis, and J. Tangorra, 2020. “Outcomes of the First Global Peace Engineering Conference”, *Procedia Computer Science*, Vol 172, p. 803-810.
- [7] Peace Engineering (PENG) for a Sustainable Planet by 2030: Call to Action 2020-2030. Summary of Peace Engineering Biome Kickoff Workshop. SAND2021-15614 R. Unclassified Unlimited Release [https://www.ifees.net/wp-content/uploads/2022/02/PENG-WorkshopSummary10Dec21\\_c.pdf](https://www.ifees.net/wp-content/uploads/2022/02/PENG-WorkshopSummary10Dec21_c.pdf)
- [8] Vesilind, P.A. *Engineering, Peace, and Justice: The Responsibility of Engineers to Society*; Springer: New York, NY, USA, 2010. 10.1007/978-1-84882-674-8.
- [9] R. Jordan, K. Agi, E. Maio, I. Nair, D. Koechner, D. Ballard (2018) "Invitation to Shape Peace Engineering, November 12, 2018", WEEF-GEDC-2018 (Albuquerque, NM, November 12-16, 2018).
- [10] The Social Dilemma. <https://www.netflix.com/title/81254224>. Accessed 24 May 2023
- [11] Peace Engineering Dashboard 2023. [https://peacedashboard.world/peace-engineering-dashboard-home/dashboard\\_2023/](https://peacedashboard.world/peace-engineering-dashboard-home/dashboard_2023/). Accessed 14 December 2023
- [12] World Economic Forum Annual Meeting 2016 Mastering the Fourth Industrial Revolution. [https://www3.weforum.org/docs/WEF\\_AM16\\_Report.pdf](https://www3.weforum.org/docs/WEF_AM16_Report.pdf).
- [13] OECD (2021), *Embedding Values and Attitudes in Curriculum: Shaping a Better Future*, OECD Publishing, Paris, <https://doi.org/10.1787/ae2adcd-en>.



- [14] Huerta, M. V., Carberry, A. R., Pipe, T., & McKenna, A. F. (2021). Inner engineering: Evaluating the utility of mindfulness training to cultivate intrapersonal and interpersonal competencies among first-year engineering students. *Journal of Engineering Education*, 110(3), 636-670. <https://doi.org/10.1002/jee.20407>
- [15] Rieken, B., Shapiro, S., Gilmartin, S. and Sheppard S. D. How Mindfulness Can Help Engineers Solve Problems. *Harvard Business Review*, January 04, 2019. Available in <https://hbr.org/2019/01/how-mindfulness-can-help-engineers-solve-problems>
- [16] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2*. IEEE, 2017. [http://standards.ieee.org/develop/indconn/ec/autonomous\\_systems.html](http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html).
- [17] T. C. D. Bueno, H. C. Hoeschl and M. B. Hoeschl, "Developing an Ontology-oriented Framework to Enable Peace-building Solutions Based on Fairplay Algorithms," 2018 World Engineering Education Forum - Global Engineering Deans Council (WEEF-GEDC), Albuquerque, NM, USA, 2018, pp. 1-6, doi: 10.1109/WEEF-GEDC.2018.8629678.
- [18] T. C. D. Bueno, and H. Hoeschl. Harmonizing Peace Engineering and Mind Engineering: A Lifelong Learning Approach for Sustainable Societies. "Manuscript submitted for publication" 2023. World Engineering Education Forum - Global Engineering Deans Council (WEEF-GEDC). Monterrey, México.
- [19] Smith, J., Anderson, B., Brown, N., Colley, A., Stoakley, A., & Turner, J. (2017). The rise of humanitarian engineering education in Australasia. In 28th Annual Conference of the Australasian Association for Engineering Education (AAEE 2017) (pp. 312-320) <https://search.informit.org/doi/10.3316/informit.390763431262433>
- [20] Trevelyan, J. P. (2022). A Social Science Research Agenda for Engineering Practice. In S. H. Christensen, A. Buch, E. Conlon, C. Didier, C. Mitcham, & M. Murphy (Eds.), *Engineering, Social Sciences, and the Humanities: Have their Conversations Come of Age?* Springer Science Business Media B.V. [https://doi.org/10.1007/978-3-031-11601-8\\_13](https://doi.org/10.1007/978-3-031-11601-8_13)
- [21] School of Engineering: University Catalog. The University of New Mexico. <https://catalog.unm.edu/catalogs/2022-2023/colleges/engineering/index.html>
- [22] United Nations Educational, Scientific and Cultural Organization (UNESCO). *The Culture of Peace Program: From National Programs to a Project of Global Scope*. Available online: <http://www.culture-of-peace.info/vita/1994/145EX15.pdf> (accessed on October 2023).

# Fortalecimiento de la Seguridad y Protección de Datos Personales en Chile: Desafíos y Perspectivas hacia el Futuro.

Sebastian Berrios, *Member, Pontificia Universidad Católica de Valparaíso*, Pamela Hermosilla, *Member, Pontificia Universidad Católica de Valparaíso*, Héctor Allende Cid, *Member, Pontificia Universidad Católica de Valparaíso*.

**Abstract-** La ley chilena de protección de datos personales, establecida en 1999, no logra abordar los desafíos contemporáneos en ciberseguridad. Un análisis comparativo con las leyes europeas y las de otros países latinoamericanos revela una disparidad notable. Esta deficiencia resulta en la persecución o permisión inadecuadas de delitos relacionados con el tratamiento de datos personales. El reciente aumento en las filtraciones de datos subraya la necesidad urgente de modernizar la legislación chilena sobre la protección de datos personales, alineándola con los estándares actuales de ciberseguridad.

**Index Terms--**Ciberseguridad, Protección de datos, Cibercrimen, Chile.

## I. INTRODUCCIÓN

En Chile, la protección de datos personales se ha convertido en un tema de creciente interés y preocupación. Impulsado por el avance tecnológico y la expansión de la digitalización, este tema ha cobrado una relevancia sin precedentes en la sociedad chilena. La legislación chilena sobre protección de datos, que se remonta a 1999, ha demostrado ser insuficiente frente a los desafíos de la era digital actual, especialmente en cuestiones de ciberseguridad. Esta insuficiencia se hace más evidente al comparar la normativa chilena con la de la Unión Europea y otros países de América Latina, donde se han adoptado medidas más avanzadas en este campo.

La creciente incidencia de brechas de seguridad y ciberataques ha puesto en evidencia las debilidades de los sistemas de protección de datos en Chile, generando un llamado urgente a la acción para fortalecer las políticas y regulaciones existentes. Este movimiento busca no solo actualizar la legislación para equipararla con los estándares internacionales, sino también fortalecer la confianza del público en las plataformas digitales y las instituciones que manejan datos personales.

Con una sociedad cada vez más consciente de la importancia de la privacidad de datos, ha surgido una demanda de mayor transparencia y responsabilidad en el manejo de la información personal por parte de entidades gubernamentales y privadas.

Esta concienciación ciudadana es un paso crucial hacia la creación de un entorno más seguro y protegido para los datos personales.

En este contexto, Chile enfrenta el reto vital de reformar y actualizar su marco normativo y sus prácticas de gestión de datos personales. Esta actualización no solo es necesaria para la protección de los ciudadanos, sino también para asegurar la adaptación de Chile a un entorno global cada vez más digital y conectado. Desde los inicios de la informática existen los ataques informáticos y virus en los sistemas, uno de los primeros exponentes de este tipo de virus es el programa Creeper, el cual fue creado en 1971 por Bob Thomas, el cual era una prueba de seguridad y no buscaba ser malicioso, pero quería comprobar si era posible replicar en la red de ARPANET, cosa que sí pudo hacer, al replicarse e “infectar” un disco duro, procedió a eliminarse a sí mismo y dejar un mensaje que decía: “Soy Creeper, ¡Atrápame si puedes!” Sin embargo, el primer virus creado con malas intenciones fue el virus de Rabbit (o Wabbit), el cual al ingresar en el equipo hacía muchas copias de sí mismo, haciendo que la computadora se ralentizará tanto que resultara en un congelamiento y eventualmente colapsarlo.

Pasado muchos años después, evolucionaron las redes y actualmente nos encontramos en la era del internet donde mucha de nuestra información se encuentra disponible en internet, ya sea de manera pública como en redes sociales, perfiles, entre otros y información privada o sensible, como por ejemplo tarjetas de crédito, credenciales, direcciones, entre otros tipos de datos. En un mundo donde cada vez más y más gente se conecta a internet, accede a servicios, todos estos datos quedan registrados en alguna base de datos, donde se guarda todo tipo de información que el usuario entregue, por lo que mucha de nuestra información se encuentra acá, ya sea públicamente accesible como no accesible. A pesar de que las bases de datos suelen estar inaccesibles al público general, la globalización y el avance de Internet han dado lugar a nuevos desafíos significativos. Entre estos, los ataques cibernéticos y la acción de los piratas informáticos representan una amenaza creciente. Estos actores malintencionados aprovechan las vulnerabilidades en la seguridad de las bases de datos para acceder a información confidencial, poniendo en riesgo la integridad y privacidad de los datos almacenados. Esta problemática subraya la importancia de implementar estrategias robustas de ciberseguridad y protección de datos para contrarrestar eficazmente tales riesgos.

## II. EVOLUCIÓN DE LAS VULNERABILIDADES

En la actualidad, con las nuevas tecnologías que se van desarrollando a medida que avanzan los años, también se encuentran nuevas vulnerabilidades y puertas traseras, las cuales son oportunidades perfectas para ser interceptado y atacado, por ende, a medida que avanzan los años, cada vez es mas facil o mas probable ser víctima de algún ataque, ya sean grandes como medianas, pequeñas o incluso ataques a individuos. Un estudio realizado por IBM Security determinó que hay 3 principales razones por las cuales es posible tener una vulneración de datos, puede ser mediante el error humano (ser víctima de phishing o ingeniería social), un ataque malicioso o un error del sistema (como no estar actualizado por ejemplo).

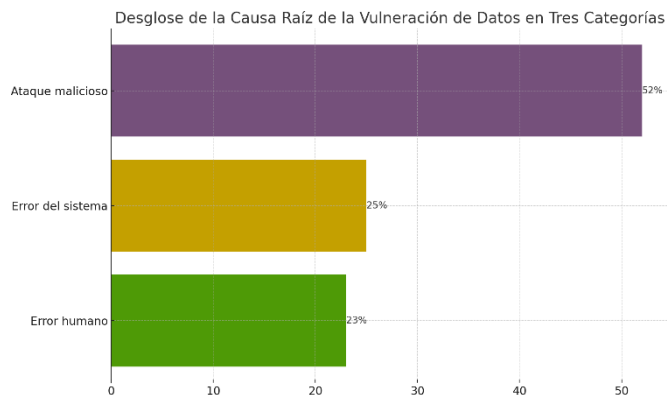


Fig. 1. Gráfico de causales de vulneración de datos, de IBM Security

Además del gráfico anteriormente mencionado por las causas en las que se pueden vulnerar los datos, existe otro gráfico más el cual es más específico con los métodos de ataque utilizados para vulnerar los datos.

**Cuentas de Empleados Comprometidas:** Estas fueron la causa más costosa de las brechas de datos, con las empresas estudiadas experimentando costos casi \$1 millón más altos en promedio por brecha en comparación con el promedio global, llegando a \$4.77 millones por incidente. El 80% de estos incidentes resultó en la exposición de información personal identificable (PII) de los clientes, siendo la PII de clientes también la más costosa para las empresas.[1]

**Credenciales Robadas o Comprometidas y Configuraciones Erróneas en la Nube:** Estos fueron los motivos más comunes de brechas maliciosas, representando casi el 40% de los incidentes maliciosos. Las empresas luchan con la complejidad de la seguridad, lo que contribuye a que las configuraciones erróneas en la nube se conviertan en un desafío creciente. Los atacantes utilizaron estas configuraciones erróneas para violar las redes en casi el 20% de los casos, aumentando los costos de brecha en más de medio millón de dólares en promedio a \$4.41 millones.

**Ataques Patrocinados por Estados:** Aunque representaron solo el 13% de las brechas maliciosas estudiadas, los ataques patrocinados por estados fueron el tipo de adversario más dañino. Estos ataques promediaron \$4.43 millones en costos de brecha de datos, superando a los ciberdelincuentes motivados financieramente y a los hacktivistas.

Estas estadísticas subrayan la importancia de abordar las vulnerabilidades de seguridad interna, como las cuentas de empleados comprometidas y las configuraciones erróneas en la nube, así como la necesidad de estar preparado para ataques complejos patrocinados por estados.

Uno de las primeras brecha de datos (o data breach como se le conoce en inglés) fue en el año 2005 a la DSW Shoe Warehouse, una tienda de zapatería ubicada en Estados Unidos, donde se tomó información sensible como tarjetas de crédito, débito y datos personales de cuentas de usuarios de más de 1 millón de personas en EE.UU. Esto generó el llamado a las autoridades, más específicamente la Comisión Federal de Comercio o Federal Trade Commission (FTC) de EE.UU, donde llegaron a la conclusión de que DSW falló en proteger la información de los usuarios de la tienda. Esto se debió a que se encontraron múltiples irregularidades y malas prácticas a la hora de almacenar los datos de los clientes, entre estas malas prácticas se encuentran:

Crear riesgos innecesarios a la información sensible al almacenar muchos archivos cuando ya no hacía falta tener esta información  
Almacenar información sensible como IDs de usuario y contraseñas de manera no encriptada  
Falta de personal para verificar los accesos no autorizados  
Falla en no utilizar el equipamiento de seguridad para limitar los equipos que se podían conectar mediante red inalámbrica

Con toda esta información obtenida, se hicieron cargos de compras fraudulentas y otros actos no deseados, por lo que DSW tuvo que terminar las cuentas, comunicarse con los clientes y ofrecer soluciones y reembolsos, lo que le costó entre 6.5 y 9.5 millones de dólares en pérdidas.

Este tipo de ataques generan mucho más daño de lo que parecen ser y se pasan por tres etapas, incidente, administración y recuperación, cuando ha ocurrido una brecha de datos se tienen que medir y hacer las correspondientes acciones, dentro de las cuales se encuentran las siguientes:

- **Reputación de imagen:** Al ver que sus sistemas fueron vulnerados y que no tienen la debida seguridad ni protección, genera la desconfianza del público general, haciendo que la gente pierda confianza y los clientes terminan retirándose y buscando una alternativa o no lo ven como una opción atractiva por el pasado que tiene, este daño a la marca puede durar hasta 5 años en poder ser recuperada la confianza.
- **Detención de los sistemas:** En este contexto, se hace necesario suspender temporalmente las operaciones de todos los sistemas de la organización. Tal acción no solo ayuda a prevenir la propagación del ataque, sino que también facilita la recopilación de evidencia crucial para entender la brecha de seguridad y tomar medidas correctivas eficaces.
- **Crear nuevas infraestructuras:** Con los equipos que probablemente estaba trabajando estaban desactualizados o sin herramientas especializadas para detener o prevenir este tipo de ataques, por lo que

hay que hacer una nueva actualización de sistemas para poder estar protegido y así evitar otro incidente similar.

- Preparar acciones legales: Una vez investigado el caso, se tiene que hacer las diversas denuncias en caso de encontrar evidencia incriminadora y de esta manera llegar a juicio con los responsables que cometieron estos delitos.

Estos apartados junto con otros más hacen que como resultado, la empresa tenga que gastar muchísimo dinero, millones y millones de dólares para poder recuperarse, volver a operar y de esta manera continuar con el negocio, en caso de que se lo pueda permitir, ya que esto es perfectamente posible administrarlo en una gran empresa con un buen poder adquisitivo, pero si un incidente así le pasa a una mediana o pequeña empresa, el daño es mucho mayor y podría hasta dejarlo fuera de negocio indefinida o permanentemente por el daño causado.

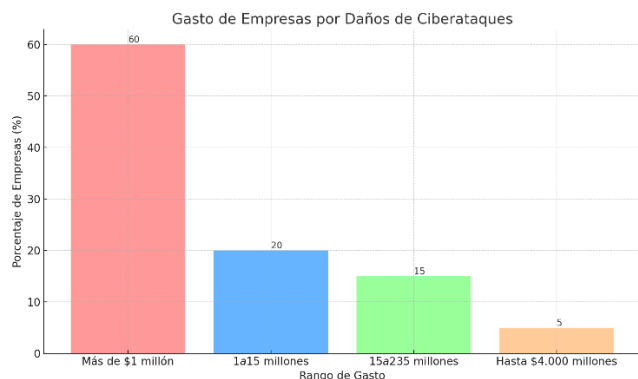


Fig. 2. Gráfico de las brechas de gasto de empresas por daños de ciberataque realizada por MinTIC de Colombia.

Dentro de estos ataques, se puede evidenciar que una gran parte de estos ataques se realizan el robo de las bases de datos, especialmente de las grandes empresas, los cuales tienen un banco importante de personas y credenciales las cuales se pueden hacer cosas como la comercialización, usurpación de identidad, entre otros.

**Impacto en la Reputación de la Empresa:** Los incidentes no solo tienen un impacto financiero directo, sino también pueden afectar la reputación de la empresa. Esto puede llevar a una pérdida de confianza de los clientes y socios, lo que a largo plazo puede ser más costoso que los daños inmediatos.

**Costos Ocultos y a Largo Plazo:** Además de los gastos obvios, como reparaciones o reemplazo de equipos, hay costos menos visibles como la disminución de la productividad, el tiempo perdido en la gestión del incidente, y posibles demandas legales. Estos costos pueden acumularse y ser significativos, especialmente para las pequeñas y medianas empresas. Algunos aspectos para considerar sobre los costos y consecuencias de incidentes en ciberseguridad empresarial:

- **Impacto en los Empleados:** Los incidentes pueden afectar la moral y el bienestar de los empleados. Esto puede traducirse en una mayor rotación de personal,

dificultades para atraer talento, y un descenso en la productividad.

- **Costos de Recuperación y Prevención:** Las empresas deben invertir en medidas de recuperación y prevención para evitar futuros incidentes. Esto incluye la formación de empleados, actualización de sistemas de seguridad, y posiblemente, seguros más costosos.
- **Diferencias en el Impacto Según el Tamaño de la Empresa:** Mientras que las grandes empresas pueden tener más recursos para recuperarse y absorber los costos, las pequeñas y medianas empresas son más vulnerables. Un incidente grave puede llevarlas al cierre, especialmente si no cuentan con seguros adecuados o planes de recuperación de desastres.
- **Pérdida de Clientes y Mercado:** Un incidente grave puede llevar a una pérdida temporal o permanente de clientes. Además, puede dar lugar a que competidores aprovechen la situación para captar una mayor cuota de mercado.
- **Impacto en la Cadena de Suministro:** Para las empresas que forman parte de una cadena de suministro, un incidente puede tener un efecto dominó, afectando a otros negocios y asociados.

Hoy en día existen múltiples formas en la cual uno pueda ser víctima de un ataque, entre los métodos existen técnicas como los mensajes o correos phishing, donde el atacante se hace pasar por una figura de autoridad y el usuario entrega voluntariamente sus datos personales. Ahora bien, existen ataques mucho más elaborados, los cuales van dirigidos directamente a grandes empresas donde se pueden encontrar una gran cantidad de datos. El ransomware es una de las amenazas más prevalentes y destructivas en el ámbito de la ciberseguridad. Este tipo de malware cifra los archivos del sistema de la víctima, exigiendo un rescate para su descifrado. A continuación, se describen los tipos más comunes de ataques de ransomware, destacando sus características y métodos de operación. Algunos tipos de ataques mas comunes son los siguientes:

- **Locker Ransomware**

El Ransomware de Bloqueo impide el acceso al dispositivo de la víctima, bloqueando la pantalla o el sistema operativo completo. Este ataque no cifra archivos individuales, sino que niega el acceso general al dispositivo. La víctima ve una notificación de rescate en la pantalla, instruyendo cómo proceder para desbloquear su dispositivo.

- **Crypto Ransomware**

El Ransomware de Cifrado es más sofisticado y dañino que el locker ransomware. Cifra archivos individuales o sistemas de archivos completos, haciendo inaccesibles documentos, bases de datos, fotos y otra información importante. Este ataque se caracteriza por permitir al usuario acceder al sistema operativo pero no a los archivos cifrados, solicitando un pago para obtener la clave de descifrado.

- Scareware

Aunque no es un ransomware en el sentido tradicional, el Scareware incluye falsos programas antivirus y aplicaciones de limpieza de sistemas que alegan haber encontrado problemas en el dispositivo de la víctima. Estos programas exigen pago para "limpiar" el sistema. A pesar de que no cifran archivos, utilizan tácticas de intimidación para extorsionar a las víctimas.

- Ransomware como Servicio (RaaS)

RaaS es un modelo de negocio en el que los desarrolladores de ransomware ofrecen su malware como un servicio a terceros. Los afiliados distribuyen el ransomware, mientras que los desarrolladores mantienen el software y cobran una parte del rescate. Este modelo ha permitido que individuos sin conocimientos técnicos lanzan ataques de ransomware.

- Ataques de Doble Extorsión

Los ataques de Doble Extorsión combinan el cifrado de archivos con la extracción de datos sensibles. Los atacantes amenazan con publicar o vender la información robada si el rescate no se paga, aumentando significativamente la presión sobre las víctimas para que cumplan con sus demandas.

- Ransomware dirigido

A diferencia de los ataques de ransomware más generalizados, los Ataques Dirigidos se enfocan en objetivos específicos, como organizaciones o industrias particulares. Los atacantes realizan una investigación previa para entender la infraestructura de TI de la víctima y diseñar un ataque que cause el máximo impacto, a menudo pidiendo rescates significativamente más altos.

Un estudio realizado por BitLife Media, hizo un gráfico viendo la cantidad de brechas de datos que han ocurrido entre 2019 y 2022.

Además de esto, el estudio también revela que los métodos de ransomware y accesos no autorizados son los principales ciberataques que se realizan.

Los ataques mediante ransomware son ataques los cuales el atacante encripta o priva de acceso a un equipo, base de datos, o cualquier dispositivo con información valiosa para el usuario y/o empresa y pide una compensación en forma de recuperar los datos, la compensación más común para la "recuperación" de sus datos es el pago de una determinada cantidad de dinero mediante criptomonedas para evitar ser rastreado.

Y los ataques mediante acceso no autorizados son ataques en el que se obtiene acceso a equipos de un individuo, ya sea particular como de una empresa y de esta manera tener acceso a información privilegiada, confidencial o sensible. Además, al tener acceso a estos equipos, el atacante puede ejecutar un virus de ransomware si tiene acceso a las máquinas con permisos de administrador.

Con todo lo anteriormente mostrado, corresponde hacerse la pregunta y decir: ¿quien se hace responsable de nuestros datos en caso de que sean filtrados?. El principal actor de quien tiene que proteger nuestros datos son a quienes se los damos y por ende, cae en ellos la responsabilidad de mantener nuestra información segura, sin embargo, como hemos visto con los gráficos y

estudios anteriormente mencionados los ataques solo van en aumento y puede pasarle tanto a una pequeña como una grande empresa, por lo que siempre se corre el peligro de que se genere una brecha y nuestros datos queden expuestos, por lo que la ley tiene que hacerse cargo en caso de que estos incidentes ocurran. Sin ir más lejos, en 2019, la Comisión para el mercado financiero (CMF) reportó que Redbanc tuvo un ciber incidente en la casilla de Incidente Operacionales, donde se filtraron la información de más de 41.000 tarjetas de credito y debito.

Otro caso similar es lo que ocurrió en 2014, donde fue accedida a la equipos de MINSAL y tomaron información médica y datos personales de muchas personas dentro del sistema, quedando totalmente expuesta su información.

Problemas con la ley de protección de datos chilena

En el reglamento de la biblioteca del congreso nacional de Chile, la ley que hablaba sobre la protección de datos es la ley 19.628 esta ley es la que nos indica qué hacer en caso de que los datos de un ciudadano chileno sea vulnerado, modificado o compartido sin el consentimiento del propietario de los mismos y por ende infringir esta ley y aplicar la debida sanción. Esta ley sin embargo, no aplica para casos donde estos crímenes hayan sido cometidos de manera virtual, por lo que tiene que ser complementada.

La regulación permite la trata de datos personales sin el consentimiento del titular en distintas ocasiones, como fuentes accesibles al público y la trata de personas juridicas, trata de datos por parte de organismos publicos y datos relacionados a la salud. En este sentido se llega a considerar el consentimiento al punto de corresponder a una excepción a diferencia de un principio fundamental.

La ley no define lo suficiente el dato personal para diferenciarlo entre un dato personal y un dato estadístico(dato que no puede ser asociado a un individuo en específico), dejando la posibilidad a la difusión de datos que constitucionalmente se encuentran consagrados, como es el caso del data leak de SERVEL del año 2022.La regulación no define específicamente el consentimiento respecto a las nuevas tecnologías y se tiene incerteza respecto a qué autorización es necesaria y como cuando se habla de datos sensibles y datos personales.

La ley no establece si se aplica a individuos u organizaciones que traten datos de nacionales, dejando la posibilidad de impunidad frente a brechas de datos personales realizadas a organizaciones fuera del territorio nacional.

La ley no establece específicamente quienes intervienen en el tratamiento de datos.[2]

Esta ley posee los siguientes artículos en los cuales se menciona la infracción de la ley de protección de datos.

En el artículo 16 se dice que si el responsable del registro o banco de datos no se pronuncia sobre la solicitud del requirente dentro de dos días hábiles, o la deniega por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente[3]

Y en el artículo 17 en particular, se establece que los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas sean requeridas por organismos públicos o por el titular de los datos. Además, se establecen las sanciones por infracciones a las normas de protección de datos personales, que pueden incluir multas, clausura temporal o definitiva del registro o banco de datos, y la responsabilidad civil por los daños y perjuicios causados.[4]

Entre las sanciones en caso de haber incumplimiento de esta ley, se encuentra la clausura temporal o definitiva del banco de datos y el dueño de este hacerse responsable de los potenciales daños causados por esta filtración. Además de esto, en caso de que el dueño de los datos sea negligente con la entrega o lo solicitado por el dueño de estos, se le aplicará una sanción con el pago de una multa que puede ir desde las dos a cincuenta UTM (Unidad de Tributarias Mensuales), haciendo que solamente reciba una pena monetaria el atacante y nuevamente pueda ser libre de realizar crímenes similares, a diferencia de otras leyes como España, o Argentina.[5][6]

La ley anteriormente mencionada no toma en cuenta los casos en los cuales se haya perpetrado esta infracción mediante el uso de algún ordenador, computador o base de datos, por lo que se tiene que complementar con la ley 19.223, la cual habla principalmente del ataque directo de equipos, ya sea utilizándolos, de manera malintencionada, tratamiento de información, difusión, entre otros, sin embargo, la ley habla de casos muy generales, a esto hay que sumarle que esta ley posee una única planta y sus sanciones no son claras fuera de un nivel de gravedad, por lo que da a lugar a múltiples vacíos legales y evasiones de ley por lo ambiguo de esta.[7][8]

### III. COMPARACIÓN ENTRE LA LEY CHILENA DE PROTECCIÓN DE DATOS Y OTROS PAÍSES

En Argentina, la cual es la ley N°25.326 esta ley por sí sola no funciona para poder ser aplicada en caso de que los datos hayan sido comprometidos en algún medio digital, pero esta ley si esta afiliada a la normativa de Ciberseguridad que tiene Argentina, por lo que sí está relacionada la protección de datos con la seguridad informática, a diferencia de la ley Chilena, donde no se reconocen o se asocian a una normativa informática o de ciberseguridad, solamente a la ley 19.223.[9][10]

Acompañado de lo anteriormente mencionado, en el capítulo VI de la ley argentina, se encuentra el apartado de Sanciones, en la cual se habla de sanciones administrativas y penales, donde en las sanciones administrativas de pueden tener penas con multas desde los mil pesos hasta cien mil pesos, clausura o cancelación del banco de datos, suspensión, entre otros cargos, y en el caso de las penales, dependiendo si se incorpora con el artículo 117 bis del Código penal o el artículo 157, en el caso del primero, se puede tener una pena de prisión desde un mes hasta tres años dependiendo de la gravedad que se estime, y en el caso del segundo artículo, puede sufrir de una pena de un mes hasta dos años en caso de revelar información que tuviera que estar

preservada por disposición de una ley.[11]

Otro país en donde se puede ver una gran diferencia es con España, la cual es la ley Orgánica 7/2021, la cual es la ley de protección de datos española. En esta ley se establecen múltiples cosas, una de las mayores diferencias especialmente con la ley de Chile, es que ahora existen múltiples autoridades las cuales regulan, previenen y detectan estas infracciones penales, como las Fuerzas y cuerpos de seguridad, administraciones penitenciarias, Dirección adjunta de vigilancia aduanera de la agencia estatal administración tributaria, entre otras entidades.

Junto a lo anteriormente mencionado, las penas en caso de cometer infracciones son mucho mayores y más graves, por ejemplo, la multa más alta que un ciudadano chileno puede recibir por incumplimiento de la ley 19.628 es de 50 UTM, o equivalente a \$3.198.000 millones de pesos chilenos o aproximadamente 3600 dólares, por el contrario, la ley Española, si se hace la falta más grave que sería una infracción de tipo muy grave, la multa puede rondar entre los 360.001 euros hasta 1.000.000 de euros o más de 1 millón de dólares.

Con estas comparaciones anteriormente vistas, podemos concluir que la ley de protección de datos chilena le falta mucho desarrollo para poder estar a la altura de los tiempos actuales donde este tipo de problemas se desarrollan principalmente en internet, por lo que se tiene que hacer algo al respecto para poder solucionar este problema y arreglar los vacíos legales que posee esta ley.

Menciones sobre la legislación penal sobre la protección de datos y cibercrimen

Las leyes anteriormente mencionadas son un antecedente de que, a pesar de que si existían protección de datos como tal, se hablaba de manera muy general y dejaba de lado el ámbito informático, por lo que se podían dar a interpretación o invalidación por lo ambiguo de este. Acá es donde, el convenio de Budapest, se genera la nueva ley de protección de datos (2022), donde esta se especializa y deroga la ley 19.223 (1993) y modifica otros cuerpos legales.[12]

La ley 21.459, toma en cuenta las primeras disposiciones y definiciones del acuerdo de Budapest, de modo que establece y tipifica los delitos informáticos, de la misma forma toma en cuenta la manera para procesar estos delitos y la forma de investigarlos. Finalmente, la ley establece las penas asociadas a estos delitos.[13] Una de las mayores diferencias respecto a la ley 19.628, es que la protección de datos ahora si abarca los delitos informáticos, dentro de los cuales se incluyen delitos como el ataque a la integridad de un sistema informático, acceso ilícito a un sistema informático, falsificación de documentos, sabotaje informático, entre otros informáticos del mismo tipo. Junto a esto, con esta ley ahora la multa no solamente es mucho más alta la cual puede ir desde las 100 a 500 UTM, sino que con esta nueva ley ahora se pueden establecer penas de presidio menor a mayor, por lo que ahora con si es posible tener una sanción penal e ir a prisión por incumplimiento de ley, el cual debe ser evaluado con un abogado.

Con todo lo anteriormente mencionado con la nueva ley, podemos concluir que es un avance significativo al compararla con la ley 19.223 por ser muy poco específica y no abarcar específicamente la figura de la protección de datos personales, y una cantidad de posibles casos donde se pudieran cometer crímenes sobre esa

materia.

#### IV. LEY 21.096, ACERCAMIENTO A UNA NUEVA LEY DE PROTECCIÓN DE DATOS

La ley 21.096 (2018) establece y consagra a nivel constitucional el derecho a la protección de datos personales, corresponde a un avance significativo hacia una ley de protección de datos, sin embargo, deja al dominio legal o de la ley la consagración de los derechos ARCO, siendo estos: derecho al acceso, rectificación, cancelación y oposición dispuestos en la ley 19.628.

Entre los derechos ARCO que existen, se especifican los siguientes:

- A. Derecho de acceso o información: Se puede solicitar información de los datos, como propósito de almacenamiento, lugares de almacenamiento, entre otros.
- B. Derecho rectificación o modificación: Se puede solicitar la modificación de los datos cuando son inexactos, erróneos, incompletos, entre otros.
- C. Derecho de oposición: Evitar que los datos sean usados con otros fines, como publicitarios, investigación de mercado, entre otros
- D. Derecho de bloqueo: Suspensión de banco de datos bajo ciertas circunstancias.

#### V. NECESIDAD DE UNA NUEVA LEGISLACIÓN SOBRE LA PROTECCIÓN DE DATOS.

Desde principios de la década el fenómeno de data leak se ha hecho un fenómeno cada vez más frecuente, de acuerdo al portal de ciberseguridad de entel es posible apreciar que el tuvo un aumento exponencial el año entre los años 2021-2022, como es posible observar en el presente gráfico.

Incremento de Eventos Registrados: Entre 2021 y 2022, hubo un incremento del 69% en la cantidad de eventos de filtración de datos registrados, y solo en los primeros 9 meses de 2023, se observó un aumento adicional del 22% sobre el total de eventos de 2022.

Filtraciones de Datos en Chile: Se identificaron 33 eventos de filtraciones de datos en Chile, involucrando a 14 actores de amenaza diferentes. Algunos de los actores más activos incluyen a Sombraman1919, Kung\_Liao, y LeakBase, quienes se enfocan principalmente en compañías de telecomunicaciones y gobiernos .

Contexto en América Latina: En total, se registraron 295 eventos de filtraciones de datos en América Latina, con Brasil, México y Chile siendo los países más afectados. Estos incidentes son

atribuidos en parte a la estabilidad de la moneda local y el desarrollo tardío de leyes y políticas de TI en la región.[14]

Este patrón refleja un aumento constante en la actividad de ciberamenazas en la región, especialmente en plataformas de Deep y Dark Web, y resalta la necesidad de medidas de seguridad y prevención más robustas en la industria TI.

Es posible además, apreciar en el siguiente gráfico que en comparación a otros países de Latinoamérica, este corresponde al tercer mayor país con filtraciones de datos después de Brasil con el primer lugar y México con el segundo.[15]



Fig. 3. Gráfico de las leaks de datos ocurridos durante el año 2023 realizado por Entel.

Entre otras formas de evidenciar el aumento de ciberataque se puede observar en el presente gráfico sobre los ataques por ransomware a los datos de organizaciones en Chile. Es evidente que diversas organizaciones actualmente manejan como método de identificación de usuario o como dato para almacenar información del usuario, como por ejemplo Correos de Chile, SP digital, entre otros. Organizaciones que pueden en algún momento ser vulnerables a ataques a sus bases de datos, en donde almacenar estos datos personales como el Rol Único Tributario no se justifica.

Datos personales a los cuales actualmente es posible acceder a través de Rol Único Tributario/Nacional son:

- A. Nombre completo.
- B. Fecha de nacimiento.
- C. Lugar de nacimiento.
- D. Edad.
- E. Sexo.



- F. Estado civil.
- G. Pertenencia a un grupo étnico.
- H. Familiares.
- I. Estado de salud.
- J. Local y mesa de votación de elecciones.
- K. Becas ganadas
- L. Listado de fármacos que se consumen
- M. Frecuencia de consultas médicas
- N. Bienes inmuebles que se poseen
- O. Historial de compras en retail
- P. Medios de pago utilizados
- Q. Lugares de trabajo
- R. Militancia política

Es posible evidenciar que el solo al acceder al RUT/RUN de una persona es posible obtener una gran cantidad de datos personales a través de los propios servicios del Estado o bien en los repositorios de páginas en los cuales se permite buscar a una persona por RUT/RUN, asimismo, es posible encontrar el RUT/RUN de una persona conociendo su Nombre completo.[16]

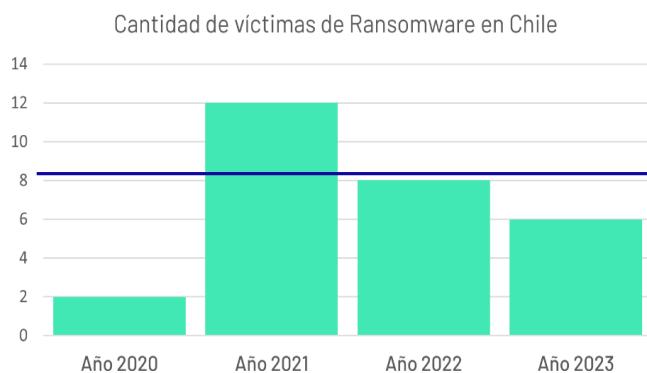


Fig. 4. Gráfico de cantidad de víctimas por ransomware en Chile proporcionado por Entel.

Es difícil determinar un número exacto de víctimas por ransomware en Chile, ya que no todas las empresas o instituciones reportan los ataques públicamente. Sin embargo, existen algunos datos que nos permiten estimar el impacto de este tipo de ataques en el país. De acuerdo a los datos disponibles, podemos estimar que ha habido al menos 28 víctimas de ransomware en Chile desde 2020 al 2023. Sin embargo, es importante destacar que esta cifra podría ser mayor, ya que no todos los ataques se reportan públicamente. Ejemplo de una vulneración a los datos personales corresponde al fenómeno sucedido año 2020, en el cual se registra un Data Breach masivo sobre la institución de Carabineros de Chile, exponiendo más de 10.000 documentos confidenciales y los datos personales de todos los funcionarios de la institución entre ellos, nombres, RUTs asociados, sexo, zona y comisarías, información de carácter sensible que pone en riesgo la integridad de los miembros del cuerpo policial.

El año 2021, en las elecciones municipales de mayo el organismo SERVEL sufrió una masiva vulneración y brecha de datos personales (data leak), correspondiente a los datos de 15 millones de personas de territorio nacional, entre cuyos datos existían; RUTs asociados a cada nombre, género, edad, y datos de pertenencia a pueblo originario. Nuevamente, el año 2022 el organismo SERVEL filtro los datos de las 15 millones de personas, correspondientes esta vez, RUTs asociados a cada nombre, género, edad, militancia, habilitación para votar y preferencia de voto.

El año 2023, octubre se registra un data breach sobre la información de 10 millones de chilenos, cuyos datos corresponden a RUTs, nombre asociado, sexo.

Los efectos de estos Data Leak corresponden a nuevas formas de que las personas sean vulneradas ya sea utilizando estos datos para realizar elaboradas estafas de phishing o spoofing, tomando en cuenta que se hacen uso de los datos personales de las personas. En este ámbito también es posible observar un aumento exponencial y generalizado de ataques phishing en Latinoamérica, de acuerdo a Kaspersky existe un aumento del 617% durante los 12 meses anteriores a julio de 2023 en comparación a los 12 meses anteriores a julio del año anterior. Así mismo es posible observar que Chile corresponde a uno de los países con mayor porcentaje de ataques por phishing en el mundo.

Las estadísticas de Kaspersky sobre ataques de phishing revelan una preocupante tendencia en el aumento y la sofisticación de estas amenazas en los últimos años:

Estadísticas Generales de 2022: Kaspersky bloqueó más de 500 millones de intentos de acceder a sitios web fraudulentos en 2022, lo que representa el doble en comparación con las cifras de 2021. Los servicios de entrega, mensajería y plataformas de criptomonedas fueron los anzuelos más comunes utilizados en estos ataques. Los usuarios de servicios de entrega fueron los más afectados, constituyendo el 27.38% de todos los intentos bloqueados, seguidos por tiendas en línea (15.56%), sistemas de pago (10.39%) y bancos (10.39%). Además, se observó un aumento en la distribución de ataques a través de mensajeros, con la mayoría de los intentos bloqueados provenientes de WhatsApp (82.71%), seguido de Telegram (14.12%) y Viber (3.17%).[17]

Estadísticas de Malware en 2023: Durante el período reportado en 2023, Kaspersky detectó un promedio de 411,000 archivos maliciosos por día, con un aumento del 3% en comparación con el año anterior. En particular, se observó un aumento del 53% en ataques que involucran documentos maliciosos de Microsoft Office y otros tipos. Kaspersky también notó un aumento significativo en el uso de backdoors para infiltrarse en sistemas de manera no detectada.[17]

Estadísticas Específicas de Phishing en 2023: En los primeros



diez meses de 2023, Kaspersky identificó 30,803,840 ataques de phishing dirigidos a tiendas en línea, sistemas de pago y bancos. Las plataformas de comercio electrónico fueron el objetivo principal, representando el 43.5% del total de ataques (13,390,142 ataques). Las páginas de phishing que imitaban plataformas de compras populares como Amazon, eBay, Walmart, AliExpress y Mercado Libre sumaron 6,232,882 en los primeros diez meses de 2023. Apple fue consistentemente el señuelo más popular, con intentos de phishing que utilizaban su nombre alcanzando 2,844,828 en el mismo período.

Estos datos subrayan la creciente amenaza de los ataques de phishing y la importancia de implementar medidas de seguridad robustas para protegerse contra estas tácticas cada vez más sofisticadas.

Se hace necesario una legislación más específica y atinente a los problemas actuales, teniendo en cuenta que el cibercrimen y la tecnología son algo que están en constante evolución.

#### VI. NUEVO PROYECTO DE LEY: LEY DE PROTECCIÓN DE DATOS

El nuevo proyecto de ley actualmente se encuentra en tercer trámite constitucional y constituye la consagración del derecho de protección de datos. Así mismo, es posible desglosar los siguientes puntos del nuevo proyecto:

- A. Creación de la Agencia de Protección de datos Personales, organismo público que tiene por objetivo velar por la efectiva protección de los derechos consagrados en la ley
- B. La ley se aplicará cuando la persona en cuestión se encuentre en territorio nacional, en este sentido se toma en cuenta que el mandatario independiente del lugar de establecimiento o constitución, realice la trata de datos personales a nombre de un responsable o constituido en territorio nacional. Especificando también cuando, el responsable o el mandatario no se encuentren en territorio nacional, pero sus operaciones de trata de datos personales fuesen destinados a titulares que se encuentren en Chile.
- C. Se definen los derechos ARCO, tales son personales, intransferibles y no pueden limitarse por ningún acto o convención.
- D. El tratamiento de datos personales requiere el consentimiento del titular, salvo en casos específicos como: obligaciones económicas, obligaciones legales, obligaciones de contrato, para el ejercicio de un

derecho ante los tribunales u órganos públicos.

- E. El tratamiento de datos personales sensibles requiere el consentimiento expreso del titular, o en el caso específico de que ya los haya hecho públicos, cuando resulte indispensable para salvaguardar la vida o salud de una persona, y en materia judicial. Aquellos datos sensibles corresponden a información relativa a la salud y al perfil biológico, de carácter biométrico y referente a niños, niñas y adolescentes
- F. Las obligaciones del responsable de datos es deber informar al titular, asegurar que el tratamiento sea lícito, informar de manera precisa, suprimir o anonimizar los datos cuando esto sea necesario y cumplir con el resto de deberes y principios que establece la ley.

En suma, la nueva legislación corrige la ausencia de un organismo fiscalizador que se encargue de velar por la protección de datos personales, además de tomar en cuenta cuando se lleve a cabo la trata de datos personales de nacionales por organismos fuera de Chile. Define específicamente los límites del consentimiento del titular respecto a los datos y responsabiliza al organismo que almacene los datos de informar al titular sobre las acciones a realizar sobre estos.

#### VII. ESTÁNDAR EUROPEO DE LA REGULACIÓN DE PROTECCIÓN DE DATOS Y EL NUEVO PROYECTO DE LEY

Una vez revisada la ley de protección de datos de Chile, sus inicios, evolución y futuro es posible comparar que tan completa está en relación al reglamento general de protección de datos (RGPD) de la Unión Europea. Debido a la extensión del reglamento europeo será desglosado en los siguientes puntos:[18]

- A. Ámbito de aplicación: El reglamento aplica a todas las organizaciones que procesen datos personales de residentes en la Unión Europea, independientemente de la ubicación de la organización
- B. Principios básicos:
  - 1. El procesamiento de datos debe realizarse de manera lícita, leal y transparente para el titular de los datos.
  - 2. Los datos personales deben recogerse con fines específicos y explícitos y no deben procesarse de manera incompatible con estos fines.
  - 3. Se deben recoger solo los datos estrictamente necesarios para la finalidad prevista.
  - 4. Los datos deben ser precisos y estar actualizados.
  - 5. Los datos personales deben conservarse solo el tiempo necesario para la finalidad del procesamiento.

C. Derechos de los interesados:

1. Las personas tienen derecho a obtener confirmación de si se están procesando sus datos personales y, en caso afirmativo, a acceder a estos datos.
2. Los titulares de datos tienen derecho a corregir datos inexactos o incompletos. Las personas tienen derecho a que se borren.
3. Las personas tienen derecho a que se borren sus datos personales en determinadas circunstancias.
4. Los titulares de datos tienen derecho a recibir sus datos personales en un formato estructurado y legible, y a transmitir esos datos a otra organización.

D. Responsabilidad y rendición de cuentas: Las organizaciones son responsables de demostrar el cumplimiento de los principios del Reglamento y deben implementar medidas para garantizar la protección de datos personales.

E. Delegado de protección de datos (DPD): Algunas organizaciones deben designar un DPD, un responsable de supervisar la conformidad con el reglamento.

F. Notificación de violaciones de datos: Las organizaciones están obligadas a notificar a la autoridad de control y, en algunos casos, a los titulares de datos, en caso de una violación de seguridad de los datos

G. Transferencias internacionales: Las transferencias de datos personales fuera de la Unión Europea solo están permitidas bajo ciertas condiciones.

Al realizar una comparación entre el reglamento europeo y la legislación chilena actual (19.628), es posible advertir las distintas falencias y ausencias existentes respecto a la protección de datos personales; como la ausencia de un órgano fiscalizador, la inexistencia de la hipótesis de que un tercero preste sus servicios de trata de datos fuera del país a un nacional en el ámbito de la territorialidad, el problema de no definir específicamente qué es un dato personal en comparación al reglamento, como también alguna especificación respecto a datos de carácter sensible, la definición del principio de consentimiento queda al debe en comparación a la europea.[19][20]

La nueva legislación en relación al reglamento corresponde a un avance ya que implementa ciertas normativas de la regulación europea, entre ellos toma la territorialidad de la ley, los principios básicos, los derechos de los interesados, e incluso adopta la creación de un delegado de protección

de datos en la normativa europea y agrega el carácter general que representa la agencia de protección de datos, ya que el delegado de protección de datos debe existir para que vele por la seguridad de los datos y el cumplimiento de la normativa, mientras que la agencia de protección de datos es un organismo general que fiscaliza, finalmente es posible evidenciar la diferencia existente entre la extensión respecto a las extensiones del reglamento en comparación con la nueva normativa chilena.[21]

VIII. POSIBLES EFECTOS DE LA NUEVA LEGISLACIÓN

Tomando en consideración la nueva normativa a llegar en los próximos años es necesario evaluar cuáles serían las consecuencias respecto a los efectos que esta legislación podría tener en cuanto a la protección de datos personales. De esta forma es posible asumir, que las responsables de los datos personales hagan una re evaluación y reestructuración respecto a qué datos son necesarios para realizar sus servicios. Es además imperativo crear otros medios por los cuales se puedan reemplazar estos métodos de identificación de usuarios como lo es el RUT/RUN. Otro efecto no inmediato de la ley corresponde a la probable desaparición de los sitios de búsqueda de personas por medio de Rol Unico Tributario, esto tomando en cuenta que las legislaciones y aplicaciones de la ley tienen un efecto transitorio en cuanto a respecta a su promulgación y su entrada en vigencia, el cual es necesario para la correcta adaptación de las organizaciones respecto a esta nueva legislación. En suma, es plausible asumir que los datos de las personas nacionales ya no estarán disponibles de la manera que actualmente se presenta o disponen en internet.[22]

La introducción de nueva normativa sobre la protección de datos personales conllevará varios cambios importantes:

- Reevaluación de la Necesidad de Datos: Las organizaciones tendrán que revisar qué datos personales son realmente necesarios para sus operaciones y servicios. Esto implica una reestructuración de sus prácticas de recolección y procesamiento de datos.
- Búsqueda de Alternativas al RUT/RUN: Será crucial desarrollar métodos alternativos para la identificación de usuarios, reduciendo la dependencia del Rol Único Tributario o Rol Único Nacional como principales medios de identificación.
- Impacto en Sitios de Búsqueda de Personas: Probablemente, los sitios web que permiten la búsqueda de personas utilizando el RUT/RUN experimentarán cambios significativos o incluso podrían desaparecer, en conformidad con las nuevas regulaciones de privacidad.
- Período Transitorio y Adaptación: La implementación de la nueva legislación incluirá un período transitorio que permitirá a las organizaciones adaptarse a las nuevas normas. Este período es crucial para garantizar una transición suave y el cumplimiento efectivo de la ley.

- Disponibilidad de Datos en Internet: Es probable que la información personal de los ciudadanos ya no esté disponible en Internet de la manera en que lo está actualmente, lo que refleja un enfoque más estricto en la privacidad y protección de datos.[24]

## IX. CONCLUSION

Desde los albores de la era informática, los ataques cibernéticos y los incidentes relacionados con la seguridad de la información han sido una amenaza persistente. En la actualidad, con la omnipresencia de Internet y la proliferación de servicios digitales, la información personal y sensible está cada vez más expuesta, incrementando el riesgo de filtraciones y uso indebido de estos datos.

Este informe ofrece un análisis detallado de la situación actual de la ley de protección de datos personales en Chile, explorando su evolución histórica, su estado presente y las perspectivas a futuro. Se enfoca en el proceso de reforma legislativa en curso, que busca actualizar la ley 19.628 a los estándares contemporáneos y abordar los retos actuales en materia de ciberseguridad. La investigación destaca las limitaciones de la legislación vigente, comparándola con las normativas de otros países y en particular con la legislación europea. El estudio concluye enfatizando la necesidad imperiosa de reformar la ley chilena de protección de datos para adecuarla a las realidades del mundo digital actual, y examina las implicaciones que el nuevo proyecto de ley podría tener en el tratamiento de datos personales por parte de las organizaciones, invitando a una reevaluación de sus prácticas en este ámbito.

El fenómeno de los ataques informáticos y los incidentes cibernéticos ha sido una constante desde los primeros días de la informática. En la era actual, donde la interconexión a través de Internet y el uso de diversas plataformas digitales son omnipresentes, la exposición de información personal y sensible se ha incrementado dramáticamente. Esto conlleva un mayor riesgo de que los datos personales sean filtrados y utilizados de manera indebida, una preocupación creciente tanto para individuos como para organizaciones. Abarcando su desarrollo histórico, desde su promulgación en 1999 hasta la actualidad, se analiza cómo ha evolucionado esta legislación frente a los desafíos emergentes en el campo de la ciberseguridad. Se observa que, a pesar de los esfuerzos iniciales, la ley ha quedado rezagada frente a las demandas del entorno digital moderno. Actualmente, Chile se encuentra en un proceso de transformación legislativa, buscando actualizar la ley 19.628 para alinearla con los estándares actuales de protección de datos y ciberseguridad. Este esfuerzo de modernización apunta a abordar las deficiencias identificadas en la ley vigente, especialmente en lo que respecta a la prevención de filtraciones de datos y la protección contra el uso indebido de información personal.

El análisis incluye una comparación detallada entre la ley chilena y las legislaciones de otros países, destacando cómo ciertas regiones, especialmente Europa con su Reglamento General de Protección de Datos (GDPR), han establecido marcos legales más robustos y efectivos en este ámbito. Esta comparación internacional resalta las áreas en las que Chile podría mejorar para garantizar una mejor protección de los datos personales.

Finalmente, el informe subraya la urgencia de una reforma legislativa en Chile en materia de protección de datos personales. Se enfatiza la importancia de adaptar la legislación a las necesidades y desafíos del mundo digital contemporáneo, considerando los posibles efectos que el nuevo proyecto de ley podría tener en el manejo de datos personales por parte de las organizaciones. Esta reevaluación legislativa es crucial para asegurar que tanto las entidades privadas como las públicas manejen los datos personales con los más altos estándares de seguridad y responsabilidad, adaptándose a un panorama global cada vez más enfocado en la ciberseguridad y la privacidad de datos.

## X. REFERENCIAS

- [1] Tipifica figuras penales relativas a la informática, ley N° 19223, Biblioteca del Congreso Nacional de Chile, 7 de Junio de 1993. Disponible en el siguiente enlace: <https://www.bcn.cl/leychile/navegar?idNorma=30590&buscar=ley%2B19223>
- [2] Sobre protección de la vida privada, Ley N° 19623, Biblioteca del Congreso Nacional de Chile, 28 de Agosto de 1999, Disponible en: <https://www.bcn.cl/leychile/navegar?idNorma=141599>
- [3] Establece normas sobre delitos informáticos, deroga la ley N° 19223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest , Ley N° 21459, Biblioteca del Congreso Nacional de Chile, 20 de Junio del 2022, disponible en: Ley Chile - Ley 21459 - Biblioteca del Congreso Nacional (bcn.cl)
- [4] “Ley 21.096, que consagra el derecho a protección de los datos personales,” Biblioteca del Congreso Nacional de Chile, 2018. [En línea]. Disponible: [\[https://www.bcn.cl/leychile/navegar?idNorma=1119730&tipoVersion=0\]](https://www.bcn.cl/leychile/navegar?idNorma=1119730&tipoVersion=0)
- [5] “Nueva ley de datos personales en Chile,” WeLiveSecurity, 2023. [En línea]. Disponible: [\[https://www.welivesecurity.com/es/privacidad/nueva-ley-datos-personal-es-chile/\]](https://www.welivesecurity.com/es/privacidad/nueva-ley-datos-personal-es-chile/).
- [6] “Evaluación de la Ley 19.628, Cámara de Diputados,” Evaluación De Ley, 2019. [En línea]. Disponible: [\[https://www.evaluaciondelaley.cl/wp-content/uploads/2019/07/informe\\_final\\_ley\\_19628\\_con\\_portada.pdf\]](https://www.evaluaciondelaley.cl/wp-content/uploads/2019/07/informe_final_ley_19628_con_portada.pdf).
- [7] “Ley 21.096, acercamiento a una nueva ley de protección de datos: Historia de La Ley::Historia de la Ley (bcn.cl),” BCN, 2023. [En línea]. Disponible: [\[https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/7551/\]](https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/7551/).
- [8] “Proyecto de ley de protección de datos,” Cámara, 2023. [En línea]. Disponible: [\[https://www.camara.cl/cms/noticias/2023/05/08/tratamiento-de-datos-personales-tendra-nuevo-marco-legal/\]](https://www.camara.cl/cms/noticias/2023/05/08/tratamiento-de-datos-personales-tendra-nuevo-marco-legal/).

- [9] “Nueva ola de correos extorsivos circula en Chile y otros países,” WeLiveSecurity, 2023. [En línea]. Disponible: <https://www.welivesecurity.com/laes/2023/07/06/nueva-ola-de-correos-extorsivos-circula-en-chile-y-otros-paises/>.
- [10] “Vulneración de datos personales: lo privado en público,” CiperChile, 2022. [En línea]. Disponible: [\[https://www.ciperchile.cl/2022/05/06/vulneracion-de-datos-personales-lo-privado-en-publico/\]](https://www.ciperchile.cl/2022/05/06/vulneracion-de-datos-personales-lo-privado-en-publico/).
- [11] “Aumento de los ciberataques en Chile en 2023: Lo que dicen las cifras,” Guioteca, 1 abril 2023. [En línea]. Disponible: [\[https://enteldigital.cl/blog/chile-registra-aumento-de-ciberataques-duran-te-primer-trimestre-del-2023-y-es-el-tercer-pa%C3%ADs-con-m%C3%A1s-v%C3%ADctimas-de-latam\]](https://enteldigital.cl/blog/chile-registra-aumento-de-ciberataques-duran-te-primer-trimestre-del-2023-y-es-el-tercer-pa%C3%ADs-con-m%C3%A1s-v%C3%ADctimas-de-latam).
- [12] “El sumario del Servel que terminó con funcionario destituido por masiva filtración de datos personales,” BioBioChile, 2023. [En línea]. Disponible: [\[https://www.biobiochile.cl/especial/bbcl-investiga/noticias/articulos/2023/05/05/el-sumario-del-servel-que-termino-con-funcionario-destituido-por-masiva-filtracion-de-datos-personales.shtml\]](https://www.biobiochile.cl/especial/bbcl-investiga/noticias/articulos/2023/05/05/el-sumario-del-servel-que-termino-con-funcionario-destituido-por-masiva-filtracion-de-datos-personales.shtml).
- [13] “Panorama de amenazas en América Latina 2023,” Kaspersky, 2023. [En línea]. Disponible: [\[https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/#:~:text=Nueva%20epidemia%3A%20el%20phishing%20se,a%205%20ataques%20por%20minuto\]](https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/#:~:text=Nueva%20epidemia%3A%20el%20phishing%20se,a%205%20ataques%20por%20minuto).
- [14] “Hackeo a Carabineros en medio de la crisis expone 10.515 archivos: entre ellos hay datos de inteligencia,” CiperChile, 2019. [En línea]. Disponible: [\[https://www.ciperchile.cl/2019/10/29/hackeo-a-carabineros-en-medio-de-la-crisis-expone-10-515-archivos-entre-ellos-hay-datos-de-inteligencia\]](https://www.ciperchile.cl/2019/10/29/hackeo-a-carabineros-en-medio-de-la-crisis-expone-10-515-archivos-entre-ellos-hay-datos-de-inteligencia).
- [15] J. Carey, A. Pinochet y C. Silva, “Los cambios que establece la nueva ley de datos personales en Chile,” Lex Latin, 2021. [En línea]. Disponible en: [\[https://www.carey.cl/wp-content/uploads/filebase/Lex-Latin-Los-cambios-que-establece-la-nueva-ley-de-datos-personales-en-Chile.pdf\]](https://www.carey.cl/wp-content/uploads/filebase/Lex-Latin-Los-cambios-que-establece-la-nueva-ley-de-datos-personales-en-Chile.pdf).
- [16] “Fundación Datos Protegidos. (2023). No doy mi Rut y tengo mis razones. [En línea]. Disponible: [\[https://datosprotegidos.org/no-doy-mi-rut/\]](https://datosprotegidos.org/no-doy-mi-rut/).
- [17] “Ciberataque expone información de 10 millones de chilenos en foros de hackers,” ElMostrador, 2023. [En línea]. Disponible: [\[https://www.elmostrador.cl/noticias/sin-editar/2023/10/18/ciberataque-expone-informacion-de-10-millones-de-chilenos-en-foros-de-hackers/\]](https://www.elmostrador.cl/noticias/sin-editar/2023/10/18/ciberataque-expone-informacion-de-10-millones-de-chilenos-en-foros-de-hackers/).
- [18] “Desafíos para adecuarse al margen europeo,” Revistas CES, [En línea]. Disponible: [\[https://revistas.ces.edu.co/index.php/derecho/article/view/6806\]](https://revistas.ces.edu.co/index.php/derecho/article/view/6806).
- [19] “Carta fundamental Europea, artículo de datos personales,” Consilium, [En línea]. Disponible: [\[https://www.consilium.europa.eu/es/policies/data-protection/#:~:text=El%20art%C3%ADculo%208%20de%20la,conciernan%20y%20a%20obtener%20su%20rectificaci%C3%ADn\]](https://www.consilium.europa.eu/es/policies/data-protection/#:~:text=El%20art%C3%ADculo%208%20de%20la,conciernan%20y%20a%20obtener%20su%20rectificaci%C3%ADn).
- [20] “Reglamento Europeo de protección de datos personales,” Europa, [En línea]. Disponible: [\[https://eurlex.europa.eu/legalcontent/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504\]](https://eurlex.europa.eu/legalcontent/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504).
- [21] “Las claves sobre el nuevo reglamento europeo de protección de datos,” Signaturit, [En línea]. Disponible: [\[https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos\]](https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos).
- [22] “Una breve historia de los virus informáticos y los que nos depara el futuro,” Kaspersky, [En línea]. Disponible: [\[https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds\]](https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds).
- [23] “Cuanto gasta una empresa para recuperarse después de un ciberataque,” La Republica, 27 de Julio de 2019, [En línea], Disponible [\[https://www.larepublica.co/internet-economy/cuanto-gastan-las-empresas-para-recuperarse-despues-de-un-ciberataque-2889536\]](https://www.larepublica.co/internet-economy/cuanto-gastan-las-empresas-para-recuperarse-despues-de-un-ciberataque-2889536).
- [24] Informe del costo de una vulneración de datos 2020, Autor: IBM [En línea], Disponible: [https://sadvisor.com/wp-content/uploads/2021/05/LA-Spanish\\_CostOfADataBreachReport\\_2020\\_eBook\\_ES.pdf](https://sadvisor.com/wp-content/uploads/2021/05/LA-Spanish_CostOfADataBreachReport_2020_eBook_ES.pdf).

## XI. BIOGRAFIAS



**Pamela Hermosilla** nacida en Valparaíso, Chile, el 8 de octubre de 1974. Graduada de Universidad Técnica Federico Santa María (UTFM Ingeniero Civil en Informática (UTFSM), Diplomada en Comercio Electrónico y Logística Empresarial (UTFSM), Auditor Interno ISO 9001 (Brain & Cia Consultores), MBA of Chief Information Officer CIO (Abet Open University), Diplomada en Docencia Universitaria de la Pontificia Universidad Católica de Valparaíso (PUCV), Diplomada en Formación Virtual Universitaria (PUCV), Symposium for Entrepreneurship Educators (Luksic Scholars – Babson College). Asesorías: miembro del Consejo Público Privado de la red Fortalece Pyme, Valparaíso - Corfo, integrante del Board de Directores, de la incubadora Chrialys PUCV. Desarrollo profesional en áreas de Aseguramiento de calidad en gestión de proyectos, Planificación estratégica organizacional, Rediseño curricular basado en competencias, Habilidades de Innovación y emprendimiento en estudiantes de ingeniería, Gamificación en el proceso de enseñanza y aprendizaje.



**Dr.(c)Sebastián Berrios** nacido el 7 diciembre de 1986. Actualmente candidato a doctor en Ingeniería informática en la Pontificia Universidad Católica de Valparaíso. Graduado de Ingeniería Civil en Computación e Informática en la Universidad De Las Américas. Magíster en Ciencias de la Ingeniería y Magíster en Ingeniería en Informática en la Pontificia Universidad Católica de Valparaíso. Actualmente docente del área de Ciberseguridad y Administrador de TI de la escuela de ingeniería informática de la Pontificia Universidad Católica de Valparaíso. Cursando un Diplomado de Inclusión en Educación en la Pontificia Universidad Católica de Valparaíso, con una duración de 140 horas. Además, se cursó un Diplomado en Seguridad de la Información de 132 horas en la Universidad de Chile y un Diplomado en Ciberseguridad de 96 horas en la misma universidad. También se obtuvo un Diplomado en Ciberseguridad de 100 horas en el Instituto Profesional IACC.



**Dr. Héctor Allende** destacado profesional en el campo de la ingeniería informática. Obtuvo su Doctorado en Ingeniería Informática en 2015 en la Universidad Técnica Federico Santa María, Chile, un reconocido centro de estudios en la región. Antes de ello, en 2009, completó su Magíster en Ciencias de la Ingeniería Informática y se graduó como Ingeniero Civil Informático en la misma universidad. Su formación académica en estas prestigiosas instituciones le ha proporcionado una sólida base en la ingeniería informática, permitiéndole desarrollarse y destacarse en su campo.

# Incorporación de la Inteligencia Artificial en el aula: Cómo comenzar a involucrar las nuevas tecnologías en la enseñanza del Derecho y la Ingeniería

Sebastián Barletta, Instituto de Estudios Interdisciplinarios de Ingeniería, UCASAL

**Abstract--** Este trabajo aborda ideas reflexivas sobre la necesidad de integrar nuevas herramientas tecnológicas a la educación contemporánea, para enfrentar los desafíos éticos y legales planteados por el surgimiento del campo de la inteligencia artificial (IA). A medida que la IA transforma la teoría y práctica de las ciencias, surgen cuestiones críticas en torno a: la privacidad de datos, equidad algorítmica y responsabilidad que se asocian a diversos riesgos que hasta podrían revestir características antropogénicas. El autor propone en este trabajo un enfoque que, desde la ética y responsabilidad tecnológica nos asista para en primer término comenzar a involucrar las nuevas tecnologías en la enseñanza del derecho y la ingeniería y así preparar académicamente a nuestros futuros profesionales capacitándolos para interactuar críticamente con la tecnología de IA, destacando la importancia de distinguir términos como privacidad de datos, ciencia de datos y la IA misma.

**Index Terms--** Aprendizaje Adaptativo, Innovación Pedagógica, Competencias Digitales, Colaboración Interdisciplinaria, Acceso a la Educación

## I. INTRODUCTION

Propone el autor la necesidad de actualizar los contenidos educativos para reflejar los desarrollos recientes en la legislación de IA, como la Ley de IA del Parlamento Europeo y otras experiencias normativas no comunitarias. Enfatizamos la importancia de incorporar conocimientos técnicos en el currículo en especial el jurídico, ya que los sistemas de IA operan sobre representaciones numéricas de datos. Los futuros abogados deben estar equipados para entender y cuestionar las bases de los modelos de IA, incluyendo los mecanismos de auditoría y la gestión de sesgos. Incorporamos el principio de responsabilidad de Hans Jonas para abordar los desafíos éticos y legales de la IA y por tanto en la nueva educación. Este principio subraya la necesidad de considerar las consecuencias a largo plazo de nuestras acciones y decisiones tecnológicas, guiando el desarrollo y aplicación ética de la tecnología.

En conclusión, abogamos por una educación contemporánea que aborde proactivamente los desafíos de la IA, equipando a los profesionales con herramientas necesarias para garantizar

la justicia y equidad en la era digital.

La integración de conocimientos de derecho, ética y tecnología es esencial para preparar a los futuros profesionales para liderar con responsabilidad, en un mundo cada vez más influenciado por la inteligencia artificial.

Un abordaje pedagógico con foco en la integridad de la educación actual, se centra en la necesidad de adaptar la misma a los desafíos éticos y legales planteados por la inteligencia artificial (IA). La generación masiva de datos sintéticos y su impacto en la sociedad destacan la importancia de proteger a sus usuarios y datos en un entorno cada vez más interconectado y multidisciplinario. La proliferación de datos plantea desafíos significativos en términos de privacidad, seguridad y equidad, haciendo urgente la necesidad de una regulación adecuada y una comprensión integral de las implicaciones éticas y sociales de la recopilación y el uso de datos. En este contexto, la convergencia dentro del campo de la IA, plantea cuestiones éticas y jurídicas de gran envergadura, desde la privacidad individual hasta la equidad en el acceso y uso de la información. La ausencia de un marco normativo sólido y actualizado podría exponernos a riesgos como la discriminación algorítmica y la vulneración de derechos fundamentales, socavando los cimientos de una sociedad justa y democrática. Por lo tanto, la elaboración de una estrategia educativa adaptada a las exigencias del siglo XXI se erige como un imperativo ineludible, garantizando la protección de los usuarios, en cuanto a privacidad y derechos individuales, promoviendo la transparencia en los sistemas de IA, la equidad en su aplicación y la rendición de cuentas de aquellos involucrados en su desarrollo y utilización. En este nuevo entorno, la responsabilidad toma diferentes formas: personal, profesional e institucional, siendo la Justicia una entidad reguladora clave del comportamiento beneficioso de una comunidad para sí misma. Es preciso no solo garantizar la protección de los usuarios de estas tecnologías, su privacidad y los derechos individuales, sino también promover la transparencia en los sistemas de inteligencia artificial, la equidad en su aplicación y la rendición de cuentas de aquellos involucrados en su desarrollo y utilización. La regulación ética y responsable de la IA, se propone en este trabajo sea inicialmente basada en el principio de responsabilidad del filósofo alemán Hans Jonas, el cual es fundamental para

abordar estos desafíos y garantizar un futuro digital más equitativo y transparente. Este principio subraya la necesidad de considerar las consecuencias a largo plazo de nuestras acciones y decisiones tecnológicas, guiando el desarrollo y aplicación ética de la tecnología, el cual entiende el autor podría ser de aplicación desde la tarea educativa hasta la praxis profesional.

## II. EL ESTADO DEL ARTE

La Unión Europea ha sido pionera en la regulación de la inteligencia artificial (IA), buscando garantizar el desarrollo y Incorporación de la Inteligencia Artificial en el aula: Cómo comenzar a involucrar las nuevas tecnologías en la enseñanza del Derecho y la Ingeniería Sebastián Barletta, Instituto de Estudios Interdisciplinarios de Ingeniería, UCASAL P 2 uso seguro y ético de esta tecnología. En abril de 2021, la Comisión Europea propuso el primer marco regulatorio de la UE para la IA, que clasifica los sistemas de IA según el riesgo que suponen para los usuarios, estableciendo obligaciones para proveedores y usuarios en función de dicho nivel de riesgo. Esta normativa busca garantizar que los sistemas de IA sean seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente, con una supervisión humana para evitar resultados perjudiciales. El Parlamento Europeo también ha enfatizado la importancia de una definición uniforme y tecnológicamente neutra de la IA, que pueda aplicarse a futuros sistemas, abordando así cuestiones de responsabilidad y ética. La normativa de la UE sobre protección de datos personales, como el RGPD, complementa estas regulaciones, enfatizando la transparencia y el respeto por la privacidad de las personas. Los cambios recientes en la legislación de la UE reflejan un compromiso con la regulación ética y responsable de la IA, abordando desafíos como la discriminación algorítmica, la transparencia y la rendición de cuentas, y estableciendo un precedente para el desarrollo de marcos legales en otras regiones. La convergencia entre los avances tecnológicos y las estructuras legales es crucial para garantizar un futuro digital equitativo y sostenible.

## III. PROBLEMÁTICA DE ESTUDIO

Para abordar adecuadamente la problemática de la IA en la educación, es fundamental enfocarse en una enseñanza que promueva la comprensión y evaluación crítica de los sistemas de IA. Esto incluye enseñar a los futuros profesionales del derecho e ingeniería a identificar y manejar los riesgos asociados con la IA, así como a aplicar principios éticos y legales en su uso y regulación. La educación debe adaptarse para incluir temas como la transparencia de la IA, la protección de datos personales y la prevención de la discriminación algorítmica, preparando a los estudiantes para enfrentar los desafíos de la era digital de manera informada y responsable. Para abordar la problemática de estudio en la educación jurídica relacionada con la inteligencia artificial (IA), se podría evaluar realizar incorporaciones específicas:

- **Inclusión de Cursos Específicos sobre IA:** Incorporar cursos y programas que se enfoquen en la IA y sus implicaciones legales y éticas, cubriendo temas como privacidad de datos, discriminación algorítmica y responsabilidad legal de los sistemas de IA.
- **Desarrollo de Habilidades Críticas:** Fomentar el pensamiento crítico y la capacidad de evaluación ética entre los estudiantes, para que puedan identificar y abordar los riesgos y desafíos asociados con la IA.
- **Enseñanza Interdisciplinaria:** Promover un enfoque interdisciplinario que integre conocimientos de derecho, ética, tecnología y ciencia de datos, preparando a los estudiantes para trabajar en entornos multidisciplinarios.
- **Simulaciones y Estudios de Caso:** Utilizar simulaciones y estudios de caso para proporcionar experiencias prácticas que permitan a los estudiantes aplicar sus conocimientos en situaciones reales relacionadas con la IA.
- **Colaboraciones con Expertos en IA:** Establecer colaboraciones con expertos en IA y tecnología para proporcionar una perspectiva actualizada y práctica sobre los avances y desafíos en el campo de la IA.
- **Actualización Continua del Currículo:** Asegurar que el currículo se mantenga actualizado con los desarrollos más recientes en IA y legislación relacionada, para que los estudiantes estén preparados para enfrentar los desafíos emergentes. Al implementar estas diferentes tareas combinado con el uso de las nuevas tecnologías mejoramos la eficacia en proteger a los estudiantes, y mejoraremos exponencialmente en prepararlos para abordar de manera efectiva los desafíos éticos y legales que plantea la IA también en su futura práctica profesional.

## IV. EL PRINCIPIO DE RESPONSABILIDAD TECNOLÓGICA COMO BASE DE LA PROPUESTA

A Si bien la conexión entre ciencias dentro del campo de la IA, ofrece oportunidades emocionantes y prometedoras, también plantea desafíos significativos que deben abordarse. A continuación, se enuncian algunos de los dilemas emergentes, tomando como premisa el denominado principio de responsabilidad, bajo la formulación del filósofo alemán Hans Jonas [4], quien argumenta que la ciencia y la tecnología deben orientar su desarrollo al bien de la humanidad y nunca apostar, en las apuestas de la acción, la existencia o la esencia del hombre en su totalidad. Para una mejor expresión de estas ideas conviene citar al autor: “...porque sobre todo la irreversibilidad de los procesos puestos en marcha, hasta que no podamos hacer proyecciones seguras **no habrá mayor valentía que la cautela, que en todo caso será un mandamiento de la responsabilidad. La inseguridad puede ser nuestro destino permanente, lo cual tiene**

**consecuencias morales".** Así siguiendo las ideas propuestas por Hans, se propone la génesis de una cultura tecnológica que impulse a las ciencias, que convergen en el ecosistema de IA, tratar propósitos específicos como los siguientes:

A) Protección de la Privacidad y los Derechos de los Individuos: La legislación podría establecer normas más claras y estrictas para la recopilación, el almacenamiento y el uso de datos personales, garantizando el consentimiento informado y la protección de la privacidad de los individuos.

B) Transparencia y Explicabilidad de los Sistemas de IA: Se podrían requerir medidas técnico-legales para garantizar que los sistemas de IA sean transparentes y explicables, lo que permitiría a los individuos comprender cómo se toman las decisiones que les afectan.

C) Equidad y No Discriminación: La legislación podría incluir más disposiciones técnico legales para prevenir la discriminación algorítmica y garantizar la equidad en el desarrollo y la implementación de sistemas de IA, mediante la identificación y mitigación de sesgos y prejuicios.

D) Responsabilidad y Rendición de Cuentas: Además de las regulaciones existentes respecto de la responsabilidad sobre la manipulación de datos (Ley de Datos Personales N° 25326 [5]). Se podrían establecer mecanismos para garantizar la responsabilidad de las partes involucradas en el desarrollo y el uso de sistemas de IA, así como para proporcionar recursos legales efectivos en caso de daños causados por decisiones algorítmicas erróneas o sesgadas. Esta nueva pedagogía podría proporcionar un marco educativo sólido y adaptable que promueva el desarrollo ético y responsable de la IA, al tiempo que protege los derechos y las libertades fundamentales de los individuos en un mundo cada vez más digitalizado y conectado. Estos elementos podrían tomarse como base para el resguardo de la intimidad y derechos individuales, en el marco de una legislación acorde a la era digital.

#### *A. Perspectivas Filosóficas y Metodológicas: Unificación de las Ciencias en el Derecho Digital*

A los fines propuestos podemos adicionar también explorar la necesidad de desarrollar una Teoría General Unificada (TGU) de Inteligencia Artificial (IA) [6,7]. Esta TGU busca unificar el lenguaje de las diversas ciencias y tecnologías convergentes. La metodología propuesta para este fin se basa en la teoría de "La unidad de la ciencia", una de las tesis fundamentales de la filosofía de la ciencia surgida del Círculo de Viena, específicamente del empirismo lógico. Esta tesis, concebida como un programa, fue elaborada por sucesivos artículos, encuentros y congresos, principalmente por Otto Neurath y Rudolf Carnap, dando lugar al proyecto más ambicioso de esta corriente epistemológica: la International Encyclopedia of Unified Science (Enciclopedia Internacional de la Ciencia Unificada) [8]. El autor en su propuesta reafirma la importancia de avanzar hacia la redacción de una TGU como método para abordar el déficit de integridad presente en el sistema de protección de la humanidad frente a los desafíos emergentes derivados de la utilización de IA. Este enfoque se complementa en su fundamentación en el principio de responsabilidad tecnológica antes descripto.

#### *B. Análisis de la unidad de la ciencia desde una perspectiva filosófica, en particular, el enfoque de Rudolf Carnap.*

Luego de que, a comienzos de los años treinta y debido a la influencia de Otto Neurath, optara por el fisicalismo en vez del fenomenalismo que había caracterizado su primera gran obra, La construcción lógica del mundo, y luego de que, a través de conversaciones con Tarski y Gödel y de la obra fundamentalmente de Tarski, se diera cuenta de que sería posible hablar de las relaciones entre lenguaje y hechos en el nuevo metalenguaje de la semántica; así como de que realizara sus investigaciones sobre los conceptos disposicionales a mediados de esos años, Carnap sostiene que podemos hablar de la unidad del lenguaje de la ciencia si y sólo si todos los términos científico empíricos:

(a) se refieren a objetos, propiedades o relaciones físicas observables; o

(b) pueden ser reducidos a términos de tipo (a) (a través de definiciones explícitas o condicionales). La llamada "tesis del fisicalismo" afirma que esa base de reducción común consiste en una clase muy pequeña y homogénea de términos del lenguaje fisicalista.

De dicha tesis se toman los conceptos de la unidad del lenguaje y la de la unidad de la ciencia. [8]

#### *C. Discusión sobre la aplicación de la metodología formal en el derecho digital y la regulación de la IA.*

La metodología formal propuesta por Carnap, centrada en el uso de formas lingüísticas en lugar de objetos concretos, puede aplicarse fructíferamente en el campo del derecho digital. Esto resulta crucial considerando la rapidez con que evolucionan los usos y aplicaciones de la tecnología. Asimismo, el enfoque formal facilita comprender y explicar los resultados de los algoritmos de manera comprensible para jueces, abogados y ciudadanos. Sin embargo, es necesario establecer salvaguardias normativas que aseguren la imparcialidad y el debido proceso en los sistemas de inteligencia artificial con implicancias legales. Deben exigirse mecanismos de auditoría que evalúen periódicamente posibles sesgos en los datos de entrenamiento y validen la ausencia de variables ocultas que podrían influir indebidamente en las decisiones. Asimismo, los sujetos afectados deben contar con canales claros para cuestionar resultados automatizados que les sean lesivos, sometiéndolos a revisión por jueces humanos. Solo aplicando estándares de transparencia, explicabilidad, no discriminación y recursos efectivos, se podrá aprovechar el potencial de la inteligencia artificial en el derecho de forma ética y garantizando a la vez los derechos fundamentales de las personas. La metodología formal resulta una herramienta útil en este propósito, siempre y cuando vaya acompañada de las oportunas salvaguardias jurídicas.

#### *D. Desafíos y Potenciales Riesgos en la Convergencia Ética y Jurídica.*

La convergencia entre el derecho y la IA plantea importantes desafíos y riesgos que es necesario abordar para garantizar un desarrollo responsable de esta tecnología. Uno de los principales desafíos es establecer mecanismos para mantener la imparcialidad de los sistemas legales ante la creciente

automatización de tareas judiciales. Los sesgos presentes en los datos de entrenamiento podrían replicarse en las decisiones algorítmicas de forma difícil de detectar, vulnerando el principio de igualdad ante la ley. Cuestiones como el género, la raza o el estado socioeconómico no deben introducir sesgos en el acceso a la justicia. Otro riesgo es la pérdida de explicabilidad de algunas herramientas de IA. Esto dificulta comprobar que las decisiones cumplen efectivamente con normas jurídicas y principios 4 constitucionales, sin un control humano adecuado, con impactos negativos difíciles de subsanar.

Finalmente, la masiva recolección y procesamiento de información personal por parte de algoritmos plantea desafíos sobre la privacidad y protección de datos. Es necesario establecer salvaguardias legales que aseguren el consentimiento informado, la portabilidad de la información, y recursos para ejercer efectivamente los derechos de los usuarios.

De no gestionarse adecuadamente, estos desafíos y riesgos podrían minar la legitimidad del sistema jurídico y vulnerar derechos fundamentales.

## V. CONCLUSIONES

En este ensayo, logramos poner el foco de la comunidad científica y académica en el abordaje de la creciente intersección entre la IA y el ámbito académico, destacando los desafíos y las oportunidades que esta convergencia plantea para nuestra sociedad ante la innegable realidad que nos encontramos en un momento crucial en el que la proliferación de inteligencias artificiales con capacidad potencialmente superior a la humana representa tanto una promesa como una posible amenaza para nuestra existencia. En el análisis, se han abordado ideas reflexivas sobre la necesidad de integrar nuevas herramientas tecnológicas a la educación contemporánea, para enfrentar los desafíos éticos y legales planteados por el surgimiento del campo de la inteligencia artificial (IA), subrayando la importancia de adoptar un enfoque que esté fundamentado en el principio de Responsabilidad, tal como lo propone Hanz Jonas, y que explore la necesidad actual e inminente de desarrollar una Teoría General Unificada (TGU) de la inteligencia artificial. Esta TGU serviría como un marco teórico y normativo que nos permitiría abordar de manera efectiva y adaptativa los desafíos éticos y legales derivados de la convergencia tecnológica actual para luego incorporarlos a los programas y cursos académicos. Además, se ha propuesto la aplicación de principios del fisicalismo positivo, en línea con la tesis de la unidad de la ciencia de Rudolf Carnap, como un medio para garantizar la flexibilidad y la adaptabilidad de nuestras regulaciones frente a la rápida evolución de la tecnología. Esta aproximación nos permitiría no solo proteger los derechos individuales y la privacidad, sino también promover la equidad y la transparencia en el desarrollo y la aplicación de sistemas de IA. Sin embargo, también resalta que es importante reconocer los desafíos y riesgos asociados con esta convergencia, como los sesgos algorítmicos y la falta de explicabilidad en los sistemas de IA. Para abordar estos problemas, necesitamos implementar programas educativos que nos permita contar con

salvaguardias legales efectivas que garanticen la imparcialidad, la transparencia y el respeto de los derechos fundamentales de los individuos. En conclusión, propone el camino hacia una educación ética y efectiva de la inteligencia artificial mediante un enfoque integral y colaborativo que integre los principios éticos y los avances tecnológicos más recientes. Solo de esta manera podremos aprovechar todo el potencial de la IA para el bienestar de la humanidad, asegurando al mismo tiempo que sus beneficios se distribuyan de manera equitativa y justa en nuestra sociedad.

## VI. REFERENCES

- [1] de la Unión Europea, C. (2001). Carta de los Derechos Fundamentales de la Unión Europea: explicaciones relativas al texto completo de la carta. Oficina de Publicaciones Oficiales de las Comunidades Europeas.  
[https://commission.europa.eu/aid-development-cooperationfundamental-rights/your-rights-eu/eu-charter-fundamental-rights\\_es](https://commission.europa.eu/aid-development-cooperationfundamental-rights/your-rights-eu/eu-charter-fundamental-rights_es)
- [2] Europeo, P. (2023). Ley de IA de la UE: primera normativa sobre inteligencia artificial. Obtenido de Noticias Parlamento Europeo: <https://www.europarl.europa.eu/news/es/headlines/society/20230601STO93804/ley-de-ia-de-la-ueprimera-normativa-sobre-inteligencia-artificial>.
- [3] Decisión de Ejecución (UE) 2019/419 de la Comisión de 23 de enero de 2019 con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la ley sobre la protección de la información personal.  
Texto:  
<https://eurlex.europa.eu/legalcontent/ES/TXT/?uri=CELEX:32019D0419>
- [4] Jonas, Hans, El principio de responsabilidad. Ensayo de una ética para la civilización tecnológica, \_Herder, Madrid, 1995, ps.309-310
- [5] de Datos Personales, L. D. P. (2000). 25.326 Congreso de la Nación Argentina. 30 Oct 2000. Consultada 09/12/2021). Disponible en: <https://www.argentina.gob.ar/normativa/nacional/ley-2532664790/texto>.
- [6] Pérez, G. V. (2009). ¿ Es posible la ciencia UNIFICADA?. Elementos: Ciencia y cultura, 16(73), 57-61.
- [7] Corvalán, Juan G. Tratado de inteligencia artificial y derecho: tomo I/ Juan Gustavo Corvalán...; dirigido por Juan Gustavo Corvalán – 2da ed. Ciudad Autónoma de Buenos Aires: La Ley. 2023.-
- [8] Valdovinos Pérez, 2009, p. 57



## VII. BIOGRAFÍA



Sebastián Daniel Barletta,  
Técnico Superior en computación,  
Abogado – Diplomado en derecho  
penal económico, cuenta con  
Cursos de Posgrado en  
Investigaciones Penales  
Patrimoniales, y especializaciones  
en MLA/PFT/PADM, análisis de  
Riesgos Corporativos RSG ESG,

Litigante en Delitos complejos, Investigador en Inteligencia  
Artificial. – Temas de interés Anti corrupción, Ética,  
Inteligencia Artificial. –

Email: [estudiobarletta@outlook.com](mailto:estudiobarletta@outlook.com) .

LinkedIn: [www.linkedin.com/in/sebastian-Barletta](http://www.linkedin.com/in/sebastian-Barletta)

# Innovación en la enseñanza del Derecho del Consumidor: Integrando la IA para un aprendizaje significativo

PERUGINI, Pablo Matías<sup>1</sup>

**Abstract--** El presente artículo explora la integración de tecnologías emergentes, en particular la inteligencia artificial, en la enseñanza del derecho del consumidor con el objetivo de fomentar el aprendizaje significativo. Se abordan los desafíos actuales en la enseñanza de esta rama legal, destacando la importancia de atraer y comprometer a los estudiantes en una materia de constante dinamismo. Se proponen herramientas y aplicaciones de inteligencia artificial para mejorar la comprensión de conceptos y promover la resolución de casos de conflicto del consumidor. Además, se discuten los beneficios y oportunidades que esta integración ofrece.

**Términos del Índice--** Derecho del consumidor- Inteligencia artificial – Neuromarketing - Políticas públicas- Aprendizaje significativo - Resolución de problemas - Simulaciones interactivas - Tecnologías educativas.

## I. INTRODUCCIÓN

La enseñanza del derecho del consumidor enfrenta desafíos particulares en la actualidad a raíz del avance de la inteligencia artificial, que reversionó el proceso de enseñanza-aprendizaje en las aulas, dinamizó el proceso de abordaje judicial de los conflictos y potenció las tácticas empresariales mediante la utilización del neuromarketing.

En este contexto, el presente artículo se propone explorar soluciones innovadoras para abordar estos desafíos. La premisa fundamental consiste en la integración de tecnologías de inteligencia artificial (en adelante “IA”) en la enseñanza del derecho del consumidor, con el objetivo de promover un aprendizaje significativo.

En la travesía analítica de estas páginas, buscaré

aproximarme a los pilares fundamentales que subyacen la imperativa integración de la IA en el contexto educativo. Buscaré determinar los objetivos de esta integración (II), abordar los antecedentes y características de la IA conversacional (III), su relación con la protección del consumidor en la era digital (IV) y los desafíos y beneficios en la educación jurídica (V y VI). Finalmente se proponen diversas áreas de aplicación de la IA (VII) y se presentan herramientas específicas para el docente (VIII).

## II. OBJETIVOS DE LA INTEGRACIÓN DE LA IA AL AULA

Los rápidos avances tecnológicos plantean múltiples riesgos y desafíos que trascienden los debates políticos y los marcos regulatorios existentes.

CUCKIERMAN sostiene que *el desafío que supone la incorporación de tecnologías de la información y la comunicación, puede actuar como una ventana abierta a la oportunidad para la innovación y la renovación de las instituciones educativas*<sup>2</sup>.

La visión de Cuckierman destaca que la incorporación de tecnologías de la información y la comunicación (TIC) en la educación plantea desafíos que actúan como catalizadores para la transformación. Este proceso desafiante impulsa a educadores y estudiantes a desarrollar nuevas competencias digitales, fomentando un aprendizaje activo y continuo para adaptarse al entorno digital en evolución.

Siguiendo este vector de pensamiento, resulta una oportunidad la integración de la IA a las aulas, que se manifiesta en la innovación pedagógica, potenciando la personalización del aprendizaje. Esta capacidad de adaptar métodos de enseñanza a estilos individuales crea un entorno educativo más receptivo, atendiendo las necesidades específicas de cada estudiante y mejorando la eficacia del proceso educativo.

Adicionalmente, la IA propicia una renovación de estrategias didácticas, promoviendo enfoques pedagógicos más interactivos y participativos. Este cambio hacia prácticas educativas dinámicas, respaldado por recursos multimedia y actividades en línea, marca una transición significativa de métodos más tradicionales hacia una educación más dinámica y centrada en el estudiante.

En Mayo de 2019, la Conferencia Internacional sobre la IA y la Educación<sup>3</sup> congregó a Estados miembros, organizaciones internacionales, sociedad civil e industria de la IA. Propició un espacio de debate sobre la anticipación de las competencias fundamentales para prosperar en la era de la IA. Además, sirvió como escenario para el intercambio de ideas respecto a las últimas tendencias en el campo de la IA y su influencia directa en la configuración de enfoques educativos y

<sup>1</sup> Abogado (Universidad FASTA, 2012), con especialización en Derecho Público. Posgrado en Derecho del consumidor y del usuario (UNMDP, 2014). Profesional en ejercicio de funciones en la Dirección General de Protección al Consumidor de la Municipalidad de General Pueyrredón, a cargo del área de instrucción acusatoria. Docente de la cátedra de “Derecho del Consumidor” (Universidad FASTA). Miembro del Observatorio del Consumidor (UNMDP).

<sup>2</sup> Citado por Giunti, G. M. (2010). Tecnología educativa: recursos, modelos y metodologías / Uriel Cuckierman; Julieta Rozenhauz y Horacio Santángelo.

Buenos Aires: Prentice Hall, 2009. xix, 208 p. ISBN 978 987 615 070-5. Información, Cultura Y Sociedad, (22), 128-131. <https://doi.org/10.34096/ics.i22.778>

<sup>3</sup> Texto del Documento final, disponible en: <https://unesdoc.unesco.org/ark:/48223/pf0000368303>

procesos de aprendizaje. Se realizó una evaluación reflexiva de las lecciones extraídas de nuevas políticas y estrategias nacionales.

En el panorama actual de la educación, la IA se presenta como un recurso transformador con el potencial de abordar desafíos cruciales. Al innovar las prácticas de enseñanza y aprendizaje, la IA puede acelerar el progreso hacia la consecución del ODS 4<sup>4</sup>: «Educación de calidad». Las características y beneficios de esta tecnología pueden mejorar la calidad y accesibilidad de la educación al facilitar y adaptarse a las necesidades de cada estudiante.

Resulta paradójico y ejemplificador que, al indagar sobre el futuro del impacto de la inteligencia artificial en la educación, se pueda recurrir a la propia inteligencia artificial para obtener perspectivas reveladoras. Un ejemplo ilustrativo de esta paradoja es consultar directamente a la IA, como el propio ChatGPT, para explorar cómo la inteligencia artificial puede influir y moldear el proceso educativo. Este caso ilustra a las claras la interconexión entre la tecnología emergente y su capacidad para proporcionar insights valiosos sobre su propio impacto en la educación<sup>5</sup>.

#### A. Retos para todos

La integración de la inteligencia artificial no debe percibirse como una amenaza, sino como una oportunidad para potenciar la enseñanza. Los educadores pueden aprovechar la IA para personalizar el aprendizaje, identificar áreas de mejora y ofrecer retroalimentación más precisa. La colaboración armoniosa entre educadores y tecnologías avanzadas puede enriquecer la experiencia educativa, preparando a los estudiantes para un mundo donde la habilidad de interactuar con la tecnología de manera crítica y ética es esencial.

En este contexto, se viene sosteniendo que los educadores enfrentan el crucial desafío de estimular tanto el pensamiento crítico como el lateral en sus alumnos<sup>6</sup>. Esta tarea adquiere una importancia singular en un mundo caracterizado por su complejidad y constante cambio, donde la capacidad de adaptación y la búsqueda de soluciones creativas se vuelven indispensables.

Explorar diversas estrategias para cultivar el pensamiento crítico y lateral se convierte en una necesidad, mediante la

implementación de actividades y proyectos que exijan a los estudiantes abordar problemas de manera analítica y creativa.

Los docentes tienen la misión de promover el desarrollo de un conocimiento holístico en los estudiantes<sup>7</sup>. Este imperativo implica aprehender la interconexión de diversas esferas del saber y aplicar los preceptos aprendidos en contextos variados. La instauración del conocimiento holístico se puede efectuar mediante la participación activa de los estudiantes en empresas y actividades que aborden problemáticas del ámbito real, facultándoles para aplicar sus conocimientos en situaciones cotidianas.

En el dominio de las competencias personales e interpersonales, los educadores desempeñan una función cardinal al incitar a los estudiantes a cultivar destrezas en la comunicación, la resolución de problemas y la toma de decisiones. Estrategias como el fomento del trabajo en equipo y diversas modalidades de tutorías pueden ser implementadas con miras a este propósito. Además, reviste suma importancia propiciar la autonomía y la asunción de responsabilidades por parte de los estudiantes en sus procesos de aprendizaje, animándolos a adoptar decisiones y a ejercer la independencia.

Otro aspecto de consideración es el rol docente como facilitador y mediador del proceso de aprendizaje. Este cometido conlleva una disposición para colaborar con los estudiantes, brindarles retroalimentación y orientarlos en su trayectoria de aprendizaje. Esta interacción estrecha entre docentes y estudiantes contribuye de manera significativa a la creación de un entorno educativo enriquecedor y participativo.

La atracción y el compromiso de los estudiantes son fundamentales para una educación efectiva. La IA puede hacer que el aprendizaje sea más atractivo y comprometido al proporcionar interacciones personalizadas y adaptadas a las necesidades individuales de los estudiantes.

*En esencia, la IA transforma los ambientes y las posibilidades de la educación. Por eso se requiere una conversación educativa amplia (...) Es importante integrar a los docentes y educadores en este diálogo y en las maneras en las cuales puede introducirse la tecnología en las escuelas con un sentido de pertinencia pedagógica y apropiación por parte de docentes y estudiantes<sup>8</sup>.*

---

<sup>4</sup> La UNESCO busca aprovechar el potencial de las tecnologías de la IA en línea con la Agenda de Educación 2030. Al mismo tiempo, asegura que la aplicación de la IA en contextos educativos se guíe por principios fundamentales de inclusión y equidad: <https://www.unesco.org/es/digital-education/artificial-intelligence>

El enfoque intrínseco de la UNESCO hacia la IA es centrado en el ser humano. Busca integrar la IA como una herramienta para abordar las desigualdades en el acceso al conocimiento, la investigación y la diversidad cultural. La aspiración es que la IA no amplíe las brechas tecnológicas dentro y entre países. La visión de "IA para todos" debe facilitar que cada individuo se beneficie de la revolución tecnológica, accediendo a innovaciones y conocimientos.

En el marco del Consenso de Beijing, la UNESCO ha desarrollado una guía para los responsables de formular políticas educativas sobre inteligencia artificial. Esta publicación tiene como objetivo enriquecer la comprensión compartida de las oportunidades y desafíos que la IA presenta para la

educación. Además, destaca las implicaciones de la IA en las competencias básicas necesarias en esta era de transformación tecnológica.

<sup>5</sup> "El impacto de la IA en la educación del futuro: una conversación reveladora con ChatGPT", disponible en <https://cabreramc.com/el-impacto-de-la-ia-en-la-educacion-del-futuro-una-conversacion-reveladora-con-chapgpt/>

<sup>6</sup> <https://ined21.com/era-de-la-inteligencia-artificial/>

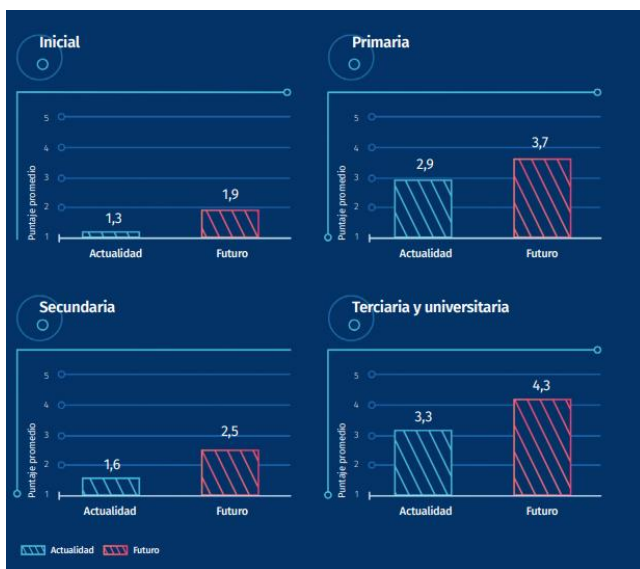
<sup>7</sup> "Cómo aprende y cómo enseña el docente", publicado por el Programa Interdisciplinario de Investigaciones en Educación (PIIE) y el Instituto de Cooperación Iberoamericana ICI. Disponible en: [https://biblioteca.clacso.edu.ar/Chile/piie/20170823052546/pdf\\_562.pdf](https://biblioteca.clacso.edu.ar/Chile/piie/20170823052546/pdf_562.pdf)

<sup>8</sup> "El Futuro de la Inteligencia Artificial en América Latina", Organización de Estados Iberoamericanos (OEI), pág.44, disponible en <https://oei.int/oficinas/secretaria-general/publicaciones/el-futuro-de-la-inteligencia-artificial-en-educacion-en-america-latina>

## B. Relevancia presente y futura de la IA en función del nivel educativo

La Fundación ProFuturo y la Organización de los Estados Iberoamericanos (OEI) mapearon las tendencias actuales y futuras sobre el desarrollo de la IA en Educación en América Latina<sup>9</sup>. Realizaron una encuesta dirigida a tres grupos de actores de la región: académicos del campo de la IA y educación, miembros del ecosistema privado de la tecnología y la educación y funcionarios gubernamentales de las áreas dedicadas a la tecnología y educación.

Los encuestados contestaron a la pregunta “Valore en qué medida está impactando actualmente la IA en los siguientes niveles educativos y en qué medida impactará en 2030 en una escala de 1 a 5 en América Latina (1. Nada – 5. Mucho)”.



10

En este sentido, es esencial fomentar la adquisición de habilidades digitales tanto en profesores como en estudiantes, permitiéndoles comprender los entornos del avance tecnológico y sus variadas potencialidades y desafíos.

Del gráfico puede observarse que los encuestados perciben que la IA tiene y tendrá un mayor impacto en la educación superior. Entre ellos, el nivel universitario ya registra hoy esa capacidad única de la IA para personalizar el aprendizaje, abordar desafíos académicos y desarrollar habilidades propias de estos tiempos. Estas características, posicionan a los estudiantes universitarios para enfrentar los desafíos y oportunidades de un mundo cada vez más digital y complejo.

## III. LA IA EN EL ECOSISTEMA UNIVERSITARIO DE LOS ESTUDIANTES DE DERECHO

BLEDEL describía hace varias décadas el perfil del estudiante universitario de derecho<sup>11</sup>. Allí invitaba a dejar la “enseñanza formalista y dogmática, fuertemente impregnada por tradiciones civilistas en el campo jurídico y por principios individualistas en el orden político-económico” evolucionando hacia un “régimen pedagógico fundado en una comprensión amplia y directa de los fenómenos sociales”.

En la elevación del Anteproyecto de Reforma del Plan de Estudios de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata, BLEDEL señalaba:

*Se ha impreso un sello...transformando a nuestras escuelas de Derecho en centros de preparación de futuros magistrados judiciales o apoderados y letrados patrocinantes. Debe reaccionarse contra este estado de cosas (...) Ha llegado la hora de abrir otros horizontes a las nuevas promociones de estudiantes que ingresen en nuestras facultades de derecho y ciencias sociales. Es imprescindible preparar otro tipo de profesional. Lo reclaman exigencias actuales del país en el orden político, económico y social*<sup>12</sup>.

El destacado jurista se preocupaba por la orientación tradicional de las facultades de derecho, históricamente centradas en la formación de futuros magistrados y letrados litigantes. Entendemos que su llamada a *reaccionar contra este estado de cosas* hoy también debe ser escuchada, ya que las nuevas tecnologías emergen como un factor clave que impulsa este cambio de paradigma.

La introducción y adopción de tecnologías en el ámbito jurídico están transformando la práctica jurídica y exigen una adaptación en la formación de los futuros profesionales.

CORVALÁN afirma que no es solo “un cambio de nombre o una mera actualización de conceptos, sino que se trata de repensar una organización que será atravesada por las innovaciones más disruptivas que ha creado el ser humano en toda su historia”<sup>13</sup>.

La digitalización de la información y la incorporación de herramientas tecnológicas en la investigación jurídica están alterando la manera en que los abogados acceden y gestionan la información jurídica. La capacidad de utilizar eficientemente bases de datos electrónicas, herramientas de análisis de datos y recursos en línea se convierte en una habilidad esencial para el abogado moderno<sup>14</sup>.

Además, la inteligencia artificial y la automatización están transformando procesos rutinarios, liberando tiempo para que los profesionales se centren en tareas más estratégicas y creativas. La comprensión de cómo estas tecnologías pueden

<sup>9</sup> Ver Informe completo, disponible en <https://oei.int/oficinas/secretaria-general/publicaciones/el-futuro-de-la-inteligencia-artificial-en-educacion-en-america-latina>

<sup>10</sup> Gráfico obtenido en: <https://oei.int/oficinas/secretaria-general/publicaciones/el-futuro-de-la-inteligencia-artificial-en-educacion-en-america-latina>

<sup>11</sup> BLEDEL, Rodolfo, “La enseñanza de las Ciencias Jurídicas y Sociales en nuestras facultades de derecho”, disponible en <https://hdl.handle.net/11185/3958>

<sup>12</sup> Ídem.

<sup>13</sup> CORVALÁN, Juan G., “Hacia una administración pública 4.0: digital y basada en inteligencia artificial. Decreto de ‘tramitación digital completa’”, LA LEY del 17/08/2018, p. 1; LA LEY 2018-D, 917.

<sup>14</sup> Cfr. DOBRATINICH, Gonzalo Ana (Dir.), “Derecho y nuevas tecnologías”, 1a ed. - Ciudad Autónoma de Buenos Aires, La Ley, 2021, disponible en <http://www.derecho.uba.ar/publicaciones/libros/pdf/2021-derecho-y-nuevas-tecnologias.pdf>

ser aplicadas éticamente en el ejercicio legal se convierte en parte integral de la formación del nuevo profesional del derecho.

Desde una perspectiva interdisciplinaria, la introducción de la IA puede catalizar un acercamiento más holístico al estudio del derecho. La capacidad de la IA para analizar grandes volúmenes de datos de manera eficiente permite una integración más efectiva de las diversas dimensiones sociales, económicas y políticas que subyacen en cualquier situación legal. Esta integración es esencial para que los estudiantes de derecho comprendan las complejas interrelaciones que existen dentro del ordenamiento jurídico.

En este sentido, la IA puede ser una herramienta valiosa para facilitar el contacto permanente entre docentes y estudiantes de derecho con disciplinas conexas. Al procesar vastas cantidades de información de manera rápida y precisa, la IA puede ayudar a identificar patrones y correlaciones entre cuestiones legales y factores económicos, sociológicos o políticos. Esta capacidad de análisis avanzado amplía las fronteras del conocimiento jurídico, permitiendo una comprensión más profunda de cómo el derecho impacta y es impactado por otras disciplinas.

Existe una variedad de herramientas de IA, entre las que se incluyen marcos para aprendizaje profundo, automatizaciones, algoritmos preentrenados para procesamiento de lenguaje natural, herramientas especializadas en clasificación sincrónica de datos, entre otros<sup>15</sup>.

Así es que la introducción de la IA en el ámbito universitario puede potenciar el desarrollo de habilidades analíticas y de resolución de problemas en los estudiantes de derecho. Al exponerlos a herramientas tecnológicas avanzadas, se les proporciona la capacidad de abordar cuestiones jurídicas con otra perspectiva y otros instrumentos. Esto no solo beneficia su formación académica, sino que también los prepara para enfrentar los desafíos multidisciplinarios que encontrarán en la práctica profesional.

Las aplicaciones de inteligencia artificial (IA) emergen como potenciales facilitadores de experiencias de aprendizaje interactivo y personalizado para los estudiantes universitarios de ciencias jurídicas. Considerando la complejidad de la formación legal, la IA, en la forma de chatbots educativos, puede desempeñar un papel central al interactuar con los estudiantes, proporcionar respuestas a sus preguntas y presentar información de manera dinámica, adaptándose a sus necesidades específicas.

En la búsqueda del aprendizaje significativo, la IA se posiciona como una herramienta estratégica al ofrecer ejemplos y aplicaciones prácticas que conectan los conceptos legales con situaciones del mundo real. Este enfoque no solo facilita la comprensión profunda, sino que también establece puentes

entre la teoría jurídica y su aplicación práctica, fortaleciendo así la formación de los estudiantes.

También la IA puede desempeñar un papel significativo al crear un entorno virtual de aprendizaje amigable y atractivo, que contribuye a desarrollar una conexión con el tema jurídico propuesto, fomentando así la motivación intrínseca en los estudiantes.

Los asistentes virtuales de IA pueden ser programados para interactuar de manera amigable y proporcionar retroalimentación positiva. Esto puede ayudar a los estudiantes universitarios a desarrollar una conexión emocional con el tema y sentirse más motivados.

#### IV. CONVERSACIONES EN EL AULA: EL DIÁLOGO SOCRÁTICO POTENCIADO POR LA IA CONVERSACIONAL<sup>16</sup>

Estoy convencido que las ciencias jurídicas tienen arraigada una naturaleza tradicional en el proceso de enseñanza-aprendizaje: un método magistral, centrado en la exposición del docente, enfocado una dialéctica de base teórica.

Sin embargo en la actualidad existe un cambio de perspectiva que será potenciado por el impacto de la IA y que se erige como un componente esencial del nuevo proceso educativo. Es en este contexto donde se enmarca la utilización del *Socratic Seminar o Diálogo Socrático*<sup>17</sup>:

Esta estrategia de enseñanza-aprendizaje implica que el profesor inicie la discusión con una opinión o pregunta provocadora, y los alumnos contribuyan sucesivamente conectando sus intervenciones con las anteriores. El rol del profesor se transforma en el de moderador, guiando la conversación al introducir los puntos clave de la teoría.

Los estudiantes, atentos a los argumentos de sus compañeros, enlazan estas ideas con sus propias opiniones, con la libertad de introducir nuevos aspectos que consideren relevantes, incluso relacionados con el desarrollo mismo del diálogo. Al concluir la discusión, tanto el profesor como los alumnos resumen las ideas principales, fortaleciendo así los conceptos analizados durante el intercambio. Este enfoque promueve una participación activa y fomenta la reflexión colectiva, consolidando la comprensión de los temas abordados.

*Se ha constatado la aptitud de este método para potenciar en los estudiantes no solo las competencias puramente cognitivas, sino también aquellas otras más de tipo experimental como la capacidad comunicativa, el dominio del lenguaje, la acometividad de los problemas, el espíritu investigador, el trabajo en equipo, el desarrollo de propuestas y el razonamiento crítico*<sup>18</sup>.

La integración del diálogo socrático en la enseñanza del

<sup>15</sup> Inteligencia artificial: conceptos básicos y aplicaciones en el desarrollo, publicación del BID: <https://blogs.iadb.org/conocimiento-abierto/es/inteligencia-artificial/>

<sup>16</sup> Para profundizar en esta metodología pedagógica, ver CASTRO FAUNE, C. (2012), "El método socrático y su aplicación pedagógica contemporánea", Bajo Palabra Revista de Filosofía, 7: 441-452. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/3941748.pdf>

<sup>17</sup> CHICHARRO LÁZARO, Alicia, "El diálogo socrático como parte de la formación práctica en los estudios de derecho", Revista Jurídica De Investigación E Innovación Educativa (REJIE Nueva Época), (14), 41-59. <https://doi.org/10.24310/REJIE.2016.v0i14.7670>

<sup>18</sup> CHICHARRO LÁZARO, Alicia, Op. Cit., pág. 14.



derecho del consumidor se potencia significativamente al aprovechar la inteligencia artificial conversacional como herramienta facilitadora. En este enfoque educativo, se propone que el docente -asumiendo el papel de moderador- utilice la IA conversacional para dinamizar y enriquecer la interacción constante con los estudiantes, propiciando un diálogo colaborativo y participativo.

La metodología del diálogo socrático, al considerar todos los criterios y puntos de vista relacionados con un problema práctico, comparte similitudes con la inteligencia artificial conversacional. En ambos casos, el intercambio abierto y bidireccional fomenta la emergencia de perspectivas diversas y preguntas inesperadas. Al igual que en el diálogo socrático, donde cada pregunta desencadena un efecto dominó de reflexiones, las plataformas de inteligencia artificial conversacional están diseñadas para responder y adaptarse a las preguntas y comentarios de los usuarios, explorando así una variedad de temas.

La conexión entre estas metodologías reside en la capacidad de ambas para propiciar diálogos dinámicos que van más allá de las preguntas planteadas, permitiendo una exploración más profunda y completa de los temas en consideración.

En el marco de las simulaciones de IA, donde los estudiantes asumen diversos roles en un conflicto de derecho del consumidor, el diálogo socrático se convierte en una experiencia aún más inmersiva. La IA conversacional actúa como un facilitador dinámico, permitiendo que el profesor lance preguntas iniciales de manera interactiva. Los estudiantes, en sus distintos roles, participan activamente en el diálogo, hilando sus intervenciones con las anteriores y aprovechando la libertad de introducir nuevos aspectos o cuestiones relevantes.

La IA conversacional proporciona al docente la capacidad de guiar la discusión de manera fluida, introduciendo tópicos esenciales y adaptando la dirección del diálogo socrático según las decisiones y avances de los estudiantes. Este enfoque no solo fomenta la aplicación práctica de conocimientos legales, sino que también mejora la accesibilidad y la inmediatez de la retroalimentación, fundamental para la comprensión profunda de los temas.



Ilustraciones creadas mediante la IA de [bing.com](https://www.bing.com), luego de cargar el siguiente *prompt*: “Te pido que crees un dibujo que ilustre el uso de la IA conversacional como facilitadora de los diálogos entre docente y alumnos”

De este modo, la inteligencia artificial conversacional no

solo sirve como un canal para la comunicación, sino que también puede desempeñar un papel activo al generar preguntas estimulantes, proporcionar información adicional o presentar escenarios específicos relacionados con el conflicto consumeril simulado. Esta interacción bidireccional entre el docente y la IA, junto con la participación de los estudiantes, crea un entorno educativo dinámico y adaptable.

Al finalizar el diálogo, la inteligencia artificial conversacional contribuye a la síntesis de las ideas principales, facilitando la consolidación del aprendizaje. Además, permite una revisión más detallada de los conceptos erróneos identificados, brindando oportunidades adicionales para la corrección y el perfeccionamiento del entendimiento.

La IA conversacional transforma la experiencia educativa en la enseñanza del derecho del consumidor. Se presenta como un facilitador invaluable para las interacciones educativas. En el acápite IX se verá el desarrollo de este aplicativo en un caso concreto y con una simulación interactiva con un asistente virtual.

En el paradigma educativo actual, la interacción y participación activa de los estudiantes son elementos esenciales para un aprendizaje significativo. En este contexto, surge un concepto crucial: el “prompt”. Este término se refiere a las preguntas, enunciados o estímulos que el docente proporciona a los estudiantes para desencadenar respuestas, reflexiones o acciones específicas<sup>19</sup>.

La inclusión del concepto de prompt adquiere un significado dialéctico fundamental en el proceso educativo. En lugar de adoptar un enfoque unidireccional donde el docente simplemente transmite información, el uso estratégico de prompts fomenta la participación activa y el pensamiento crítico de los estudiantes. Estos estímulos no sólo guían el aprendizaje, sino que también impulsan la exploración autónoma, permitiendo a los estudiantes conectar conceptos, analizar situaciones y aplicar conocimientos en contextos prácticos.

En este sentido, el docente se convierte en un facilitador del diálogo educativo al emplear prompts efectivos. Estas preguntas cuidadosamente diseñadas estimulan la reflexión, la discusión y la generación de ideas, transformando el aula en un espacio dinámico donde el conocimiento se construye de manera colaborativa. En última instancia, la incorporación significativa de prompts en la enseñanza empodera a los estudiantes para ser partícipes activos en su propio proceso de aprendizaje.

En este contexto, el docente asume un papel crucial al orientar a los estudiantes en la generación de *prompts* efectivos. Esta habilidad de “saber preguntar” se convierte en una competencia esencial en la era digital, donde la destreza para formular preguntas que estimulen el pensamiento crítico y promuevan la exploración profunda de los temas adquiere una relevancia significativa.

En síntesis, la inteligencia artificial y la labor del docente convergen para enriquecer las conversaciones educativas,

<sup>19</sup> “Efectivos Prompt para Innovar la Enseñanza”, disponible en: <https://articulandoo.com/planificacion-docente-con-chatgpt/>

destacando la importancia de guiar a los estudiantes hacia interacciones significativas y reflexivas.

## V. IA Y PROTECCIÓN DEL CONSUMIDOR: DESAFÍOS JURÍDICOS EN LA ERA DIGITAL

Las nuevas tecnologías y prácticas comerciales han generado la necesidad de regulaciones específicas. En este sentido, el auge del comercio electrónico ha motivado la creación de normativas que protejan a los consumidores en transacciones en línea.

Por ejemplo, en nuestro país las Resoluciones 270/2020<sup>20</sup> y 271/2020<sup>21</sup> de la Secretaría de Comercio Interior incorporaron normativa del Mercosur al derecho interno y reglamentaron lo relativo a las contrataciones electrónicas de adhesión y a la solicitud de baja de servicios contratados en línea.

La Subsecretaría de Tecnologías de la Información, bajo la Jefatura de Gabinete de Ministros de nuestro país, emitió la disposición 2/2023 el 2 de junio pasado, aprobando las "Recomendaciones para una Inteligencia Artificial Fiable" junto con dos anexos explicativos<sup>22</sup>. Este acontecimiento ocurre en un contexto en el que las tecnologías, en especial aquellas basadas en Inteligencia Artificial (IA), están ganando protagonismo, ofreciendo niveles superiores de automatización, innovación y productividad.

Dentro de este panorama, las IA tienen el potencial de mejorar la eficiencia de la gestión estatal al optimizar los diseños e implementaciones de políticas y servicios. Esto ha generado la necesidad de garantizar la transparencia, equidad y responsabilidad en el desarrollo y uso de estas tecnologías. Con el objetivo de asegurar que los beneficios de los avances tecnológicos sean aprovechados por toda la sociedad, se han establecido normas claras. Estas normas buscan promover la responsabilidad en la recopilación y uso de datos personales, prevenir la discriminación algorítmica y gestionar los riesgos asociados al uso de la IA para evitar perjuicios.

El documento se centra en proporcionar herramientas tanto teóricas como prácticas para aquellos involucrados en proyectos de innovación pública mediante tecnologías, especialmente cuando se utiliza IA. En términos éticos, se destacan cuatro etapas dentro del ciclo de la IA: 1) diseño y modelado de datos, 2) verificación y validación, 3) implementación, y 4) operación y mantenimiento.

En resumen, este manual ofrece orientación tanto a nivel

teórico como práctico para aquellos que participan en el sector público, ya sea liderando proyectos de innovación, desarrollando tecnologías, adoptando soluciones desarrolladas por otros equipos o formulando especificaciones técnicas para adquisiciones.

### A. Impacto jurídico de la IA en el derecho del consumidor

El desarrollo de la IA y los procesos automatizados de toma de decisiones también presentan desafíos para la confianza y el bienestar del consumidor. Cuando los consumidores interactúan con un sistema de este tipo, se les debe informar adecuadamente sobre cómo funciona.

Dado el impacto de la IA, la Unión Europea viene desarrollando normas para gestionar sus oportunidades y amenazas<sup>23</sup>. El Parlamento Europeo instó el 23 de enero del 2020 a la Comisión Europea<sup>24</sup> que examine si es necesario adoptar medidas adicionales para proteger a los consumidores. En una resolución de la Comisión Parlamentaria de Mercado Interior del dicho Parlamento, solicita que aclare cómo va a garantizar que los consumidores estén protegidos ante prácticas comerciales desleales y/o discriminatorias, o de los riesgos que conllevan los servicios profesionales impulsados por la IA.

La axiología de estas directrices debería garantizar una mayor transparencia en los procesos de interacción con el consumidor y asegurarse de que solo se utilicen conjuntos de datos de alta calidad y sin sesgos. *Tenemos que asegurarnos de que se garantice la protección y la confianza del consumidor, que las normas de la UE sobre seguridad y responsabilidad por productos y servicios sean adecuadas para la era digital*<sup>25</sup>, señaló la presidenta de la comisión de Mercado Interior del PE, Petra De Sutter.

Por ejemplo, la Comisión ha referido que los agentes económicos siguen siendo plenamente responsables de que la IA respete las normas existentes en materia de protección de los consumidores. Igualmente, insiste en que debe prohibirse todo uso de los algoritmos con relación al comportamiento de los consumidores cuando se vulneren las normas existentes, y tales vulneraciones deben sancionarse en consecuencia.

Otra de las propuestas consistió en atender a las necesidades especiales de los consumidores vulnerables, como los niños, las personas mayores o las personas con discapacidad, así como las

<sup>20</sup> Mediante la Resolución 270/2020, la Secretaría de Comercio Interior (SCI), en su carácter de autoridad de aplicación de la Ley N° 24240 de Defensa del Consumidor (LDC), resolvió adoptar e incluir en la legislación nacional la Resolución 37 dictada por el Grupo Mercado Común del Mercado Común del Sur (Mercosur).

<sup>21</sup> La Resolución 271/2020 de la SCI estableció algunas precisiones sobre: (i) la forma y ubicación de la publicación de los contratos de adhesión en las páginas web de los proveedores de acuerdo lo establece el artículo 38 de la LDC, y (ii) la rescisión o baja de servicios en los términos del artículo 10 ter de la LDC.

<sup>22</sup> <https://www.argentina.gob.ar/noticias/argentina-aprobo-una-guia-para-una-inteligencia-artificial-etica-y-centrada-en-las-personas>

<sup>23</sup> El Parlamento Europeo creó una comisión especial sobre este asunto e hizo hincapié en la necesidad de contar con una legislación centrada en las personas.

Propuso un régimen de responsabilidad civil para la IA que establece quién es responsable cuando los sistemas de IA causan daños o perjuicios a los consumidores:

<https://www.europarl.europa.eu/news/es/headlines/priorities/inteligencia-artificial-en-la-ue/20200918STO87404/inteligencia-artificial-oportunidades-y-desafios>

<sup>24</sup> Resolución del Parlamento Europeo sobre procesos automatizados en la toma de decisiones: garantizar la protección del consumidor: [https://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/IMCO/DV/2020/01-22/RE\\_1194746\\_EN.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2020/01-22/RE_1194746_EN.pdf)

<sup>25</sup> "Inteligencia artificial: abordar los riesgos para los consumidores": <https://www.europarl.europa.eu/news/es/headlines/society/20200206STO72030/inteligencia-artificial-abordar-los-riesgos-para-los-consumidores>

personas con dificultades económicas o los consumidores con acceso limitado a internet ya que ellos necesitan salvaguardias específicas frente al potencial de la IA. Ante el aumento masivo de las compras online y la facilidad con la que los consumidores pueden llegar a endeudarse, el Parlamento Europeo impulsa nuevas normas de crédito al consumo, destinadas a proteger a las personas de las deudas por tarjetas de crédito, cargos por sobregiro y préstamos inadecuados para su situación financiera.

En este orden de ideas, el derecho del consumidor debe cuidar el modo de integración de la IA en el diseño e implementación de las prácticas comerciales de los proveedores. Para que la aplicación de esta técnica y el empleo de algoritmos no sean etiquetados como desleales y agresivos, es necesario no solo respetar el principio de dignidad, sino también salvaguardar la libertad y la privacidad de la persona humana, conforme a lo establecido en las declaraciones y tratados de derechos humanos<sup>26</sup>.

Además, la integración de tecnologías como la inteligencia artificial y el neuromarketing plantea desafíos que requieren respuestas legales para prevenir prácticas engañosas y garantizar que los consumidores tomen decisiones informadas.

Según un estudio<sup>27</sup>, el procedimiento de fijación de precios que utilizan los sitios web más conocidos, se realiza con un potente algoritmo que busca e identifica los productos más demandados en cada momento y si una o varias páginas bajan el precio un día por el motivo que sea, el precio del mismo producto en la gran plataforma comercial baja automáticamente.

## **B. El rol de los operadores del derecho del consumidor en la era de la IA**

La globalización y las transacciones transfronterizas también influyen en la evolución del derecho del consumidor. La creciente interconexión de los mercados exige la armonización de normativas para salvaguardar los derechos de los consumidores en contextos internacionales<sup>28</sup>.

La asimetría de información entre las empresas y los consumidores es un desafío clave en el derecho del consumidor. Por eso la enseñanza de esta asignatura debe abordar cómo los abogados pueden ayudar a equilibrar esta asimetría y empoderar a los consumidores para tomar decisiones informadas.

Cierto es que la respuesta jurídica y regulatoria debe adaptarse de manera continua para abordar las nuevas problemáticas y desafíos emergentes. La legislación debe ser ágil y eficaz, garantizando que las protecciones ofrecidas sean adecuadas y relevantes en un entorno en constante cambio.

*Los algoritmos interactúan en el mundo del consumo de masa*<sup>29</sup>. En este orden de ideas, la evolución del derecho del consumidor es esencial para mantener la eficacia y relevancia de las protecciones legales en el dinámico escenario del consumo contemporáneo. Por ejemplo, los términos y condiciones de un sitio web de comercio electrónico pueden modificarse regularmente para adaptarse a nuevas estrategias de negocio.

Además los algoritmos *están sirviendo para conformar plataformas de solución de conflictos de consumo*<sup>30</sup>. Las empresas utilizan algoritmos de inteligencia artificial para recopilar y analizar datos de consumidores, lo que les permite personalizar estrategias de marketing y publicidad. Esto incluye la optimización de la presentación de productos y servicios, lo que puede influir en las decisiones de compra de los consumidores sin que estos sean plenamente conscientes de ello.

El creciente uso de IA y el neuromarketing en el ámbito comercial plantea un escenario complejo en el cual la vulnerabilidad de los consumidores puede intensificarse de manera significativa. Este fenómeno se sustenta en la capacidad de estas tecnologías para influir en las decisiones y comportamientos de los consumidores de manera sutil, a menudo sin su conocimiento pleno o consentimiento explícito.

La incorporación de la inteligencia artificial (IA) en la creación de mensajes publicitarios presenta un impacto positivo al fortalecer la generación de actitudes favorables hacia una marca<sup>31</sup>. La capacidad de la IA para potenciar la fuerza del mensaje transmitido crea una conexión más efectiva con los consumidores, influyendo directamente en la percepción positiva de la marca<sup>32</sup>.

De allí que los marcos regulatorios deben adaptarse para abordar los desafíos específicos que surgen de la intersección entre la inteligencia artificial, el neuromarketing y la protección del consumidor. Se deben formar operadores del derecho que impulsen normativas claras y efectivas que aseguren la transparencia en las prácticas empresariales, protegiendo así la integridad de la toma de decisiones del consumidor.

<sup>26</sup> “¿Dónde deben estar los límites?: una perspectiva de derechos humanos sobre lo que está por llegar en el terreno de la inteligencia artificial y las tecnologías nuevas y emergentes”, declaración de Volker Türk, Alto Comisionado de las Naciones Unidas para los Derechos Humanos: <https://www.ohchr.org/es/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner>

<sup>27</sup> Índice de percepción de precios en torno a los distribuidores online, de la consultora Boomerang Commerce: <https://www.pnnewswire.com/news-releases/boomerang-commerce-introduces-price-perception-index-for-online-retailers-300019677.html>

<sup>28</sup> Cfr. PÉREZ, Romina Julieta; VACCARO, Valeria Verónica, “La implementación ética y responsable de la inteligencia artificial a luz de los principios del derecho del consumidor”, ponencia en el marco de las XXVIII Jornadas Nacionales de Derecho Civil:

<https://www.jornadasnacionalesderechocivil.org/ponencias/comisi%C3%B3n-5-derecho-de-los-consumidores>

<sup>29</sup> “Derecho del consumo y protección del consumidor sustentable en la sociedad digital del siglo XXI”, Silvia Barona Vilar (editora) Primera edición: junio, 2023 Santiago, Chile Ediciones Universidad Autónoma de Chile, DOI: <https://doi.org/10.32457/UA.167>, ISBN 978-956-6201-53-3.

<sup>30</sup> Ídem.

<sup>31</sup> DOOLEY, Roger, “Brandwashing? Neuroscience Marketing”, disponible en: <https://www.neurosciencemarketing.com/blog/articles/brandwashing.htm>

<sup>32</sup> FERRUZ-GONZÁLEZ, Sonia A., SIDORENKO-BAUTISTA, Pavel y SANTOS LÓPEZ, Cristina, “Neuromarketing e inteligencia artificial: el caso de la campaña Con mucho acento de Cruzcampo”, ex.comunicación, 13(2), 147-169, disponible en <https://doi.org/10.33732/ixc/13/02Neurom>



## VI. DESAFÍOS ACTUALES EN LA ENSEÑANZA DEL DERECHO DEL CONSUMIDOR

Los casos y situaciones en el derecho del consumidor evolucionan constantemente. Ese dinamismo es una riqueza fundamental para el entorno áulico.

La naturaleza cambiante de los casos y situaciones en el derecho del consumidor asegura que el contenido educativo sea relevante y esté actualizado. Los docentes tienen la oportunidad de incorporar ejemplos y casos recientes que reflejen las tendencias y desafíos actuales en el ámbito del consumo, lo que permite a los estudiantes conectar teoría y práctica de manera inmediata.

### A. Perspectiva del estudiante del derecho del consumidor

El dinamismo en los casos del derecho del consumidor obliga a los estudiantes a adaptarse a nuevos desafíos y problemáticas. Esto les proporciona una experiencia práctica en la resolución de problemas y les enseña a abordar cuestiones jurídicas emergentes. La capacidad de adaptación es una habilidad valiosa en un entorno jurídico que está constantemente respondiendo a cambios sociales, tecnológicos y económicos.

En el sector de las criptomonedas y las fintech, las regulaciones y prácticas comerciales cambian con rapidez. Las nuevas tecnologías emergen constantemente, lo que puede dificultar el seguimiento y comprensión de las implicaciones legales.

En la contratación de servicios en línea y en todo el ecosistema de comercio electrónico, los consumidores pueden estar mal informados acerca de los términos y condiciones. A menudo, no leen los largos contratos o no entienden las implicaciones legales, lo que crea una asimetría de información que favorece a las empresas.

Los ejemplos vistos ilustran como los nuevos profesionales del derecho del consumidor deben estar actualizados y formar su comprensión ante estos cambios, para asesorar de manera efectiva.

La evolución de los casos en el derecho del consumidor permite la interconexión con temas emergentes, como el neuromarketing y las ciencias del comportamiento. Los docentes pueden integrar estos conceptos de manera fluida, mostrando a los estudiantes cómo las tendencias actuales en comportamiento del consumidor se vinculan con los institutos

jurídicos clásicos y modernos.

Al enfrentarse a una variedad de situaciones cambiantes, los estudiantes adquieren una experiencia que los prepara para la complejidad de la práctica profesional. Desarrollan habilidades de resolución de problemas y toma de decisiones en un contexto legal dinámico, lo que mejora su capacidad para enfrentar desafíos del mundo real una vez que ingresen al ejercicio profesional.

### B. Educación Jurídica 2.0: nuevos desafíos del profesor de Derecho del Consumidor

En el entorno dinámico de las transformaciones en la educación jurídica, el docente del derecho del consumidor se enfrenta a desafíos significativos. Este escenario cobra una complejidad adicional al considerar la influencia directa de las ciencias del comportamiento, el neuromarketing y la innovación legal en el proceso educativo.

Vemos fundamental que los docentes se adapten y evolucionen para enfrentar los desafíos planteados por las nuevas fronteras en la educación jurídica y la innovación legal. La adaptabilidad se presenta como una habilidad clave para abordar las cambiantes demandas del contexto educativo y profesional.

La trascendencia de la IA en este nuevo rol docente del derecho del consumidor es innegable. El docente debe integrar la comprensión de cómo la inteligencia artificial puede influir en la toma de decisiones y en la gestión de casos en el ámbito del derecho del consumidor.

La intersección entre las ciencias del comportamiento y el derecho del consumidor adquiere una nueva dimensión con la incorporación de la inteligencia artificial<sup>33</sup>. Los docentes deben enseñar cómo las herramientas de la IA pueden analizar patrones de comportamiento del consumidor y cómo estas tecnologías pueden influir en la formulación de estrategias jurídicas para la protección del consumidor.

Esto significa que la enseñanza debe ser ágil y estar constantemente actualizada para reflejar los desarrollos actuales en la tecnología y su impacto en los derechos del consumidor.

Resulta sustancial preparar a los estudiantes para un futuro profesional donde la automatización puede afectar tareas rutinarias: presentación de escritos en la justicia, confección de documentos de traslado, notificaciones electrónicas, research inteligente de jurisprudencia, procesos judiciales automatizados<sup>34</sup>.

<sup>33</sup> Ver en este sentido: SALORT, Gastón, "Inteligencia artificial, marketing y derecho. Influencers virtuales y neuromarketing", disponible en <http://www.saij.gob.ar/gaston-facundo-salort-inteligencia-artificial-marketing-derecho-influencers-virtuales-neuromarketing-dacf200215-2020-10-15/123456789-0abc-defg5120-02fcanirtcod?q=%20%20autor%3Amedina&o=1&f=Total%7CTipo%20de%20Documento/Doctrina%7CFecha%7COrganismo%7CPublicaci%F3n%7CTribunal%7CTema%7CEstado%20de%20Vigencia%7CAutor%7CJurisdicci%F3n&t=24>

<sup>34</sup> El Poder Judicial de Río Negro dictó casi 6.000 fallos con sistemas automatizados. Aplicados dentro del fuero Contencioso Administrativo en labores estandarizadas y repetitivas, la nueva tecnología brinda mayor celeridad permitiendo a los empleados judiciales abocarse a tareas de mayor relevancia. El funcionamiento comienza cuando la Agencia de Recaudación Tributaria de Río Negro presenta una demanda y el sistema corrobora que esté toda la información necesaria y que sea sólida. Si los datos son correctos, genera el expediente de forma automática. Una vez que se constata la información, la IA genera la sentencia, que debe ser verificada y luego firmada. Ver más en:

Por ejemplo, la Fiscalía de Estado bonaerense creó el Laboratorio de Inteligencia Artificial con el objetivo de impulsar el análisis y la incubación de soluciones IA a partir de un modelo de innovación abierta que permita acelerar los procesos de investigación y desarrollo. Para su trabajo, la Fiscalía de Estado utiliza VELOX, una plataforma que funciona como base para cada una de las pruebas de concepto o prototipos que se desarrollan, con una arquitectura de microservicios (una sola plataforma que va sumando prototipos que prestan “servicio” al personal de abogacía según necesidades de cada área)<sup>35</sup>.

Estos antecedentes impulsan una tarea docente que promueva el desarrollo de habilidades complementarias.

Dada la creciente influencia de la inteligencia artificial en la profesión legal y el mercado laboral, el operador del derecho de estos tiempos debe entrenar la competencia en el LegalTech. Esto es, familiarizarse con las herramientas y plataformas tecnológicas diseñadas para mejorar la eficiencia en la práctica legal. Esto puede incluir sistemas de gestión de casos, software de análisis normativo y jurisprudencial, plataformas de resolución de disputas en línea, entre otras.

Otro desafío consiste en desarrollar una comprensión básica de cómo funcionan los algoritmos de inteligencia artificial y cómo pueden aplicarse en el campo jurídico. También se destaca la necesidad de ejercitar habilidades analíticas y de datos, donde los abogados gestionan la interpretación de información compleja, para tomar decisiones basadas en datos.

Complementando estas competencias, la IA se presenta como una aliada valiosa al utilizar simulaciones interactivas desde la cursada de la asignatura “Derecho del Consumidor”. Estas simulaciones, basadas en casos de conflicto del consumidor reales, permiten a los estudiantes actuar como operadores del derecho desde distintos roles, brindándoles una experiencia práctica esencial.

La IA no solo facilita la simulación de conflictos consumeriles del mundo real, sino que también contribuye a desarrollar habilidades prácticas fundamentales para enfrentar escenarios profesionales futuros. Esto implica no sólo un entendimiento profundo de los efectos jurídicos asociados con el uso de la IA y el neuromarketing, sino también la capacidad de anticipar y contrarrestar posibles prácticas abusivas.

## VII. BENEFICIOS DE LA INTEGRACIÓN DE LA IA A LA ENSEÑANZA DEL DERECHO DEL CONSUMIDOR

La integración de la IA en la enseñanza del derecho del consumidor representa un cambio paradigmático al ofrecer a los estudiantes oportunidades sin precedentes para participar en un

aprendizaje experiencial y multidimensional. Esta incorporación proporciona una plataforma sólida para una educación jurídica más efectiva, dinámica y adaptada a las necesidades específicas de cada estudiante, preparándolos de manera integral para enfrentar los desafíos complejos y cambiantes en el campo del derecho del consumidor.

Como botón de muestra, desarrollaremos algunas ventajas sobresalientes.:

### A. Aprendizaje activo y participativo

*El aprendizaje activo implica la participación directa de los estudiantes en su propio proceso educativo*<sup>36</sup>. En el ámbito de las ciencias jurídicas, este enfoque de enseñanza fomenta una comprensión más profunda y duradera de los conceptos del ordenamiento jurídico.

En la dinámica de aplicar este modelo, los estudiantes de derecho del consumidor ejecutan tareas de investigación de casos reales. Esto implica analizar documentación, recolectar pruebas digitales, identificar problemas jurídicos y proponer posibles soluciones. También deben identificar prácticas comerciales abusivas y publicidad engañosa. Además se enfrentan a tareas de análisis activo de contratos y términos de servicio de empresas, identificando cláusulas abusivas.

Se ha sostenido que la *Inteligencia Artificial permite a los estudiantes aprender mediante la experiencia, lo que facilita la retención de conocimientos*<sup>37</sup>. Resalto nuevamente acá el aporte de estas tecnologías en la generación de simulaciones interactivas basadas en casos reales, donde los estudiantes interactúan con escenarios virtuales y toman decisiones en tiempo real. Esto simula experiencias prácticas, permitiendo a los estudiantes aplicar sus conocimientos en contextos dinámicos y realistas.

Antes hacía referencia a que los estudiantes tienen la tarea académica de identificar prácticas comerciales abusivas y publicidad engañosa, entrenándose durante el cursado de esta asignatura. En este escenario, la IA puede analizar grandes conjuntos de datos para identificar patrones de prácticas comerciales abusivas.

El alumno de derecho del consumidor debe realizar análisis activos de los contratos y de los términos de un servicio, identificando cláusulas abusivas. En este sentido, las herramientas de procesamiento de lenguaje natural impulsadas por IA pueden ayudar a escanear y analizar contratos de manera eficiente. Los estudiantes, al utilizar estas herramientas, experimentan el análisis activo de contratos de una manera práctica y efectiva.

También observamos que la IA puede adaptar las

<https://palabrasdelderecho.com.ar/articulo/4553/Inteligencia-Artificial-El-Poder-Judicial-de-Rio-Negro-dicto-casi-6.000-fallos-con-sistemas-automatizados>

<sup>35</sup> En el documento titulado “VELOX: Inteligencia artificial aplicada a las vistas. Una nueva PoC para la gestión interna de la Fiscalía de Estado de PBA”, se especifica la labor. Dicho trabajo ha recibido la mención a la Mejor Exposición de Trabajo en SID - Simposio Argentino de Informática y Derecho 2022 expedida por Sociedad Argentina de Informática (SADIO).

<https://abogados.com.ar/argentina-inteligencia-artificial-y-su-impacto-en-el-poder-judicial/33792>

<sup>36</sup> <https://www.cambridgeinternational.org/Images/579618-active-learning-spanish-.pdf>

<sup>37</sup> Stapleton, L., & Stefaniak, J. (2019). Cognitive constructivism: Revisiting Jerome Bruner's influence on instructional design practices. *TechTrends*, 63, 4-5, citado en LOZADA, Roberto, “Los Riesgos de la Inteligencia Artificial en la Educación”, texto disponible en:

<https://ciencialatina.org/index.php/cienciala/article/view/8301/12500>

simulaciones y tareas según el progreso y las áreas de fortaleza o debilidad de cada estudiante. Esto personaliza la experiencia de aprendizaje, ofreciendo desafíos adecuados a cada individuo y mejorando la retención al abordar directamente sus necesidades específicas<sup>38</sup>.

Incluso el docente puede implementar algoritmos y aplicativos que proporcionen retroalimentación inmediata sobre las soluciones propuestas por los estudiantes. Esta retroalimentación instantánea mejora la comprensión y permite a los estudiantes ajustar y perfeccionar sus enfoques de resolución de problemas en tiempo real.

## B. Preparación profesional

La preparación profesional es esencial para los estudiantes que desean trabajar en el campo del derecho del consumidor. Estoy convencido que en este aspecto también la IA proporciona oportunidades para desarrollar habilidades prácticas y aplicar conceptos a casos del mundo real.

Las simulaciones de IA emergen como un vehículo educativo transformador. En este sentido, existe un potencial en las simulaciones de IA que permiten a los estudiantes asumir los distintos roles en un conflicto de derecho del consumidor: cliente, patrocinante, abogado de la empresa, operador de la justicia. De este modo, los estudiantes practican y desarrollan habilidades prácticas que son relevantes para su futuro desempeño jurídico.

Esta metodología no solo se trata de una simulación superficial, sino de una inmersión profunda en escenarios de auténticos conflictos entre consumidores y proveedores. Los estudiantes aplican teorías e institutos jurídicos propios del derecho de consumidor y experimentan las complejidades y dinámicas asociadas con diferentes roles en el proceso jurisdiccional.

La diversificación de roles, facilitada por la IA, no solo se traduce en una experiencia rica y variada, sino que también promueve el desarrollo de habilidades prácticas cruciales.

Este enfoque mira no solo el contenido del derecho del consumidor, sino que también cultiva habilidades transversales esenciales, como la toma de decisiones estratégicas, la resolución de problemas complejos, la comunicación efectiva y la colaboración interdisciplinaria. La adaptabilidad de las simulaciones de IA a escenarios cambiantes refleja la naturaleza dinámica de la práctica legal, preparando a los estudiantes para enfrentar situaciones del mundo real con confianza y competencia.

En última instancia, la integración de la IA en la simulación de roles en el ámbito del derecho del consumidor propulsa a los estudiantes más allá de la teoría académica, ofreciéndoles una experiencia auténtica que amalgama conocimientos jurídicos con habilidades prácticas. Al practicar y desarrollar estas

habilidades relevantes para su futuro laboral, los estudiantes no solo se convierten en profesionales jurídicos bien informados, sino también en agentes de cambio capaces de abordar los desafíos complejos del mundo jurídico contemporáneo.

## VIII. ÁREAS DE APLICACIÓN DE LA IA EN LA ENSEÑANZA DEL DERECHO DEL CONSUMIDOR

### A. Usuarios financieros

La educación sobre los derechos del consumidor en servicios financieros es crucial debido a la complejidad de los productos y servicios financieros y la importancia de proteger a los consumidores en estas transacciones. La IA puede ayudar a los estudiantes a comprender los aspectos legales de estas transacciones y cómo afectan a los consumidores.

Las fintech utilizan IA para evaluar la solvencia crediticia de los clientes y ofrecer préstamos personalizados. En el aula, los estudiantes pueden utilizar simulaciones de IA que imiten este proceso para comprender cómo se toman decisiones financieras y cómo esto puede afectar a los consumidores.

### B. Políticas públicas y comportamiento del consumidor

La IA desempeña un papel creciente en la formulación de políticas públicas y la intervención en el comportamiento del consumidor. Los gobiernos utilizan IA para analizar grandes conjuntos de datos y tomar decisiones basadas en evidencia en la formulación de políticas públicas. En el aula, los estudiantes pueden utilizar herramientas de IA para analizar datos sobre el comportamiento del consumidor y comprender cómo se pueden desarrollar políticas efectivas.

## IX. ALGUNAS HERRAMIENTAS DE IA QUE SE ADECUAN A ESTE PROPÓSITO

Un docente universitario que enseñe derecho del consumidor debe tener en cuenta la fenomenología de las relaciones entre consumidores y proveedores, así como los beneficios de la inteligencia artificial en este campo. La propuesta didáctica deberá estar marcada por una *epistemología experimental*<sup>39</sup> de las relaciones de consumo, para comprender las percepciones de los consumidores en sus interacciones con los proveedores, así como la influencia de factores culturales, sociales y psicológicos en sus decisiones de compra.

Se debe considerar a la IA como una tecnología idónea para analizar grandes volúmenes de datos de consumo, identificar patrones de comportamiento, predecir tendencias y personalizar

<sup>38</sup> “Explorando el papel de la IA en la mejora de los resultados de aprendizaje de los estudiantes”, disponible en: <https://ts2.space/es/la-ia-y-su-impacto-en-la-experiencia-de-aprendizaje-de-los-estudiantes/#gsc.tab=0>

<sup>39</sup> Cfr. VARGAS GUILLÉN, Germán, “Fenomenología e inteligencia artificial. Los límites de la subjetividad”, Estudios de Filosofía (Universidad de Antioquia), 1999, pág. 123.

la experiencia del consumidor. Además, la inteligencia artificial puede ser útil para simular escenarios de conflictos consumeriles, *modelando un ambiente de experiencias*<sup>40</sup> en donde el estudiante de derecho aprenda al interactuar con el consumidor y el proveedor.

#### A. Plataformas de simulación de compras

La utilización de plataformas de simulación de compras en la enseñanza del derecho del consumidor desempeña un papel fundamental al permitir a los estudiantes experimentar y observar con un ojo clínico jurídico la legitimidad del contexto de compra. Estas plataformas proporcionan un entorno de aprendizaje en el cual los estudiantes pueden aplicar los principios del derecho del consumidor para evaluar la validez de las transacciones de compra.

Un ejemplo reciente es el simulador de compra electrónica ideado por el español Jorge Carrion Romero<sup>41</sup>:



Este invento presenta características innovadoras que revolucionan la experiencia de compra en línea. Entendemos que esta innovación resulta útil en la enseñanza del derecho del consumidor, por su capacidad para proporcionar una experiencia de aprendizaje práctica y contextualizada.

La simulación ofrece a los estudiantes universitarios una experiencia práctica y contextualizada de cómo se desarrollan las transacciones comerciales en el entorno digital. Les permite explorar virtualmente un establecimiento comercial, navegar los productos y ver el entorno de la toma de decisiones del consumidor.

*Como la publicidad persigue en sí misma principalmente la captación de consumidores y usuarios, naturalmente se vale de técnicas de persuasión y manipulación del mensaje que en sí mismo comunica, el que se compone de modo mixto por una porción de elementos subjetivos que se mezclan estratégicamente con otros elementos objetivos del mensaje*

*publicitario que tienen una finalidad informativa sobre el producto o servicio que se publicita*<sup>42</sup>.

Esta metodología de aprendizaje a partir de un simulador, permite a los estudiantes analizar anuncios y descripciones de productos para identificar posibles casos de publicidad engañosa e ilícita. Con el auxilio pedagógico del docente entrenan la habilidad de revisar el cumplimiento de los estándares jurídicos y así determinar si la información proporcionada en el anuncio resulta veraz y transparente.

La propuesta en desarrollo ofrece a los estudiantes la oportunidad de explorar la dinámica, el ruido del contexto de compra y los sesgos cognitivos presentes.

Este escenario educativo les permite comprender los desafíos y las responsabilidades legales vinculadas a la protección del consumidor en un entorno digital.

Las simulaciones pueden incluir interacciones con vendedores o empresas que emplean prácticas comerciales potencialmente abusivas. Los estudiantes pueden aprender a reconocer situaciones en las que se violan los derechos del consumidor y a tomar acciones apropiadas (administrativas y judiciales).

Los estudiantes también pueden explorar los términos y condiciones asociados con compras en línea y evaluar su conformidad con las leyes de protección del consumidor. Esto les permite entender la importancia de la transparencia y proporcionar información clara a los consumidores.

Asimismo, las plataformas de simulación pueden incluir escenarios en los que los estudiantes tengan que lidiar con problemas de devolución de productos o hacer valer garantías. De esta manera, pueden aprender a identificar situaciones en las que los derechos del consumidor están siendo vulnerados y a abogar por soluciones adecuadas.

#### B. Chatbots que favorecen el aprendizaje

La optimización de las tecnologías en el entorno educativo ha evolucionado notablemente, extendiéndose más allá de la simple provisión de material o la implementación de plataformas virtuales para la enseñanza.

Un aspecto crucial de esta evolución se centra en la comunicación. Actualmente, además de las opciones convencionales como el correo electrónico, los foros y la mensajería instantánea, contamos con herramientas más interactivas y eficaces. Entre ellas, destacan los programas de robots conversacionales, conocidos como chatbots, que se integran fácilmente en espacios de interacción frecuentados por los estudiantes, como las redes sociales.

Hace unos años, en la Facultad de Ciencias Jurídicas de la Universidad de La Plata se realizó una prueba con la creación de un bot, que funcionaba como un asistente virtual para los estudiantes<sup>43</sup>. Se buscó proporcionar a los estudiantes una

<sup>40</sup> Ídem, pág. 98.

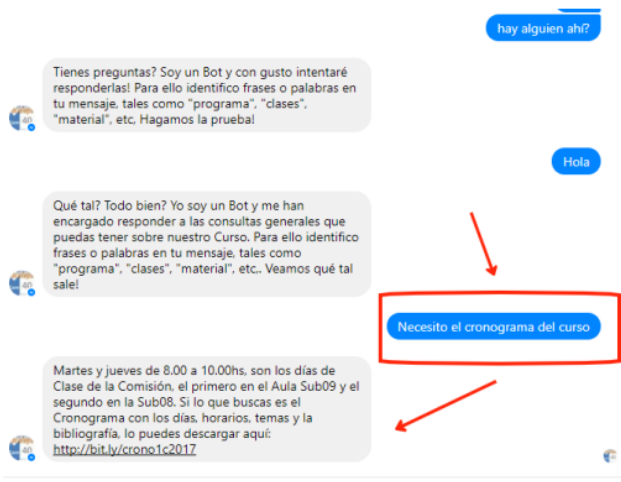
<sup>41</sup> <https://www.inventoseinventores.com/inventos/los-ultimos-inventos/27-grupo-a-necesidades-corrientes/1073-simulador-de-compra-electronica>

<sup>42</sup> FALIERO, Johanna C., “¿Qué efectos tiene la «publicidad» y qué se considera publicidad engañosa?”, MJ-DOC-17214-AR||MJD17214, 29-06-2023.

<sup>43</sup> BATISTA, Alejandro, “Uso de chatbots como apoyo para la comunicación en el Aula: un asistente virtual 24x7x365 colaborando con el curso”, Facultad



alternativa para consultas conceptuales sobre autores y contenidos de la asignatura.



44

Vemos que este tipo de experiencias reflejan que el uso de estos chatbots son una oportunidad significativa: en la sistematización de respuestas a consultas operativas recurrentes, evacuar dudas prácticas y generar una dinámica conversacional sobre conceptos o temas específicos de la asignatura.

Al aprovechar los chatbots de manera estratégica, podemos fomentar la participación activa de los estudiantes, facilitando discusiones significativas sobre los contenidos del curso. Además, esta herramienta puede adaptarse a diversos estilos de aprendizaje, brindando un soporte flexible que se ajusta a las necesidades individuales de los estudiantes.

Otro caso relevante fue la implementación de un asistente virtual en la Facultad de Ingeniería de la Universidad Simón Bolívar en Colombia. Se resolvió agilizar y mejorar el proceso de información, especialmente para atender las consultas de los estudiantes en períodos de ausencia de los docentes y administrativos<sup>45</sup>.

### C. Simulación de charla con el Asistente Virtual de la Cátedra de Derecho del Consumidor

En la búsqueda constante de innovación en la enseñanza del Derecho del Consumidor, la introducción de tecnologías como los chatbots ha ampliado significativamente las oportunidades de aprendizaje interactivo. Estos asistentes virtuales programados para abordar consultas y proporcionar información específica se han convertido en aliados valiosos para los estudiantes, ofreciendo respuestas instantáneas y adaptándose a sus necesidades individuales.

A continuación expondré una simulación de charla con el asistente de la cátedra de Derecho del Consumidor. Esta experiencia propone destacar cómo la interacción con un chatbot especializado puede transformarse en un diálogo

fructífero y enriquecedor para el estudiante de Derecho del Consumidor. El diálogo intenta revelar la aplicación de esta IA conversacional como herramienta pedagógica para profundizar en temas específicos de la asignatura.

Chatbot: 🤖

Estudiante: 😊

🤖 Hola Pablo, ¿cómo estás? Soy tu asistente virtual en la cursada de Derecho del Consumidor. Contame una temática que te esté interesando profundizar, para poder conversar juntos.

😊 Hola, todo bien. Quiero aprender más sobre la compra a distancia a través de medios electrónicos.

🤖 Muy bien. Vamos con este caso:

Juan, un consumidor, decide comprar un televisor en línea a través de un sitio web de comercio electrónico muy conocido. Después de navegar por el sitio, selecciona un televisor de alta definición y realiza la compra utilizando su tarjeta de crédito. En el momento de la compra, el sitio web indica que la entrega se realizará en un plazo de 5 a 7 días hábiles.

Pasados los 7 días hábiles, Juan aún no ha recibido el televisor. Se comunica con el servicio de atención al cliente del sitio web y le informan que hay un problema con el stock y que la entrega se retrasará por otras dos semanas. Juan, sintiéndose frustrado, decide cancelar la compra y solicitar un reembolso.

Al intentar cancelar, se encuentra con dificultades para comunicarse con el servicio al cliente y le piden que espere un tiempo adicional. Finalmente, después de varias semanas, Juan recibe un televisor diferente al que originalmente compró y que no cumple con las especificaciones anunciadas.

Pablo, ¿qué elementos de incumplimiento identificas en el accionar del proveedor?

😊 En el caso de Juan, identifico varios elementos de incumplimiento por parte del proveedor. En primer lugar, el retraso en la entrega del televisor más allá del plazo inicialmente establecido es un incumplimiento de la obligación de entregar el producto en el tiempo acordado. Además, la falta de comunicación oportuna sobre el problema de stock también representa una violación de la transparencia que se espera en las transacciones comerciales.

🤖 Bien. Ahora, centrémonos en el derecho de arrepentimiento ¿Consideras que Juan tenía el derecho de cancelar la compra y solicitar un reembolso?

😊 Sí, considero que Juan tenía el derecho de cancelar la compra y solicitar un reembolso. Según lo que hemos aprendido, en compras a distancia a través de medios electrónicos, los consumidores suelen tener el derecho de arrepentimiento. En este caso, el proveedor no cumplió con el plazo de entrega inicialmente establecido, y luego hubo un problema con el producto recibido, lo que justificaría la solicitud de cancelación y reembolso por parte de Juan.

🤖 Correcto, Pablo. El derecho de arrepentimiento es

fundamental en las compras en línea para proteger a los consumidores en situaciones como estas. Ahora, hablemos sobre las dificultades que Juan enfrentó al intentar cancelar la compra. ¿Qué institutos jurídicos relacionados con la cancelación deberíamos considerar en este caso?

🗣️ *En este caso vale considerar la obligación del proveedor de facilitar y garantizar un proceso de cancelación sencillo y accesible para el consumidor (Art. 34 de la LDC).*

👤 Excelente punto, Pablo. No te olvides de otros institutos que sirven de auxilio en este tipo de casos, como el botón de compra y el proceso de revocación. Ahora, hablemos sobre la entrega de un producto diferente al originalmente comprado. ¿Cómo podríamos abordar jurídicamente esta situación?

🗣️ *En este caso, podríamos considerar la normativa que regula la conformidad de los productos, asegurándonos de que el consumidor reciba lo que efectivamente compró: principio de integridad del Art. 10 bis de la LDC. Si el televisor recibido no cumple con las especificaciones anunciadas, podría considerarse un incumplimiento por parte del proveedor, y el consumidor tendría derechos para exigir una solución, como la devolución del producto o un reemplazo adecuado.*

👤 Muy buena observación, Pablo. Identificaste varios aspectos clave en la protección del consumidor en compras a distancia. Te felicito por este avance ¿Tenes alguna otra pregunta o aspecto que te gustaría profundizar en este tema?

Luego continúa la interacción generativa de aprendizajes, bajo este modelo conversacional:

🗣️ Respuesta → 🗣️ → 🗣️ → 🗣️ → 🗣️

Después de esta conversación inicial, la interacción continúa de manera generativa, brindando al estudiante la oportunidad de profundizar aún más en aspectos específicos del derecho del consumidor. El chatbot, diseñado para adaptarse a las necesidades individuales de cada estudiante, sigue proporcionando información relevante, sugiriendo lecturas adicionales, y planteando preguntas que despiertan el interés y la reflexión.

Otra arista de aplicación práctica sería usar esos chatbots para guiar a los estudiantes a través del proceso de resolución de un conflicto de un cliente ficticio. Ello con el objetivo de entrenar las habilidades del alumno para canalizar adecuadamente aquel problema a través de las vías administrativas y judiciales disponibles.

Esta práctica les otorga un rol activo en las tareas de identificar información clave sobre “su cliente”, los derechos en juego, los institutos jurídicos, los plazos, los procedimientos y las estrategias que pueden emplearse.

Vemos como una ventaja la oportunidad de aplicar este tipo de IA, puesto que brinda a los estudiantes una experiencia práctica que les permite aplicar los conocimientos teóricos adquiridos en el aula a situaciones del mundo real. Esto no solo fomenta una comprensión más profunda de los conceptos legales del derecho del consumidor, sino que también les da la confianza y las habilidades necesarias para abordar futuros casos de conflicto del consumidor de manera efectiva.

La implementación de un chatbot especializado en derecho del consumidor se presenta como una herramienta educativa

invaluable, capitalizando los beneficios inherentes de una dinámica conversacional. Esta innovadora solución no sólo promovería la fluidez y la instantaneidad en la interacción, sino que también permitiría abordar temas específicos a partir del interés actual del estudiante.

En este sentido, entiendo que la naturaleza conversacional del chatbot crearía un espacio educativo dinámico, donde los estudiantes podrían plantear preguntas y recibir respuestas de manera inmediata. Este enfoque facilita un acercamiento casuístico y gradual a los conceptos fundamentales del derecho del consumidor. Al propiciar conversaciones contextualizadas, se fomenta un aprendizaje más significativo al conectar los principios legales con situaciones prácticas.

Un aspecto a destacar es que la fluidez en la interacción es clave para mantener la participación activa de los estudiantes. Cuando el alumno interactúa, experimenta la instantaneidad de las respuestas del chatbot, lo que contribuye con un aprendizaje más ágil y adaptado a las necesidades individuales de cada estudiante. Además, al abordar temas basados en el interés actual del estudiante, se promueve una mayor relevancia y aplicación práctica de los conceptos apprehendidos.

El chatbot no solo sirve como una fuente de información, sino también como un guía que puede dirigir a los estudiantes hacia áreas específicas del derecho del consumidor que despierten su interés. Esta capacidad de personalización contribuiría a un aprendizaje más autónomo y motivador.

Este modelo de aprendizaje tiene como matriz un enfoque casuístico, que permite a los estudiantes enfrentarse a situaciones del mundo real, analizar casos específicos y aplicar los principios jurídicos a contextos concretos. Este entrenamiento fomentaría una comprensión más profunda y práctica de los conceptos del derecho del consumidor.

En síntesis, se propone la implementación de un chatbot en el ámbito educativo del derecho del consumidor como una estrategia pedagógica innovadora y efectiva. Es un instrumento que potencia la calidad de la interacción educativa. Al programar estos asistentes virtuales de manera reflexiva, podemos transformarlos en aliados efectivos para impulsar la participación y el entendimiento profundo de los temas académicos.

#### D. Plataformas de participación en políticas públicas y comportamiento del consumidor

En el marco de la enseñanza integrada por aportes de la IA, los estudiantes pueden explorar cómo las decisiones políticas afectan el comportamiento del consumidor. En este sentido, resultan útiles las plataformas que permiten a los estudiantes participar en simulaciones de toma de decisiones de políticas públicas relacionadas con el derecho del consumidor.

Utilizando algoritmos de aprendizaje automático, estos aplicativos pueden analizar datos históricos para prever tendencias y comportamientos futuros de los consumidores. Esto es esencial para evaluar la eficacia de las políticas públicas al anticipar posibles desafíos y áreas de enfoque.

Con las herramientas de IA se pueden analizar grandes

cantidades de datos de medios sociales para evaluar la percepción pública sobre políticas específicas y su impacto en el comportamiento del consumidor. Esto proporciona una perspectiva en tiempo real sobre cómo las políticas son percibidas y adoptadas por los consumidores.

Por ejemplo, la empresa SALESFORCE lanzó recientemente “Tableau Analytics”, una IA que mejora la toma de decisiones, obteniendo información automatizada y arrojando flujos inteligentes con esos datos<sup>46</sup>.

Este componente de la IA facilita el análisis de grandes conjuntos de datos para identificar patrones y correlaciones. Esto es crucial para evaluar la efectividad de las políticas públicas al observar cambios significativos en el comportamiento del consumidor a lo largo del tiempo.

Gobiernos locales en todo el mundo buscan incorporar las nuevas soluciones tecnológicas para abordar sus desafíos públicos. *La implementación responsable de la IA, combinada con una visión centrada en las personas, ya transforma las ciudades en lugares más eficientes y habitables*<sup>47</sup>.

Existen numerosos casos de cómo las ciudades pueden implementar políticas públicas innovadoras a partir del uso de IA<sup>48</sup>. Por ejemplo, un proyecto local propone el reconocimiento automático de patrones urbanos, generando simulaciones sociales masivas a fin de evaluar el diseño de políticas públicas viables<sup>49</sup>.

Otra innovación sobresaliente la aporta un trabajo colaborativo entre la Universidad de San Luis y el Ministerio de Hacienda y Finanzas de la Provincia de Buenos Aires. El proyecto desarrolla un aplicativo para la obtención automática de datos para el índice de precios al consumidor PBA. Se impulsa el desarrollo de una app que mediante web-scraping e Inteligencia Artificial permite obtener automáticamente información de precios de bienes y servicios ofrecidos vía web para incorporar el comercio digital al cálculo del Índice de Precios al consumidor (IPC) en la Provincia de Buenos Aires<sup>50</sup>.

Estas experiencias permiten alentar a los estudiantes en las tareas de investigación, diseño y proposición de futuras políticas públicas, a partir del uso de la IA para exponer prácticas comerciales abusivas.

De la colaboración entre unidades académicas y organismos públicos pueden emerger proyectos innovadores, como plataformas que utilicen algoritmos de aprendizaje automático para analizar datos recopilados a través de la participación ciudadana.

La colaboración entre unidades académicas y organismos públicos abre la puerta a proyectos innovadores. La fusión de conocimientos académicos con la experiencia práctica del sector público puede dar lugar a soluciones más efectivas y pragmáticas. Esta colaboración puede generar insights valiosos sobre prácticas comerciales abusivas, permitiendo a las autoridades tomar decisiones informadas y rápidas.

También resulta viable la colaboración con otros cibersitios de comercio electrónico, para acceder a datos sobre el comportamiento de compra del consumidor, el uso de promociones y la presencia de dark patterns en sus interfaces. Esta información en tiempo real es esencial para comprender las tácticas utilizadas por las empresas y adaptar las políticas en consecuencia.

Se proyecta la creación de este tipo de plataformas no solo para reproducir informes automáticos, sino para que los estudiantes generen experimentos a partir de las prácticas comerciales abusivas detectadas. Estos informes pueden servir como una herramienta valiosa para las autoridades locales y los organismos de protección del consumidor. Incluso los estudiantes pueden gestionar en esa plataforma dinámicas de retroalimentación automática, recopilando los comentarios de los consumidores sobre la implementación de aquellas políticas.

La oportunidad de desarrollar proyectos que tengan un impacto real en la sociedad brinda a los estudiantes una experiencia valiosa y motivadora. Ver cómo sus esfuerzos contribuyen a cambios positivos refuerza su compromiso y confianza en su capacidad para influir en asuntos públicos. Los estudiantes no solo aprenden sobre la ley, sino que también se convierten en agentes activos del cambio social.

## X. CONCLUSIÓN

La integración de la inteligencia artificial en la enseñanza del derecho del consumidor emerge como una respuesta a los desafíos contemporáneos y una plataforma para el avance educativo. Desde la articulación de los objetivos iniciales hasta la exploración de las áreas de aplicación específicas, he delineado un panorama donde la tecnología no sólo enfrenta los retos actuales, sino que también redefine la experiencia educativa.

La inteligencia artificial, enriqueciendo el diálogo socrático

<sup>46</sup> Disponible en:

<https://www.salesforce.com/es/products/analytics/overview/>

<sup>47</sup> “Las ciudades inteligentes y sostenibles combinan diversas tecnologías para reducir el impacto ambiental y ofrecer a la población una mejor calidad de vida. Esto no sólo es un desafío técnico; el cambio organizacional de los gobiernos es esencial. Es un desafío multidisciplinario que se debe realizar en conjunto con los funcionarios locales, los proveedores, las autoridades nacionales, la academia y la sociedad civil”, define la Comisión Europea:

[https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives\\_es](https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives_es)

<sup>48</sup> Amsterdam está midiendo y mejorando la accesibilidad en la ciudad gracias al Big Data y a la inteligencia artificial. En 2022, comenzó una prueba que permite a cualquier usuario en línea explorar las calles e informar sobre lugares que no son inclusivos para personas con discapacidades físicas o movilidad

reducida. La ciudad neerlandesa integró el servicio en una plataforma especial, desarrollada por investigadores de la Universidad de Maryland y que utiliza imágenes interactivas de Google Street. Con los datos obtenidos gracias a la participación ciudadana, se entrenan algoritmos de aprendizaje automático para encontrar rápidamente los problemas de accesibilidad. Así, la información se podrá visualizar en mapas y servirá a las autoridades para tomar decisiones. Ver más en: <https://www.mascomunidad.org.ar/inteligencia-artificial-y-ciudades-10-casos-de-aplicacion-en-las-gestiones-urbanas-parte-1/>

<sup>49</sup> Este proyecto y otros seleccionados por la Fundación Sadosky en 2022:

<https://solucionesinnovadoras.fundacionsadosky.org.ar/proyectos-seleccionados-en-2022/>

<sup>50</sup> Este proyecto y otros seleccionados por la Fundación Sadosky en 2023:

<https://solucionesinnovadoras.fundacionsadosky.org.ar/proyectos-seleccionados-en-2023/>



en el aula y abordando los desafíos jurídicos de la era digital, ha demostrado ser un aliado valioso tanto para estudiantes como para profesores. La perspectiva del estudiante del derecho del consumidor y los nuevos desafíos para los educadores se ven transformados por este enfoque innovador.

Los beneficios se manifiestan en un aprendizaje activo y participativo, preparando a los estudiantes para un escenario profesional en constante evolución. Desde la aplicación en áreas específicas, como usuarios financieros y políticas públicas, hasta el uso de herramientas como plataformas de simulación y chatbots, la inteligencia artificial se integra de manera orgánica en la enseñanza, abriendo horizontes educativos sin precedentes.

En conclusión, la incorporación de la inteligencia artificial va más allá de abordar desafíos; es un catalizador que transforma la educación jurídica, brindando herramientas para la comprensión, defensa y protección efectiva de los derechos del consumidor en un mundo en constante cambio. Este enfoque dinámico redefine la naturaleza misma de la enseñanza del derecho del consumidor, preparando a las generaciones futuras para enfrentar los desafíos con agilidad y profundidad.

# Inteligência Artificial e Propostas Regulatórias Brasileiras: uma análise acerca da explicabilidade

Colombo, Cristiano, Professor do Mestrado em Direito da Empresa e dos Negócios da UNISINOS e da Faculdade Verbo Jurídico. Dal Paz, Lucas, Mestrando em Direito da Empresa e dos Negócios da UNISINOS. Stroppa, Tatiana, Professora do Centro Universitário de Bauru.

**Resumo:** O presente artigo descreve as iniciativas de regulação legislativa da Inteligência Artificial, no Brasil e, a partir de uma visão histórica dos projetos de lei, destaca a importância da exigência de explicabilidade nas decisões algorítmicas. A pesquisa é teórica, analisa projetos de textos legislativos, avançando na temática de forma exploratória e descritiva, aplicando procedimentos técnicos bibliográficos.

**Palavras-chave:** *Assimetria informacional; Explicabilidade; Inteligência Artificial; Projetos de Lei.*

**Abstract:** This article describes the legislative regulation initiatives for Artificial Intelligence in Brazil and, based on a historical view of bills, highlights the importance of the requirement for explainability in algorithmic decisions. The research is theoretical, analyzes draft legislative texts, advancing the theme in an exploratory and descriptive way, applying technical bibliographic procedures.

**Keywords:** *Information asymmetry; Explainability; Artificial intelligence; Bills.*

## I. INTRODUÇÃO

O estudo se dedica a observar as iniciativas de regulação legislativa da Inteligência Artificial, no Brasil, a partir de uma visão histórica dos projetos de lei, destacando a importância da explicabilidade na regulação da IA e alguns de seus contornos.

Na Seção II, apresentar-se-ão, sem esgotar os temas: A) Aspectos da Inteligência Artificial; B) Propostas legislativas

brasileiras ; C) PL 2338/2023 e as assimetrias e desigualdades ; D) A presença da explicabilidade, como elemento de *lege ferenda*; tudo, para, ao final, refletir sobre sua importância no *framework* regulatório. A pesquisa é teórica, analisa projetos legislativos, avançando na temática de forma exploratória e descritiva, aplicando procedimentos técnicos bibliográficos.

## II. DA INTELIGÊNCIA ARTIFICIAL E PROPOSTAS REGULATÓRIAS BRASILEIRAS ACERCA DA EXPLICABILIDADE

### A. Inteligência Artificial

A Inteligência Artificial (IA) se apresenta com exuberância no campo das novas tecnologias por duas características que lhe são próprias: o “autoaprendizado” e o “agir com certo nível de autonomia”.<sup>1</sup> Quanto ao primeiro aspecto, sua capacidade *self-learning* se destaca pela possibilidade de “identificar padrões”, inferir “novas informações” e “predizer eventos futuros”.<sup>2</sup> Vale-se, sobretudo, de *data mining*, dedicando-se a “descobrir o conhecimento”, com classificação e clusterização, bem como *machine learning*, que se trata da “melhora com a experiência”.<sup>3</sup>

Quanto a “agir com certo nível de autonomia”, decorre das tomadas de decisão pela IA que não são “pré-programadas”, todavia, dependem da “situação particular”.<sup>4</sup> A IA tem como escopo a predição “para o reconhecimento de probabilidades no escrutínio da solução mais eficiente para determinado problema hierarquizado”.<sup>5</sup> Posto isso, é necessário reconhecer que, mesmo que infinitas e imprevisíveis sejam as possibilidades de sua aplicabilidade, a IA, atualmente, goza de certa limitação.

Nos dias de hoje, não se verificam exemplos em operação de IA forte, com a “criação de sistemas capazes de tomar decisões inteligentes em diferentes áreas”.<sup>6</sup> Por outro lado, a

<sup>1</sup> CUSTERS, Bart; FOSCH-VILLARONGA, Eduard. Humanizing Machines: Introduction and Overview. In: CUSTERS, Bart; FOSCH-VILLARONGA, Eduard (Orgs.) **Law and Artificial Intelligence**. Regulating AI and Applying AI in Legal Practice. Haia: T.M.C. Asser Press, 2022, 3-28, p. 8.

<sup>2</sup> CUSTERS, Bart; FOSCH-VILLARONGA, Eduard. Humanizing Machines: Introduction and Overview. In: CUSTERS, Bart; FOSCH-VILLARONGA, Eduard (Orgs.) **Law and Artificial Intelligence**. Regulating AI and Applying AI in Legal Practice. Haia: T.M.C. Asser Press, 2022, 3-28, p. 8.

<sup>3</sup> CUSTERS, Bart; FOSCH-VILLARONGA, Eduard. Humanizing Machines: Introduction and Overview. In: CUSTERS, Bart; FOSCH-VILLARONGA, Eduard (Orgs.) **Law and Artificial Intelligence**. Regulating AI and Applying AI in Legal Practice. Haia: T.M.C. Asser Press, 2022, 3-28, p. 8.

<sup>4</sup> CUSTERS, Bart; FOSCH-VILLARONGA, Eduard. Humanizing Machines: Introduction and Overview. In: CUSTERS, Bart; FOSCH-VILLARONGA, Eduard (Orgs.) **Law and Artificial Intelligence**. Regulating AI and Applying AI in Legal Practice. Haia: T.M.C. Asser Press, 2022, 3-28, p. 8.

<sup>5</sup> PINTO, Henrique Alves; ERNESTO, Leandro Miranda. Inteligência Artificial aplicada ao Direito: por uma questão de ética. In: COLOMBO, Cristiano; Engelmann, Wilson; FALEIROS JÚNIOR, José Luiz de Moura (Orgs.) **Tutela Jurídica do Corpo Eletrônico**. Novos Desafios ao Direito Digital. Indaiatuba: Foco, 2022. v. 1, p. 673-689, p. 673.

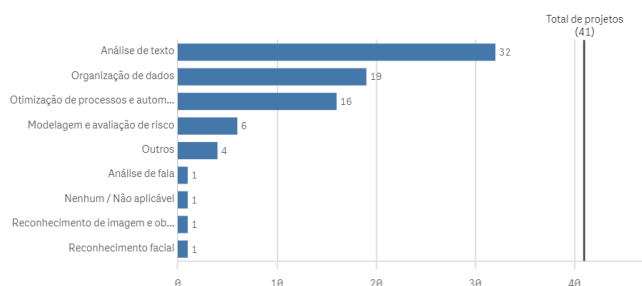
<sup>6</sup> FERRARI, Isabela. Discriminação algorítmica e poder judiciário: limites à adoção de sistemas de decisões algorítmica no poder judiciário brasileiro. 1ª Ed. Florianópolis. Emais, 2023.

“IA Fraca”<sup>7</sup>, está nas tarefas do cotidiano, e, por mais que não possua empatia, tampouco internalize sentimentos genuinamente, como seres humanos, possui “efeitos significativos nos modos de ser e viver das coletividades humanas e impactos relevantes em sua atividade econômica.”<sup>8</sup>.

Nesse contexto, ainda que sejam inteligências diversas, “o intuito da criação da IA é fazer com que ela tenha a capacidade de pensar como uma pessoa e possa aprender por meio das experiências. Assim como o cérebro tem a memória, a IA tem os dados, interligados pela rede neural artificial.”<sup>9</sup> De forma exemplificativa, a IA pode ser personificada nos “algoritmos de análise de dados que fazem cruzamentos (analytics) e os sistemas que conseguem aprender sozinhos por aprendizado de máquinas (machine learning)”<sup>10</sup>.

O avanço da IA também é favorecido pelo momento em que se difunde, isto é, aquilo que Schwab<sup>11</sup> define como 4ª Revolução Industrial, caracterizando-se “pela universalização da Internet e pela aparição em larga escala da inteligência Artificial (IA)”<sup>12</sup>. A título de exemplo, a importância da IA se revela na otimização da prestação jurisdicional, fazendo com que o Conselho Nacional de Justiça (CNJ), desde 2019, lançasse uma plataforma para acompanhamento dos projetos de IA desenvolvidos por tribunais brasileiros. Os “Projetos com Inteligência Artificial no Poder Judiciário”<sup>13</sup> abordam de forma visual e intuitiva as principais características desses projetos em andamento, sendo 41 projetos em 32 tribunais brasileiros. Destaca-se que os projetos variam da IA por análise de texto para também aquela que possui reconhecimento facial. Para melhor demonstrar, colaciona-se o gráfico extraído da plataforma apontada<sup>14</sup>:

Quais dos seguintes recursos se aplicam à ferramenta?



Do mesmo modo, a preocupação em regular tal tecnologia está diretamente ligada à preservação dos direitos em que poderá interferir a partir do seu uso desenfreado, sendo necessário um “instrumento de preservação de direitos fundamentais, diante da amplificação dos produtos e serviços que se utilizam em maior ou menor grau de inteligência artificial”<sup>15</sup>.

Nesse caminho, iniciam as discussões a respeito dos parâmetros legais e éticos que deverão ser fixados para estabelecer os limites de uma tecnologia que possui tamanho poder construtivo, mediante “a necessidade social que faz urgir a regulamentação do uso de tecnologia, e notadamente para os fins deste estudo, da inteligência artificial, leva a norma jurídica ao futuro”<sup>16</sup>, mas também pelos riscos que acompanham a difusão de tecnologia em uma era digital que é “marcada pela pelos riscos a desinformação em massa (*fake news* e *deep fake*)”<sup>17</sup>. De tal forma, a construção do debate acerca de (auto) regulação da inteligência artificial no Brasil é medida necessária.

## B. Aspectos históricos das propostas legislativas Brasileiras

A Lei Geral de Proteção de Dados (LGPD), sob o nº 13.709, desde o ano de 2018, dispõe acerca da Inteligência Artificial, em seu artigo 20, eis que estabelece comando específico às decisões unicamente automatizadas, que, frequentemente, se valem de algoritmos dinâmicos. Interessante registrar que a redação originária estabelecia, inclusive, o direito à revisão das decisões unicamente automatizadas por “pessoa natural”, ou seja, que caberia a um ser humano proceder à reanálise do *output*, seja determinando a sua correção ou, mesmo, a manutenção da decisão exclusivamente sintética. Temática intrinsecamente ligada às reflexões apresentadas, que toca diretamente à explicabilidade da decisão, inclusive, para que possa ser adequadamente revisada.

No entanto, a expressão “pessoa natural” acabou por ser extraída do texto, pelo advento da Medida Provisória sob o nº 869 de 2018, com a posterior conversão na Lei 13.853 de 2019, o que, em tese, permite, atualmente, no Brasil, que a revisão se opere por outro software, com ou sem IA mitigando, no particular, o princípio da supervisão humana. Outrossim, é verdade, que a legislação não afasta a apreciação pelo Poder

<sup>7</sup> FERRARI, Isabela. Discriminação algorítmica e poder judiciário: limites à adoção de sistemas de decisões algorítmica no poder judiciário brasileiro. 1ª Ed. Florianópolis. Emais, 2023.

<sup>8</sup> FERRARI, Isabela. Discriminação algorítmica e poder judiciário: limites à adoção de sistemas de decisões algorítmica no poder judiciário brasileiro. 1ª Ed. Florianópolis. Emais, 2023.

<sup>9</sup> VASCONCELOS FILHOS, Oton de Albuquerque. SILVA, Gabriel Carvalho Nunes. Direito e Inteligência Artificial: A eficácia das decisões judiciais no contexto do PL 5.051/2019. Revista de Processo. Vol. 321/2021. P.367/391. Nov. 2021.

<sup>10</sup> COSTA, Aryela Couto. BITTENCOURT, Luís Antônio de Aguiar. Inteligência Artificial: uma visão prospectiva sobre seus principais efeitos jurídicos. Revista das Faculdades Integradas Vianna Júnior. V.12. n.2. Juiz de Fora. Jul-dez 2021.

<sup>11</sup> SCHWAB, Klaus.

<sup>12</sup> PINTO, Henrique Alves. GUEDES, Jefferson Carús. CÉSAR, Joaquim Portes de Cerqueira. (coordenadores). Inteligência Artificial aplicada ao processo de tomada de decisões. 1 ed. São Paulo: D'Plácido, 2022.

<sup>13</sup> Conselho Nacional de Justiça. Disponível em: <https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,cursel>. Acesso em: 11 de outubro de 2023.

<sup>14</sup> Idem.

<sup>15</sup> BARBOSA, Mafalda Miranda. BRAGA NETTO, Felipe. FALEIROS JÚNIOR, José Luiz de Moura. (coordenadores). Direito Digital e inteligência Artificial: diálogos entre brasil e europa. São Paulo: Editora Foco, 2021.

<sup>16</sup> BLUM, Renato Opice. LÓPEZ, Nuria. Os desafios da regulamentação de inteligência artificial. Revista de Direitos e Novas Tecnologias. Vol. 9/2020. Out-dez/2020.

<sup>17</sup> PINTO, Henrique Alves. GUEDES, Jefferson Carús. CÉSAR, Joaquim Portes de Cerqueira. (coordenadores). Inteligência Artificial aplicada ao processo de tomada de decisões. 1 ed. São Paulo: D'Plácido, 2022.

Judiciário de decisões automatizadas, que, em última *ratio*, estarão sob os olhos de um ser humano: o julgador. Ainda que se pense em IA aplicada ao Poder Judiciário, sua vocação não substitui o ser humano, no ato de julgar.<sup>18</sup>

Em se tratando de regulação específica sobre Inteligência Artificial, o Projeto de Lei 5051/2019 promoveu reflexões pioneiras sobre a questão no Brasil, inclinando-se para a linha principiológica, como anuncia em seu artigo 1º. Trata-se de projeto com sete dispositivos, vocacionado a indicar os “princípios de Inteligência Artificial”, tendo apontado os seguintes “fundamentos”, a saber: “o reconhecimento de que se trata de tecnologia desenvolvida para servir as pessoas com a finalidade de melhorar o bem-estar humano em geral”; “respeito aos direitos humanos, à pluralidade e à diversidade”; “a garantia da proteção da privacidade e dos dados pessoais”; “a transparência, a confiabilidade e a possibilidade de auditoria dos sistemas”; “a supervisão humana”.<sup>19</sup>

Em seu artigo 3º, apresenta o balanço necessário entre a “promoção e a harmonização da valorização do trabalho humano e do desenvolvimento econômico”.<sup>20</sup> No artigo 4º, eleva o princípio da supervisão humana, inclusive, imputando responsabilidade civil ao supervisor. Nos artigos 5º e 6º desenvolve uma visão programática das ações e demandas da IA, inclusive, na aplicação pelo Estado Brasileiro, estabelecendo uma *vacatio legis* de 45 (quarenta e cinco) dias.

A partir de uma análise crítica, depreende-se que o projeto chama a atenção positivamente sobre a necessidade da regulação via princípios, que estão menos suscetíveis à obsolescência, diante da evolução tecnológica. A exemplo, o advento da IA Generativa, que resultou em novas questões jurídicas e caminhos inéditos a serem desenhados, em pouco tempo. E, ainda, especialmente, em sua justificação, coloca como ponto central o princípio da supervisão humana, ocupando a IA o posto auxiliar na tomada de decisão humana. Por outro lado, não define, nem limita o que seja a IA, embora seja verdade que a doutrina enfrenta dificuldade em assim defini-la tecnicamente, também não dispõe de forma mais detalhada acerca do instituto da responsabilidade civil e seus diversos aspectos. É um projeto que se pauta pela concisão, de característica principiológica e trilha o caminho do geral, sem recortes específicos.

No ano seguinte, dois novos projetos foram elaborados para fomentar a discussão pertinente, sendo o Projeto de Lei 21/2020 e o 240/2020. O PL 21/2020, principalmente, destacou-se por expressar os “princípios, direitos, deveres e instrumentos de governança de IA.”, avançando em dimensão e pontos, em comparação à proposta do PL 5051, de 2019, que se limitou aos “fundamentos”. Apresenta quinze dispositivos. Em seu artigo 1º, “determina as diretrizes para a atuação da União, dos

Estados, do Distrito Federal e dos Municípios, pessoas físicas e jurídicas, de direito público ou privado, e entes sem personalidade jurídica em relação à matéria.”<sup>21</sup> Ou seja, o projeto dispõe que a regulação deve ser observada por pessoas de direito público e privado, inclusive, entes não personificados, havendo ampla sujeição passiva. Em seu artigo 2º, apresenta glossário, apontando-se como destaque o conceito de “sistema de inteligência artificial”, definido como “sistema baseado em processo computacional que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões e recomendações ou tomar decisões que influenciam ambientes reais ou virtuais;”.<sup>22</sup> No artigo 3º, traz critério hermenêutico, a encaminhar a matéria, dispondo que “na interpretação da lei”, deve-se considerar “a relevância da inteligência artificial para a inovação, o aumento da competitividade, o crescimento econômico sustentável e inclusivo e a promoção do desenvolvimento humano e social”. Em seus artigos 4º e 5º, estão presentes os fundamentos e os objetivos, para, mais adiante, no artigo 6º, estabelecer o conjunto de princípios, entre eles: a finalidade, no sentido de “buscar resultados benéficos para as pessoas e o planeta, com o fim de aumentar as capacidades humanas, reduzir as desigualdades sociais e promover o desenvolvimento sustentável”; a “centralidade no ser humano: respeito à dignidade humana, à privacidade e à proteção de dados pessoais e aos direitos trabalhistas”; “não discriminação: impossibilidade de uso dos sistemas para fins discriminatórios, ilícitos ou abusivos”; “transparência e explicabilidade”; “segurança: utilização de medidas técnicas e administrativas, compatíveis com os padrões internacionais, aptas a permitir a funcionalidade e o gerenciamento de riscos dos sistemas de inteligência artificial e a garantir a rastreabilidade dos processos e decisões tomadas durante o ciclo de vida do sistema;” “responsabilização e prestação de contas: demonstração, pelos agentes de inteligência artificial, do cumprimento das normas de inteligência artificial e da adoção de medidas eficazes para o bom funcionamento dos sistemas, observadas suas funções”.<sup>23</sup>

Na sequência, os artigos 7º e 8º descrevem os “direitos das partes interessadas no sistema de inteligência artificial, utilizado na esfera privada ou pública”, como, por exemplo, “acesso a informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo sistema de inteligência artificial que lhes afetem adversamente, observados os segredos comercial e industrial” e defesa do interesse da parte interessada, tanto individualmente, como coletivamente.

O artigo 9º estabelece “deveres dos agentes de inteligência artificial”, a refletir na própria questão da responsabilidade civil, tais como: “IV - implantar um sistema de inteligência artificial somente após avaliação adequada de seus objetivos, benefícios e riscos relacionados a cada fase do sistema e, caso

<sup>18</sup> MACHADO, Fernanda de Vargas; COLOMBO, Cristiano. Inteligência artificial aplicada à atividade jurisdicional: desafios e perspectivas para sua implementação no Judiciário. Revista da Escola Judicial do TRT4, [S. l.], v. 3, n. 5, p. 117–141, 2021. Disponível: <https://rejtrt4.emnuvens.com.br/revistaejud4/article/view/113>. Acesso: 25 de fevereiro de 2024.

<sup>19</sup> BRASIL, Projeto de Lei 5051/2019. Brasília, DF. Acesso em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1708613194891&disposition=inline>. Acesso em: 25 de fevereiro de 2024.

<sup>20</sup> BRASIL, Projeto de Lei 5051/2019. Brasília, DF. Acesso em: [https://legis.senado.leg.br/sdleg-](https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1708613194891&disposition=inline)

[getter/documento?dm=8009064&ts=1708613194891&disposition=inline](https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1708613194891&disposition=inline). Acesso em: 25 de fevereiro de 2024.

<sup>21</sup> BRASIL, Projeto de Lei 21/2020. Brasília, DF. Acesso em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Acesso em: 25 de fevereiro de 2024.

<sup>22</sup> BRASIL, Projeto de Lei 21/2020. Brasília, DF. Acesso em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Acesso em: 25 de fevereiro de 2024.

<sup>23</sup> BRASIL, Projeto de Lei 21/2020. Brasília, DF. Acesso em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Acesso em: 25 de fevereiro de 2024.

seja o responsável pelo estabelecimento do sistema, encerrar o sistema se o seu controle humano não for mais possível; V - responder, na forma da lei, pelas decisões tomadas por um sistema de inteligência artificial; e VI - proteger continuamente os sistemas de inteligência artificial contra ameaças de segurança cibernética.” Os dispositivos seguintes se voltam aos deveres do Estado e sua possibilidade de fiscalização.

No caso, a partir da descrição de seus dispositivos, verifica-se uma preocupação pelo proponente Eduardo Bismarck (PDT-CE), em descrever com maior robustez, procurando dar uma organicidade ao instrumento, na busca de um corpo legislativo que possa enfrentar os principais problemas apresentados pela Inteligência Artificial. O principal objetivo dos parlamentares foi a valorização e a criação de um texto “princípios lógico norteador da inteligência artificial (IA) no Brasil”.<sup>24</sup>

Tais temáticas e questões complexas demandam uma abordagem aprofundada, bem como do reconhecimento da necessidade de se amparar o estudo, compreensão e aplicação de tais temáticas em uma moldura teórica, reconhecendo-se a importância e uma análise interdisciplinar, sobretudo, na perspectiva dos direitos fundamentais. No entanto, deixava de abordar de maneira criteriosa questões relevantes, como a existência de um órgão regulador, questões atinentes a assimetria informacional proporcionada pela velocidade de produção de dados inerente a Inteligência Artificial, bem como naqueles casos em que há decisões automatizadas<sup>25</sup>. Além disso, o texto praticamente não tratou a temática do algoritmo, silenciando sobre um dos aspectos mais importantes da Inteligência Artificial. Aliás, poderia haver uma abordagem e uma discussão voltada para o “desenvolvimento de negócios e da tecnologia”<sup>26</sup>. Eis a necessidade de uma discussão aprofundada com os agentes do mercado e com as empresas que desenvolvem tal tecnologia em solo brasileiro. Tal passo atenderia às reais necessidades das definições basilares da Inteligência Artificial, oportunizando diálogo e transdisciplinaridade de áreas do conhecimento que conversam e convergem com a IA, quais sejam: Economia e Ciência de Dados.

Nesse ponto, a defesa pela adoção de práticas de autorregulação regulada e alteração do modelo tradicional regulatório para um novo paradigma, ganham destaque nas discussões, como acentua Wilson Engelman<sup>27</sup>:

Se abre, portanto, um espaço por onde o Direito precisará se mover, talvez, inovar, mudando o seu modo de comunicação, passando de um Direito Analógico – ainda fortemente caracterizado pela presença regulatória do Estado, especialmente por parte do Poder Legislativo – para um Direito Digital –

viabilizado pelas Tecnologias Digitais (TD), com a valorização de fontes do Direito já existentes, como a Doutrina, os Contratos, especialmente os *Smart Contracts*, a ressignificação das normas contidas nos Tratados Internacionais de Direitos Humanos, além das decisões das esferas judiciais que decidem a partir dessas normas. Posto isso, é notório que a Quarta Revolução Industrial está, mais do que seus antecedentes, forçando a ruptura da tradicional “produção legislativo-estatal”<sup>28</sup>.

Nessa linha, muito mais que a valorização do discurso do mercado e dos entendimentos privados em franco diálogo com as necessidades públicas, é preciso reconhecer que a tecnologia é uma ciência disruptiva e que o direito não é suficiente para tratar o tema, como argumentam Luciano Timm e Rodrigo Dufloth<sup>29</sup>.

Então, por meio do instituto da autorregulação regulada o Estado fixa, por lei, os *standarts* mínimos de governança que devem ser seguidos e possibilita aos entes privados a implementação sectorial, com a flexibilidade e adaptabilidade exigidas para a inovação. Conforme Ricardo Campos e Rodrigo Badaró:

Diversos fatores podem ser ponderados para fortalecer e apoiar esse enfoque: a participação ativa e multidisciplinar de uma ampla gama de partes interessadas na concepção e construção de ferramentas autorregulatórias para a IA pode potencializar o compromisso e a aceitação dessas iniciativas, o que permite incorporar uma diversidade de perspectivas e conhecimentos, enriquecendo o processo como um todo. Além disso, a busca por abordagens inovadoras é essencial para lidar com os custos percebidos e os ônus associados à implementação de mecanismos de autorregulação<sup>30</sup>.

Dentre os projetos ora analisados, observa-se que o PL 2338/2023 se inclina para a autorregulação regulada (corregulação) promovendo espaços para que os agentes regulados mitiguem riscos de forma preventiva, por exemplo.

Há uma escolha de política legislativa em favor de uma autorregulação regulada com o intuito de promover nos agentes regulados atitude preventiva e a antecipação de riscos a liberdades fundamentais

Outro ponto problemático está na fixação do regime de responsabilidade civil. Cite-se nota técnica da LAPIN,

<sup>24</sup> LAPIN, Laboratório de Políticas Públicas e Internet. Nota Técnica PL nº 21-A/2020 (Redação Final): sobre o marco legal do desenvolvimento e uso da inteligência artificial no Brasil. Novembro de 2021. Acesso em: 10 de junho de 2023. Disponível em: <https://lapin.org.br/2021/11/09/nota-tecnica-atualizada-discute-o-pl-21-a-2020-do-marco-legal-de-ia/>

<sup>25</sup> BARBOSA, Mafalda Miranda. BRAGA NETTO, Felipe. FALEIROS JÚNIOR, José Luiz de Moura. (coordenadores). Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa. São Paulo: Editora Foco, 2021.

<sup>26</sup> COLOMBO, Cristiano. ENGELMANN, Wilson. FALEIROS JÚNIOR, José Luiz de Moura (coordenadores). Tutela Jurídica do Corpo Eletrônico: Novos Desafios ao Direito Digital. Editora Foco: São Paulo. 2022.

<sup>27</sup> BARBOSA, Mafalda Miranda. BRAGA NETTO, Felipe. FALEIROS JÚNIOR, José Luiz de Moura. (coordenadores). Direito Digital e inteligência Artificial: diálogos entre Brasil e Europa. São Paulo: Editora Foco, 2021.

<sup>28</sup> Idem.

<sup>29</sup> LONGHI, Maria Isabel Carvalho Sica. *Et al.* Direito e Novas Tecnologias. São Paulo: Almedina. 2020.

<sup>30</sup> CAMPOS, Ricardo; BADARÓ, Rodrigo. Desafios e aspectos da regulação da inteligência artificial. Dezembro de 2023. Acesso em: 10 de fev.2024. Disponível em: <https://legalgroundsinstitute.com/blog/desafios-e-aspectos-da-regulacao-da-inteligencia-artificial/>.

direcionada ao Senado Federal, criticando o regime de responsabilidade civil escolhido no PL nº 21-A/2020, porquanto a “aplicação pode ocorrer nas formas e nos contextos mais distintos possíveis”<sup>31</sup>, evidenciando as “diferentes características da inteligência artificial trazem diferentes riscos e desafios regulatórios, o que se reflete também nos diferentes regimes de responsabilização”<sup>32</sup>.

Ademais, traçar a responsabilidade subjetiva a casos de IA em que a imprevisibilidade, “derivado de sistemas baseados em *deep learning*, por exemplo, cujo funcionamento é extremamente complexo e difícil de ser compreendido por seus próprios desenvolvedores”<sup>33</sup>, revela insegurança, porquanto totalmente desconectada de aspectos voltados para o mercado, bem como inerentes às preocupações e características próprias da IA.

No que toca ao segundo projeto mencionado, sob o nº 240/2020, apresenta-se como uma “resposta” ao PL 21/2020, na medida em que busca retornar à proposta de concisão, com o número de sete artigos, não tendo apresentado glossário, voltando-se aos princípios, diretrizes, deveres gerais, bem como determinações ao Poder Público. Na justificação do projeto, assim se manifesta o Deputado Léo Moraes, para dar razão à proposta: “Especialistas apontam critérios que devem nortear os princípios e limites dessa nova tecnologia, como: a) Fator Humano: A I.A. deve ser o vetor de uma sociedade equitativa, servindo aos direitos humanos fundamentais, sem restringir a autonomia humana. b) Segurança: Uma I.A. precisa de algoritmos seguros, confiáveis e robustos para lidar com erros ou inconsistências em todas as suas fases. c) Privacidade: Os cidadãos devem ter controle total dos seus dados pessoais e saber quais deles podem ser usados contra eles de maneira prejudicial ou discriminatória. d) Transparência: A rastreabilidade dos sistemas de I.A. deve ser assegurada. e) Diversidade, não-discriminação e equidade: A I.A. deve levar em conta toda a gama de capacidades, habilidades e necessidades humanas. f) Bem-estar social e ambiental: Os sistemas de I.A. devem ser usados para apoiar mudanças sociais positivas e aumentar a responsabilidade ecológica. g) Prestação de contas: Mecanismos devem ser colocados em prática para garantir a responsabilidade das empresas por seus sistemas I.A., bem como pelos seus resultados.” O que se verifica é que a justificativa apresentada se revela com maior aprofundamento sobre os princípios, que o próprio texto do projeto de Lei, o que não é recomendável, na tradição jurídica brasileira.

Ainda em 2021, dois novos episódios para a formação da legislação de IA, no Brasil, foram determinantes, sendo eles a tramitação e aprovação em medida de urgência do Projeto de Lei 21/2020, na Câmara dos Deputados, e apresentação de outro Projeto de Lei, no Senado Federal, número 871/2021.

Em 2022, o Senado Federal, criou uma Comissão de Juristas com o objetivo de subsidiar uma minuta para a substituição dos

projetos até então apresentados no Congresso Nacional. Nesse contexto, em maio de 2023, foi apresentado o projeto de Lei nº 2338/2023.

### C. PL 2338/2023 e as assimetrias e desigualdades

A partir o momento em que se apresentam ferramentas econômicas, estatísticas e tecnológicas distribuídas em larga escala a custo acessível no mercado, aptas a – fazendo uso de *big data*, inteligência artificial e softwares sofisticadíssimos – medir leis, carteiras de processos e decisões judiciais (com capacidade preditiva, inclusive), surgem discussões acerca da capacidade explicativa desses sistemas, com impactos direto sobre a justificação normativa das decisões e no direito de informação dos cidadãos e usuários das tecnologias.

Aqueles que acompanharem este movimento exponencial estarão em franca vantagem perante os seus concorrentes. A abordagem crítica da legislação pretensa é fruto de um entendimento alinhado com Manoel Gustavo Neubarth Trindade ensina como assimetria informacional<sup>34</sup>, principalmente quando aplicada a questões que envolvem direito e mercado, sendo necessário a criação de meios capazes de desburocratizar a resolução de eventuais falhas de mercado das tecnologias da inteligência artificial.

Como exemplo do impacto das decisões tomadas por IA cite-se a demanda securitária que tem sido transformada pela recente multiplicação dos dados e sofisticação dos métodos de seu processamento.<sup>35</sup> As informações relacionadas ao consumidor dos seguros privados são organizadas, elaboradas e direcionadas para fins de elaboração de métricas preditivas e balizadoras da conjuntura negocial estabelecida entre os contratantes, justamente em razão da utilização de *Big data* e IA, conforme ensina Thiago Junqueira.<sup>36</sup> Nesse contexto, mesmo que se reconheça um avanço relativo a precisão e a quantidade de dados para o fornecimento do adequado seguro ao consumidor, é de reconhecer que a inteligência artificial proporciona “uma inversão na assimetria informativa existente na relação securitária”<sup>37</sup>.

Nessa conjuntura, Thiago Junqueira<sup>38</sup> personifica a assimetria informacional – tema que não foi apontado pelo PL 21-A/20 : “Diante do avanço tecnológico e da possível inversão da assimetria informativa (ou seja, os seguradores, por meio de rastreamento on-line, poderão saber mais sobre a vida e riscos dos segurados do que os próprios segurados), será imprescindível combater atitudes oportunistas dos seguradores, sob pena de que, ao fim e ao cabo, o conjunto de novas tecnologias atue como um “cavalo de troia” para os consumidores.” Outrossim, o PL 21-A/20 era carente de aspectos sancionatórios e que privilegiam a “segurança jurídica, trazendo um desequilíbrio em tais relações jurídicas já

<sup>31</sup> LAPIN, Laboratório de Políticas Públicas e Internet. Nota Técnica PL nº 21-A/2020 (Redação Final): sobre o marco legal do desenvolvimento e uso da inteligência artificial no Brasil. Novembro de 2021. Acesso em: 10 de junho de 2023. Disponível em: <https://lapin.org.br/2021/11/09/nota-tecnica-atualizada-discute-o-pl-21-a-2020-do-marco-legal-de-ia/>.

<sup>32</sup> Idem.

<sup>33</sup> Idem.

<sup>34</sup> TRINDADE, Manoel Gustavo Neubarth. Análise Econômica do Direito dos Contratos: Uma nova abordagem do direito contratual como redutor de falhas de mercado. Londrina, PR. Troth, 2021.

<sup>35</sup> BARBOSA, Mafalda Miranda. BRAGA NETTO, Felipe. FALEIROS JÚNIOR, José Luiz de Moura. (coordenadores). Direito Digital e inteligência Artificial: diálogos entre brasil e europa. São Paulo: Editora Foco, 2021.

<sup>36</sup> Idem.

<sup>37</sup> Idem.

<sup>38</sup> BARBOSA, Mafalda Miranda. BRAGA NETTO, Felipe. FALEIROS JÚNIOR, José Luiz de Moura. (coordenadores). Direito Digital e inteligência Artificial: diálogos entre brasil e europa. São Paulo: Editora Foco, 2021.

assimétricas”<sup>39</sup>, como o exemplo do mercado securitário abordado acima. A falta de *enforcement* (execução forçada)<sup>40</sup> e a imprecisão no tocante à objetividade/subjetividade da Responsabilidade Civil adotada<sup>41</sup> eram outros dois exemplos de lacunas no PL 21-A/20, evidenciando a necessidade de atenção pelo legislador em valorizar os aspectos diretamente relacionados com os custos de transação<sup>42</sup> estabelecidos entre a utilização da responsabilidade civil<sup>43</sup>. Em protesto, importantes civilistas<sup>44</sup> brasileiros direcionaram carta aberta ao Senado Federal, abordando os aspectos contraproducentes da legislação já aprovada na Câmara de Deputados, “inviabilizando a produção probatória por parte das vítimas de danos causados por Inteligências Artificiais”<sup>45</sup>.

Isso posto, segue trecho transcrito da carta em protesto a PL 21-A/20:

A proposta, ao contrário, ao privilegiar o regime da responsabilidade subjetiva, não somente impõe os custos do desenvolvimento de aplicações de Inteligência Artificial ao cidadão - em inversão patente da tábua de valores constitucional - como não fomenta os necessários incentivos para que as devidas medidas de precaução sejam tomadas quando do seu emprego. Ainda, a eleição do regime de natureza subjetiva como prioritário, em abstrato, ao contrário do que se tem defendido, não favorece o ecossistema de investimentos no Brasil. A norma cria, antes, um cenário de irresponsabilização generalizada, na medida em que torna praticamente impossível a prova pelas vítimas da culpa dos agentes que atuam na cadeia de desenvolvimento e operação de sistemas de Inteligência Artificial.<sup>46</sup>

Já, o PL 2338/2023, em sentido diferente, reconhece que o Brasil é assimétrico e desigual, positivando, dentre as definições do art. 4º, os conceitos de discriminação (direta e indireta) da Convenção Interamericana contra o Racismo, adotada pelo Brasil em 2022 com *status normativo* constitucional. Frisa, ainda, a participação de grupos vulneráveis na avaliação e no gerenciamento dos riscos de IAs que os afetam (§ 3º do Art. 7).

Justamente o ponto que envolve a compreensão a forma como os sistemas de IA atuam é foco de intensas discussões que envolvem a transparência e a explicabilidade. Cabe destacar que, conforme antes apontado, o sistema de Inteligência Artificial é fundado num banco de dados, a partir de

programação de sistemas de informática, isto é, executado por Algoritmos.

Nesse aspecto, Isabel Ferrari, Daniel Becker e Erik Navarro Wolkart ensinam: “o algoritmo é uma sequência de instruções que diz a um computador o que fazer. Como na metáfora da escada, o algoritmo divide determinada tarefa (chegar até o topo) em tarefas menores (passar por cada um dos degraus). Quanto ao seu funcionamento, podemos dividir os algoritmos em duas espécies: os programados e os não programados. Algoritmos programados seguem as operações (“o caminho”) definidas pelo programador. Assim, a informação “entra” no sistema, o algoritmo faz o que está programado para fazer com ela, e o resultado (output) “sai” do sistema. Referindo à operação de algoritmos programados, Alan Turing, no seminal *Computing Machinery and Intelligence*, escrito em 1950, propunha que, no lugar de se imitar o cérebro de um adulto, programando todas as operações a serem realizadas, seria mais produtivo adotar estratégia diversa: simular o cérebro de uma criança, com capacidade randômica de aprendizado. É mais ou menos isso que fazem os algoritmos não programados, chamados *learners*. Esses algoritmos criam outros algoritmos. Nesse caso, os dados e o resultado desejado são carregados no sistema (input), e este produz o algoritmo (output) que se transforma um no outro. Como destaca Pedro Domingos, o computador escreve a própria programação, de forma que humanos não tenham que fazê-lo.”<sup>47</sup>

Nesse contexto, vale apontar a existência de um problema inerente à utilização da I.A., isto é, a transparência algorítmica como um direito dos usuários dos sistemas de I.A, ao passo que se torna uma obrigação daqueles que geram e criam a tecnologia.

#### D. A exigência da explicabilidade como elemento de *lege ferenda*

Um ponto central das discussões que envolve a regulação do uso da Inteligência Artificial está na fixação de medidas que podem minorar a opacidade dos sistemas e, conseqüentemente, permitir a responsabilização por resultados ilegais promovidos pelos diferentes modelos de inteligência artificial.

Ensina Floridi que a explicabilidade ou “explainability” determina que “a decisão deve ser compreensível não somente aos cientistas de dados ou controladores, mas aos titulares

<sup>39</sup> COLOMBO, Cristiano. ENGELMANN, Wilson. FALEIROS JÚNIOR, José Luiz de Moura (coordenadores). *Tutela Jurídica do Corpo Eletrônico: Novos Desafios ao Direito Digital*. Editora Foco: São Paulo. 2022.

<sup>40</sup> TRINDADE, Manoel Gustavo Neubarth. *Análise Econômica do Direito dos Contratos: Uma nova abordagem do direito contratual como redutor de falhas de mercado*. Londrina, PR. Troth, 2021.

<sup>41</sup> COLOMBO, Cristiano. ENGELMANN, Wilson. FALEIROS JÚNIOR, José Luiz de Moura (coordenadores). *Tutela Jurídica do Corpo Eletrônico: Novos Desafios ao Direito Digital*. Editora Foco: São Paulo. 2022.

<sup>42</sup> TRINDADE, Manoel Gustavo Neubarth. *Análise Econômica do Direito dos Contratos: Uma nova abordagem do direito contratual como redutor de falhas de mercado*. Londrina, PR. Troth, 2021.

<sup>43</sup> COLOMBO, Cristiano. ENGELMANN, Wilson. FALEIROS JÚNIOR, José Luiz de Moura (coordenadores). *Tutela Jurídica do Corpo Eletrônico: Novos Desafios ao Direito Digital*. Editora Foco: São Paulo. 2022.

<sup>44</sup> DONEDA, Danilo. *Et al.* Conj. Disponível em: <https://www.conjur.com.br/2021-out-27/especialistas-questionam-artigo-pl-marco-legal-ia>. Acesso em: 03 de setembro de 2021.

<sup>45</sup> COLOMBO, Cristiano. ENGELMANN, Wilson. FALEIROS JÚNIOR, José Luiz de Moura (coordenadores). *Tutela Jurídica do Corpo Eletrônico: Novos Desafios ao Direito Digital*. Editora Foco: São Paulo. 2022.

<sup>46</sup> DONEDA, Danilo. *Et al.* Conj. Disponível em: <https://www.conjur.com.br/2021-out-27/especialistas-questionam-artigo-pl-marco-legal-ia>. Acesso em: 10 de junho de 2023.

<sup>47</sup> BRASIL, **Lei Geral de Proteção de Dados**. Brasília, DF. Lei nº 13.709, de 14 de Agosto de 2018. Acesso em: 11 de fevereiro de 2024. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm).



leigos dos dados (ou algum representante) afetados pela decisão.”<sup>48</sup>

Renato Leite Monteiro defendendo um direito à explicação esclarece que ele não deve se confundir com a publicização de códigos-fonte e que a o direito à explicação está relacionado com o empoderamento dos indivíduos e da sociedade em, a partir de informações úteis sobre processos automatizados, entenderem o seu funcionamento e tomarem decisões sobre esses, evitando muitas práticas discriminatórias e inadequadas.<sup>49</sup>

Existem riscos quando não se compreende como uma decisão exclusivamente automatizada foi tomada, sendo que pode ser pautada por erros, discriminações, tratando-se de um resultado enviesado. Benanti refere sobre os riscos desta “nova época”, na medida em que os estudiosos têm abandonado a “pesquisa da causa” dos eventos, a “cognitio rei per causas”, rumo a uma nova forma de buscar a verdade por meio da correlação, ou seja, de dados estatísticos entre duas grandezas. Aqui há o risco da correlação espúria, que é aquela que não necessariamente tem uma relação direta entre causa e efeito.<sup>50</sup>

No que toca à explicabilidade, como se verifica, no PL 5051 de 2019, já existiam propostas de disposições expressas quanto à explicabilidade, na medida que em seu artigo 2º, estabelece com fundamento: “IV – a transparência, a confiabilidade e a possibilidade de auditoria dos sistemas; No PL 21 de 2020, em seu artigo 2º, há referência que “conhecimento em inteligência artificial” significa “entender”. Para entender, deve haver uma explicação de como foram gerados os resultados, de que não existem violações a direitos fundamentais. E, no artigo 6º, de forma expressa dispõe que: “IV - transparência e explicabilidade: garantia de transparência sobre o uso e funcionamento dos sistemas de inteligência artificial e de divulgação responsável do conhecimento de inteligência artificial, observados os segredos comercial e industrial, e de conscientização das partes interessadas sobre suas interações com os sistemas, inclusive no local de trabalho;”. Interessante que o tema acaba por ser tratado tanto pelo direito à informação da pessoa que de qualquer forma foi exposta à tecnologia, como também sob a regência da propriedade intelectual, como do próprio direito do trabalho. Ressalte-se que, no artigo 7º, do PL 21/2020, há o dever de que haja: “I - ciência da instituição responsável pelo sistema de inteligência artificial; II - acesso a informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo sistema de inteligência artificial que lhes afetem adversamente, observados os segredos comercial e industrial; e III - acesso a informações claras e completas sobre o uso, pelos sistemas, de seus dados sensíveis, conforme disposto no art. 5º, II, da Lei 13.709, de 2018 – Lei Geral de Proteção de Dados.” De tal forma, presente um plexo de direitos que garantem a explicabilidade.

Por sua vez, o Capítulo IV, do PL 2338/2023, elenca as obrigações dos agentes envolvidos na construção da I.A. da

utilização do termo “Governança dos sistemas de Inteligência Artificial”, evidenciando as características do Art. 4 do PL 2338/2023, como observa-se: “Art. 19. Os agentes de inteligência artificial estabelecerão estruturas de governança e processos internos aptos a garantir a segurança dos sistemas e o atendimento dos direitos de pessoas afetadas, nos termos previstos no Capítulo II desta Lei e da legislação pertinente, que incluirão, pelo menos: I – medidas de transparência quanto ao emprego de sistemas de inteligência artificial na interação com pessoas naturais, o que inclui o uso de interfaces ser humano-máquina adequadas e suficientemente claras e informativas; II – transparência quanto às medidas de governança adotadas no desenvolvimento e emprego do sistema de inteligência artificial pela organização; III – medidas de gestão de dados adequadas para a mitigação e prevenção de potenciais vieses discriminatórios; IV – legitimação do tratamento de dados conforme a legislação de proteção de dados, inclusive por meio da adoção de medidas de privacidade desde a concepção e por padrão e da adoção de técnicas que minimizem o uso de dados pessoais; V – adoção de parâmetros adequados de separação e organização dos dados para treinamento, teste e validação dos resultados do sistema; e VI – adoção de medidas adequadas de segurança da informação desde a concepção até a operação do sistema. § 1º As medidas de governança dos sistemas de inteligência artificial são aplicáveis ao longo de todo o seu ciclo de vida, desde a concepção inicial até o encerramento de suas atividades e descontinuação. § 2º A documentação técnica de sistemas de inteligência artificial de alto risco será elaborada antes de sua disponibilização no mercado ou de seu uso para prestação de serviço e será mantida atualizada durante sua utilização.”

A transparência algorítmica, termo cunhado para melhor resumir a conjuntura de ações previstas na construção legislativa, é acompanhada de outras características que garantem a explicabilidade e auditabilidade. Importante frisar que a ideia de transparência algorítmica não necessariamente passa por revelar os códigos “ou das equações matemáticas que possibilitam a operação computacional inteligente, mas que os sistemas em uso possam ser verificados mediante técnicas de inferência”. Sendo assim, o que o texto busca demonstrar é a necessidade de criar mecanismos que sejam capazes “de explicitar de modo inteligível as etapas fundamentais da formação da decisão” vinculada ao sistema de Inteligência Artificial.

Posto isso, o Art. 20 da Lei Geral de Proteção de Dados aborda, objetivamente, que o titular dos dados tem o direito de solicitar a revisão dos dados de decisões automatizadas, isto é, por IA unicamente, sem a intervenção humana.<sup>51</sup> Assim, elencam-se três mecanismos para garantir a explicabilidade, isto é, a transparência algorítmica, no processo de tomada de decisão da IA, quais sejam:

- i. Compreensão plena da tomada de decisão automatizada;

<sup>48</sup> FLORIDI, Luciano et ali. **The ethics of algorithms Mapping the debate**. Big Data & Society July–December 2016: 1–21 The Author(s) 2016 Reprints and permissions:sagepub.com/journalsPermissions.nav DOI: 10.1177/2053951716679679 bds.sagepub.com

<sup>49</sup> MONTEIRO, Renato Leite. **Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de dados no Brasil.2021**. Tese. Universidade de São Paulo.

<sup>50</sup> BENANTI, Paulo. **Human in the loop**. Decisioni umane e intelligenze artificiali. Florença: Mondadori Università, 2024, p. 38-39. Benanti refere o número de pombinhas no céu e o número de casamentos, como correlação espúria, não havendo relação de causa e efeito, mas coincidência da migração das aves com a época em que noivos têm preferência para se matrimoniarem.

<sup>51</sup> BRASIL, **Lei Geral de Proteção de Dados**. Brasília, DF. Lei nº 13.709, de 14 de Agosto de 2018. Acesso em: 11 de fevereiro de 2024. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm).

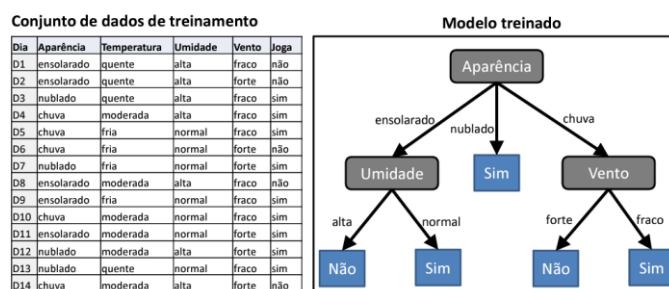
- ii. Reflexos cíveis daqueles que desenvolveram a tecnologia;
- iii. Ética como preceito fundamental no processo de decisão.

Outrossim, ao citar os princípios da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) para inteligência artificial, a Dra. Isabela Ferrari lembra que o Brasil aderiu a tais mandamentos, especialmente a explicabilidade e transparência, *it litteris*:

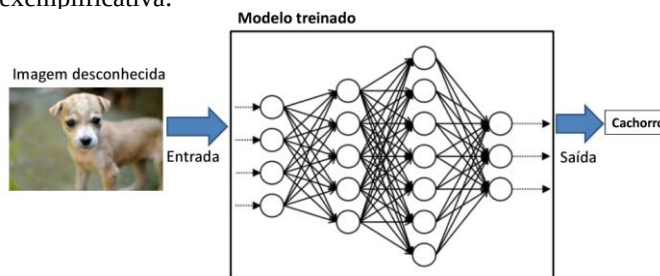
O Brasil aderiu aos princípios da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) para a inteligência artificial em 21/05/2019. Eles são aplicáveis aos sistemas inteligentes, entendidos como aqueles que, baseados em máquinas, são empregados para fazer previsões, recomendações ou tomar decisões que influenciam ambientes reais ou virtuais a partir de um conjunto de objetivos definidos por humanos. Sua incidência dura todo o ciclo de vida dos sistemas inteligentes, compreendendo o seu design, a seleção de dados e modelagem; sua verificação e validação; seu desenvolvimento, operação e monitoramento. Incidem sobre todos os atores de IA, indivíduos ou organizações que desempenhem papel importante durante o ciclo de vida do sistema. São cinco os princípios da OCDE para a IA confiável: crescimento inclusivo, desenvolvimento sustentável e bem-estar; valores centrados no ser humano e na equidade; transparência e Explicabilidade; robustez, segurança e proteção; e responsabilização/prestação de contas (accountability). A equidade é endereçada diretamente no segundo princípio, ocasião em que se destaca que os atores de IA devem respeitar os direitos humanos durante todo o ciclo do sistema inteligente, no que se incluem as ideias de não discriminação e igualdade, diversidade, equidade e justiça social. No bojo do princípio da transparência e explicabilidade, ressalta-se a necessidade de estimular um entendimento geral sobre os sistemas de IA, e de permitir que os adversamente afetados por esses softwares compreendam os seus resultados e possam impugná-los, bem como aos dados e à lógica que deram origem a eles. No âmbito da robustez, segurança e proteção destaca-se que os atores de IA devem garantir a rastreabilidade com relação a bases de dados, processos e decisões tomadas durante o ciclo de vida da IA para permitir a análise de seus resultados e sanar dúvidas, de

acordo com o estado da arte, e atentos ao contexto em que empregados os algoritmos inteligentes.<sup>52</sup>

Como se percebe, os desafios são muitos, tanto do ponto de vista tecnológico quanto do lado jurídico. Os desafios do direito, principalmente, estão relacionados a complexidade da tecnologia como um todo, porquanto a existência de redes neurais profundas e de difícil interpretação – não sendo irrelevante ler explicabilidade como o ato de interpretar a tecnologia no caso da IA –, ao passo que os desenvolvedores também buscam a eficiência da tecnologia para criarem produtos comercializáveis.<sup>53</sup> Para demonstrar em imagem a definição de uma rede neural interpretável de IA, segue modelo retirado do trabalho de José Carbonera<sup>54</sup>:



Assim, num cenário de IA interpretável, os riscos de não haver a compreensão necessária são baixos, conforme o exemplo acima demonstrado. Porém, se porventura a análise da explicabilidade se der numa IA Opaca, isto é, tecnologia de redes neurais artificiais que utilizam *deep learnig*, não presunção absoluta das informações utilizadas para o *output*, ou seja, “os algoritmos de aprendizagem profunda transformam as informações de entrada (inputs) usando mais camadas de do que algoritmos de aprendizagem superficial”<sup>55</sup>. No intuito de elucidar de maneira ainda mais clara, segue mais uma figura exemplificativa:



56

Por essas razões, o PL 2338/23 busca definir o grau de riscos mediante a utilização da IA, conforme dispõe no Capítulo III do texto. A sua divisão é feita em três seções nas quais dividem-se em: Avaliação preliminar; Risco excessivo e Alto Risco. Especificamente na questão relacionada aos riscos, a doutrina

<sup>52</sup> FERRARI, Isabela. Discriminação algorítmica e poder judiciário: limites à adoção de sistemas de decisões algorítmica no poder judiciário brasileiro. 1ª Ed. Florianópolis. Emais, 2023, pg.359.

<sup>53</sup> FERRARI, Isabela. Discriminação algorítmica e poder judiciário: limites à adoção de sistemas de decisões algorítmica no poder judiciário brasileiro. 1ª Ed. Florianópolis. Emais, 2023, pg.53.

<sup>54</sup> CARBONERA, José Luís. A inteligência Artificial e o poder judiciário. Acesso em: 11 de fevereiro de 2024. Disponível em: [https://www.trf3.jus.br/documentos/emag/Cursos/550\\_-\\_Inteligencia\\_Artificial\\_e\\_o\\_Poder\\_Judiciario/Arquivos\\_para\\_download/CARBONERA\\_Joel\\_Luis\\_-\\_Explicabilidade\\_em\\_IA.pdf](https://www.trf3.jus.br/documentos/emag/Cursos/550_-_Inteligencia_Artificial_e_o_Poder_Judiciario/Arquivos_para_download/CARBONERA_Joel_Luis_-_Explicabilidade_em_IA.pdf).

<sup>55</sup> FERRARI, Isabela. Discriminação algorítmica e poder judiciário: limites à adoção de sistemas de decisões algorítmica no poder judiciário brasileiro. 1ª Ed. Florianópolis. Emais, 2023, pg.53.

<sup>56</sup> CARBONERA, José Luís. A inteligência Artificial e o poder judiciário. Acesso em: 11 de fevereiro de 2024. Disponível em: [https://www.trf3.jus.br/documentos/emag/Cursos/550\\_-\\_Inteligencia\\_Artificial\\_e\\_o\\_Poder\\_Judiciario/Arquivos\\_para\\_download/CARBONERA\\_Joel\\_Luis\\_-\\_Explicabilidade\\_em\\_IA.pdf](https://www.trf3.jus.br/documentos/emag/Cursos/550_-_Inteligencia_Artificial_e_o_Poder_Judiciario/Arquivos_para_download/CARBONERA_Joel_Luis_-_Explicabilidade_em_IA.pdf).

já se debruça para parametrizar e facilitar a compreensão do usuário da IA no que, de fato, aquela tecnologia por ele utilizada tem poder de alcançar.

Destaque-se a redação do Art. 11 do PL 2388/2023 que exige revisão humana quando as decisões, previsões ou recomendações geradas por sistemas de inteligência artificial tenham um impacto irreversível ou de difícil reversão ou envolvam decisões que possam gerar riscos à vida ou à integridade física de indivíduos<sup>57</sup>.

Aprofundando sobre a necessidade de assegurar mecanismos regulatórios que garantam aos indivíduos compreender as informações que lhe serão fornecidas, é que o LAPIN, ao apresentar nota técnica ao PL 2338/2023, salienta que a regulação tem que trazer garantia contra uma possível “opacidade por transparência”. Esta ocorre quando há um fornecimento de informações em excesso que torna impossível a outra pessoa ler tudo que ali contém, impedindo a compreensão efetiva de seu conteúdo<sup>57</sup>.

Ademais, a explicabilidade pode incidir em duas dimensões: sobre os dados de entrada utilizados; acerca do processo de tomada de decisão. Verifique-se a explicação sobre os processos de tomada de decisão devem ser de superlativa exigência para os produtos tecnológicos voltados ao setor jurídico como provedores de analytics (análise de dados) e jurimetria, uma vez que “qualquer ato ou decisão judicial ou administrativa somente é juridicamente válido na medida em que possa ser juridicamente justificado”<sup>58</sup>

É fundamental que toda informação prestada a respeito do sistema ao sujeito afetado seja suficiente para que este compreenda seu funcionamento e suas decisões e previsões. Em outras palavras: o sujeito precisa conseguir identificar potenciais violações de seus direitos pelo sistema. Portanto, devem ser providas de forma clara, concisa, em linguagem de fácil compreensão, e permitir, especialmente em casos de usos de sistemas de alto risco, mecanismos para requisição de mais informações.

Nesse sentido, a importância da explicabilidade, como elemento dos projetos legislativos, compondo o *framework* regulatório, a fim de que discriminações, erros, equívocos ou mesmo correlações espúrias sejam evitadas, importando em violações a direitos fundamentais. A explicabilidade mesmo nos casos mais complexos é medida que deve ser buscada para construção de sistemas que contribuam para a proteção de direito.

### III. CONSIDERAÇÕES FINAIS

As discussões acerca das respostas regulatórias aptas a reger a utilização da IA estão na pauta brasileira, com destaque para o legislativo federal, aliás em consonância com uma movimentação global de busca por governança e regulação dos sistemas de IA. Nesse sentido, o PL 21-A/2020, por mais bem intencionado, não traz soluções efetivas, padecendo de densidade normativa capaz de promover um direcionamento

jurídico eficaz para o tema. O texto substitutivo, elaborado por Comissão de Juristas, corporificado no Projeto de Lei 2338/2023, afasta diversas lacunas fixando procedimentos que permitam uma classificação de acordo com o risco dos sistemas de IA. A assimetria informacional seguramente é um dos maiores desafios para o legislador contemporâneo que precisa assegurar o direito fundamental dos indivíduos à informação e, consequentemente, fixar um direito à explicabilidade das decisões e escolhas algorítmicas, sem descuidar para a proteção do segredo industrial.

Por outro lado, não há mais espaço para avançar sem a presença e o avanço da utilização de sistemas de inteligência artificial explicáveis em seus processos e indicações de decisões, em suas mais diversas e infinitas possibilidades de utilização.

### IV. REFERÊNCIAS BIBLIOGRÁFICAS

- BARBOSA, Mafalda Miranda. BRAGA NETTO, Felipe. FALEIROS JÚNIOR, José Luiz de Moura. (coordenadores). Direito Digital e inteligência Artificial: diálogos entre brasil e europa. São Paulo: Editora Foco, 2021.
- BENANTI, Paulo. Human in the loop. Decisioni umane e intelligenze artificiali. Florença: Mondadori Università, 2024, p. 38-39.
- BLUM, Renato Opice. LÓPEZ, Nuria. Os desafios da regulamentação de inteligência artificial. Revista de Direitos e Novas Tecnologias. Vol. 9/2020. Out-dez/2020.
- BRASIL, Código de Defesa do Consumidor, Brasília, DF. Lei nº 8.078, de 11 de setembro de 1990. Acesso em: 10 de junho de 2023. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/18078compilado](https://www.planalto.gov.br/ccivil_03/leis/18078compilado).
- BRASIL, Projeto de Lei 5051/2019. Brasília, DF. Acesso em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1708613194891&disposition=inline>. Acesso em: 25 fev de 2024.
- BRASIL, Projeto de Lei 21/2020. Brasília, DF. Acesso em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Acesso em: 30 de agosto de 2022.
- BRASIL, Projeto de Lei 2338/2023, Brasília, DF. Acesso em: 10 de junho de 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>.
- BRASIL. Constituição Federal, promulgada em 05 de outubro de 1988. Brasília, DF. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 27.07.2022.
- CAMPOS, Ricardo; BADARÓ, Rodrigo. Desafios e aspectos da regulação da inteligência artificial. Dezembro de 2023. Acesso em: 10 de fev.2024. Disponível em: <https://legalgroundsinstitute.com/blog/desafios-e-aspectos-da-regulacao-da-inteligencia-artificial/>.
- COLOMBO, Cristiano. ENGELMANN, Wilson. FALEIROS JÚNIOR, José Luiz de Moura (coordenadores). Tutela Jurídica

<sup>57</sup> LAPIN, Laboratório de Políticas Públicas e Internet. Nota Técnica PL nº 2338/2023 (Redação Final): sobre o marco legal do desenvolvimento e uso da inteligência artificial no Brasil. Acesso em: 10 de junho de 2023. Disponível em: <https://lapin.org.br/2022/07/05/contribuicao-a-comissao-de-juristas-do-senado-federal-responsavel-por-subsidiar-a-elaboracao-de-minuta-de-substitutivo-para-o-marco-regulatorio-da-inteligencia-artificial-no-brasil/>.

<sup>58</sup> MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. Suprema: revista de estudos constitucionais, Brasília, v. 1, n. 1, p. 154-180, jan./jun. 2021

do Corpo Eletrônico: Novos Desafios ao Direito Digital. Editora Foco: São Paulo. 2022.

CUSTERS, Bart; FOSCH-VILLARONGA, Eduard. Humanizing Machines: Introduction and Overview. In: CUSTERS, Bart; FOSCH-VILLARONGA, Eduard (Orgs.) Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice. Haia: T.M.C. Asser Press, 2022, 3-28

Comissão de Juristas responsável por subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nº 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da Inteligência Artificial no Brasil, criada pelo Ato do Presidente do Senado Federal nº 4, de 17 de fevereiro de 2022. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento/download/211b69b7-dfcf-45fd-9de6-763becafca90>. Acesso em: 10 de junho de 2023.

Conselho Nacional de Justiça. Disponível em: <https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,currsel>. Acesso em: 11 de outubro de 2023.

COSTA, Aryela Couto. BITTENCOURT, Luís Antônio de Aguiar. Inteligência Artificial: uma visão prospectiva sobre seus principais efeitos jurídicos. Revista das Faculdades Integradas Vianna Júnior. V.12. n.2. Juiz de Fora. Jul-dez 2021.

DONEDA, Danilo. *Et al.* Conj. Disponível em: <https://www.conjur.com.br/2021-out-27/especialistas-questionam-artigo-pl-marco-legal-ia>. Acesso em: 03 de setembro de 2021.

FERRARI, Isabel. BECKER, Daniel. WOLKART, Erik Navarro. Arbitrium Ex Machina: Panorama, riscos e necessidades das decisões informadas por algoritmos. Revista dos Tribunais. vol. 995/2018. p. 635 - 655. Set, 2018.

FERRARI, Isabela. Discriminação algorítmica e poder judiciário: limites à adoção de sistemas de decisões algorítmica no poder judiciário brasileiro. 1ª Ed. Florianópolis. Emais, 2023.

HELDER, Darlan. Biden assina 1º decreto para a regulamentar inteligência artificial nos EUA. Disponível em: <https://g1.globo.com/tecnologia/noticia/2023/11/01/biden-assina-1o-decreto-para-regulamentar-inteligencia-artificial-nos-eua-veja-os-principais-pontos.ghtml>. Acesso em: 12 de outubro de 2023.

FLORIDI, Luciano et ali. The ethics of algorithms Mapping the debate. Big Data & Society July–December 2016: 1–21 The Author(s) 2016 Reprints and permissions:sagepub.com/journalsPermissions.nav DOI: 10.1177/2053951716679679 bds.sagepub.com

LAPIN, Laboratório de Políticas Públicas e Internet. Nota Técnica PL nº 21-A/2020 (Redação Final): sobre o marco legal do desenvolvimento e uso da inteligência artificial no Brasil. Novembro de 2021. Acesso em: 02 de novembro de 2022. Disponível em: <https://lapin.org.br/2021/11/09/nota-tecnica-atualizada-discute-o-pl-21-a-2020-do-marco-legal-de-ia/>

LAPIN, Laboratório de Políticas Públicas e Internet. Nota Técnica PL nº 2338/2023 (Redação Final): sobre o marco legal do desenvolvimento e uso da inteligência artificial no Brasil. Acesso em: 10 de junho de 2023. Disponível em: <https://lapin.org.br/2022/07/05/contribuicao-a-comissao-de-juristas-do-senado-federal-responsavel-por-subsidiar-a-elaboracao-de-minuta-de-substitutivo-para-o-marco-regulatorio-da-inteligencia-artificial-no-brasil/>.

LONGHI, Maria Isabel Carvalho Sica. *Et al.* Direito e Novas Tecnologias. São Paulo: Almedina. 2020.

MACHADO, Fernanda de Vargas; COLOMBO, Cristiano. Inteligência artificial aplicada à atividade jurisdicional: desafios e perspectivas para sua implementação no Judiciário. Revista da Escola Judicial do TRT4, [S. l.], v. 3, n. 5, p. 117–141, 2021. Disponível: <https://rejtrt4.emnuvens.com.br/revistaejud4/article/view/113>. Acesso: 25 fev. 2024.

MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. Suprema: revista de estudos constitucionais, Brasília, v. 1, n. 1, p. 154-180, jan./ jun. 2021. Disponível em: [https://cadmus.eui.eu/bitstream/handle/1814/71840/MARANH%C3%83O\\_et\\_al\\_2021.pdf?sequence=1&isAllowed=y](https://cadmus.eui.eu/bitstream/handle/1814/71840/MARANH%C3%83O_et_al_2021.pdf?sequence=1&isAllowed=y).

MELO, Bricio da Anunciação. ANDRADE, Diogo de Calasans Melo. Inteligência Artificial e União Europeia: uma breve análise quanto à proposta de regulação apresentada pelo conselho Europeu. Revista dos Tribunais. vol. 1041/2022. p. 203 - 219. Julho, 2022.

MONTEIRO, Renato Leite. Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de dados no Brasil. 2021. Tese. Universidade de São Paulo.

PARLAMENTO EUROPEU, Proposta de Regulamento do parlamento Europeu e do Conselho que estabelece Regras Harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados Atos Legislativos da União Europeia. Acesso em: 10 de junho de 2023. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A52021PC0206>.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 3 de maio de 2022, sobre a inteligência artificial na era digital. Disponível em: [https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140\\_PT.html](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_PT.html). Acesso em: 10 de junho de 2023.

PINTO, Henrique Alves. GUEDES, Jefferson Carús. CÉSAR, Joaquim Portes de Cerqueira. (coordenadores). Inteligência Artificial aplicada ao processo de tomada de decisões. 1 ed. São Paulo: D'Plácido, 2022.

TRINDADE, Manoel Gustavo Neubarth. Análise Econômica do Direito dos Contratos: Uma nova abordagem do direito contratual como redutor de falhas de mercado. Londrina, PR. Troth, 2021.

VASCONCELOS FILHOS, Oton de Albuquerque. SILVA, Gabriel Carvalho Nunes. Direito e Inteligência Artificial: A eficácia das decisões judiciais no contexto do PL 5.051/2019. Revista de Processo. Vol. 321/2021. P.367/391. Nov. 2021.

# LAS COMPETENCIAS DIGITALES EN LA FORMACION DEL ABOGADO Y LA PRÁCTICA DEL DERECHO

Chávez Valdivia, Ana Karin <sup>1</sup>

## Abstract

*La tecnología en sus diversas manifestaciones se encuentra inmersa en todas las áreas del conocimiento humano, si bien su presencia no es igualmente significativa en cada una de ellas, indiscutiblemente su vertiginoso desarrollo demanda la presencia de abogados con conocimientos en temáticas legales convergentes con la tecnología y que además cuenten con ciertas competencias en el manejo de herramientas de esta naturaleza.*

*Si bien, desde sus inicios, uno de los principales cuestionamientos en torno a la incursión de la IA en el ejercicio legal se ha centrado en el razonamiento jurídico y la argumentación, el panorama se complejiza cada vez más debido a la presencia de diferentes plataformas que no sólo coadyuvan al desarrollo de la labor del operador jurídico, sino que también, en cierto punto y en determinados contextos, llegan a sustituirla.*

*Este escenario, conlleva necesariamente a cuestionarse en torno a la diversidad de repercusiones e implicancias que acarreará el desarrollo tecnológico dentro del derecho; más aún, cuando muchos abogados no han sido dotados de los conocimientos básicos que les permita ejercer su profesión de la mano con las herramientas existentes que nos ofrece la tecnología.*

**Palabras clave:** tecnología, legaltech, competencias digitales, Derecho, formación legal, inteligencia artificial, plan de estudios,

argumentación jurídica, práctica jurídica, abogado.

## I. INTRODUCCIÓN

Nos encontramos en un escenario en el cual la práctica jurídica está cambiando vertiginosamente; si bien los avances tecnológicos de las últimas décadas no sólo han cambiado la forma de comunicarse, revolucionado los procesos empresariales e impulsado aún más la globalización; la profesión jurídica - que no suele responder a los cambios con rapidez - ha reconocido que estas transformaciones son inevitables debido a que en la práctica jurídica, como en otras profesiones, el empleo de la tecnología maximiza la eficiencia y la productividad, al tiempo de mejorar la comunicación.

En los últimos años los diversos avances tecnológicos han conducido al abandono progresivo de las formas jurídicas tradicionales; siendo así, en sus inicios se identificaron aquellos procesos que van desde la digitalización y posterior gestión de recursos jurídicos con el consecuente incremento de bases de datos; posteriormente se constataron las plataformas diseñadas para interactuar en múltiples formas dentro de los sectores público y privado además del empleo de diferentes herramientas capaces de realizar las labores que un abogado hacía años atrás, así como un uso progresivo de la inteligencia artificial que supone un cambio significativo en la forma de realizar y comprender el valor que implica un trabajo legal. Al tiempo que se evidencia la existencia de modelos computacionales que tendrán la

---

<sup>1</sup> achavez@ulasalle.edu.pe, Coordinadora académica de la Facultad de Derecho y Relaciones Internacionales de la Universidad La Salle de Arequipa-Perú.

capacidad de argumentar jurídicamente y modelos de razonamiento jurídico.

Oskamp y Lodder [1] señalan que para que el desarrollo de sistemas y tecnologías tengan realmente un impacto en la práctica jurídica es necesario contar desde una fase muy temprana con el aporte de las personas que tienen que trabajar con ellas, pero para que esto suceda tendrán que comprender al menos algunas de las cosas que estos sistemas pueden y no pueden hacer.

En este contexto, si bien la formación legal ofrecida por algunas universidades intenta cubrir las necesidades relacionadas a los conocimientos esenciales para la formación de los abogados; es probable que aún no sea posible atenderla de una manera completa y eficaz en razón a que: no todas las facultades de Derecho priorizan las competencias tecnológicas legales en sus estudiantes por diversas razones; no existe un método estándar para establecer y medir las habilidades, la comprensión y la competencia en tecnología legal de un abogado, al tiempo que las capacidades digitales de los docentes muchas veces son objeto de observación y análisis.

Consideramos que las universidades deben contribuir no solo con la formación profesional de los estudiantes, sino hasta cierto punto deben asegurar su transición exitosa al mundo laboral legal. No obstante, debe tenerse presente que ya algunos sectores vaticinan el fin de muchas profesiones y oficios en los próximos años, por lo que la necesidad de replantearse los contenidos de los planes de estudio en las facultades de Derecho deviene en una tarea imperativa.

## **II. COMPETENCIAS DIGITALES Y SUS IMPLICANCIAS**

Vargas [2] señala que el objetivo principal del aprendizaje consiste no sólo en la adquisición de conocimientos por parte del estudiante, sin que éstos queden supeditados al desarrollo de una serie de competencias, esto es, desarrollen complejos sistemas de conocimientos, capacidades y actitudes, en función de los perfiles académicos y de los correspondientes perfiles profesionales.

El enfoque actual obliga al desplazamiento de una educación centrada en la enseñanza hacia una educación centrada en el aprendizaje y en este proceso es evidente la relevancia del enfoque centrado en las competencias. Se pasa de un énfasis en la adquisición y transmisión del conocimiento a un nuevo paradigma más centrado en el estudiante, una transformación del papel del educador, una nueva definición de objetivos, un cambio en el enfoque de las actividades educativas, un desplazamiento del

énfasis en los suministros de conocimientos (input) a los resultados (output) y un cambio en la organización del aprendizaje. Aquí entran de lleno el término de competencias, que incluye conocimientos, comprensión y habilidades que se espera que el estudiante domine, comprenda y demuestre después de completar un proceso de aprendizaje.

En cuanto al objeto de aprendizaje, el reto que supone desarrollar competencias, entendidas éstas como habilidades personales o tendencias de comportamiento, frente al tradicional conocimiento técnico, implica la necesidad de dotar al profesional de oportunidades de práctica reales. El uso del término competencia es una consecuencia de la necesidad de superar una enseñanza que, en la mayoría de los casos, se ha reducido al aprendizaje memorístico de conocimientos, que conlleva la dificultad para que estos conocimientos puedan ser aplicados en la vida real.

En la práctica jurídica, así como en otras profesiones y diversas áreas del conocimiento, el uso creciente de la tecnología en sus diversas manifestaciones no es nuevo; sin embargo, su inminente desarrollo, así como la diversidad de aplicaciones derivadas de sus múltiples funcionalidades, han planteado, y seguirán planteando retos a la profesión jurídica de manera cada vez más profunda y dando lugar muchas veces a cambios de naturaleza disruptiva.

En este contexto, señala June Wang [3] que si bien la abogacía debe adaptarse a los cambios tecnológicos, con mayor razón debe hacerlo la formación jurídica impartida a los futuros profesionales por lo que refiere que las tecnologías en la enseñanza del Derecho nos plantean tres conjuntos de consideraciones, a saber: la adopción y adaptación de las tecnologías a la enseñanza y el aprendizaje; el estudio y la investigación de las perturbaciones y otros impactos de las tecnologías en la sociedad para ayudar a formular respuestas jurídicas a los mismos; y la preparación de los futuros abogados.

Por su parte O'Leary [4] señala que la tecnología ha cambiado el ejercicio moderno de la abogacía, pero la mayoría de las facultades de Derecho no incorporan el llamado "Deber de Competencia Tecnológica" en el plan de estudios obligatorio. Si bien la formación jurídica que se les brinda a los estudiantes debería contemplar este tipo de competencias, no hay una forma clara de cómo integrar esta valiosa competencia profesional en el plan de estudios de todos los estudiantes.

En consideración de O'Leary el plan de estudios debe reflejar las expectativas de cómo

los abogados del siglo XXI realizan las tareas fundamentales de este siglo y estas tareas incluyen enfrentar nuevos desafíos éticos y utilizar herramientas para crear productos de trabajo eficientes y eficaces, por lo que las competencias en tecnología ya no serán opcionales. Siendo así; los contenidos de los planes de estudios pueden concientizar sobre el impacto de la tecnología en el trabajo jurídico cotidiano y proporcionar a los estudiantes experiencia práctica.

En este orden de ideas, la autora aborda cinco competencias necesarias a su entender: Competencia en dominio de documentos legales, analítica jurídica e integración de documentos, e-discovery, tecnología en práctica del derecho, seguridad de datos y agrega que éstas serán trascendentes para seguir siendo competitivo y relevantes [4].

De otro lado Mironova, Bogdanova y Simonova [5] anotan que actualmente casi todos los estudiantes pertenecen a la generación de nativos digitales, por lo que demuestran mucho mayor propensión a emplear la tecnología en su día a día; siendo así, consideran que en la era de la digitalización del Derecho los abogados tienen la oportunidad de liberar su potencial creativo a través de la creación de productos Legaltech.

Por su parte, Díaz y Loyola [6] consideran que el concepto de Competencia Digital es relativamente reciente y ubican sus orígenes en el 2010 en Europa continental y posteriormente en otras regiones, como América Latina y Estados Unidos. Agregan los autores que si bien se podría definir que una persona competente digitalmente es aquella que puede manejar TIC; las competencias digitales son mucho más que una simple pericia en el manejo de programas y equipos informáticos y de comunicación digital, por lo que en consideración de los autores el concepto de competencia digital es multidimensional debido a que engloba un conjunto de habilidades y actitudes interrelacionadas que comprenden la técnica, la información, la creación de contenidos, los medios, la comunicación, la resolución de problemas, así como la toma de decisiones estratégicas y éticas.

Acorde a Arias, Torres y Yáñez [7] las competencias digitales están vinculadas a los servicios que se proporcionen dentro de las actividades on line, agregan los autores que las competencias digitales no solo abarcan la adquisición de las destrezas o habilidades en la utilización de las tecnologías; sino también, saber cuándo, cómo y para qué utilizarlas.

En este orden de ideas, Kate Galloway [8] señala que los contextos más amplios reúnen una

variedad de temas y problemas reflejados en la educación legal y ofrecen la oportunidad de una experiencia de aprendizaje más crítica y atractiva que resulta en un graduado más completo, por lo que considera que comprender y comprometerse con las tecnologías digitales en un contexto amplio demanda alfabetizaciones digitales con la finalidad de lograr una educación legal reimaginada como preparación para la práctica legal contemporánea y futura, al tiempo que como resultado del aumento rápido y exponencial de la tecnología aborda la importancia del diseño del plan de estudios.

Refiere la autora que, el término de alfabetización digital ha evolucionado de manera bastante orgánica, por lo que, en un concepto ampliado, se enfatiza en la diversidad de prácticas sociales y culturales que cubren el término en sí mismo y sus diversas clasificaciones; así mismo, respalda el conocimiento digital y las habilidades y las actitudes particulares propias del Derecho.

Evidenciamos la necesidad de una integración coherente y lógica entre el Derecho informático (llamado también Derecho tecnológico, Derecho de la alta tecnología, Derecho digital - entre otras terminologías afines-) las tecnologías viabilizadoras del ejercicio del Derecho y el Derecho como tecnología, para así poder informar los planes de estudios de las carreras y contribuir al proceso de enseñanza- aprendizaje ya que consideramos que esta articulación permitirá desarrollar conocimientos, habilidades y atributos centrales para la formación profesional especializada, incluso dentro de una estructura regulada de educación legal.

En esta línea, según el documento denominado Marco de Competencias Digitales para la formación del personal de Justicia, emitido por el Ministerio de Justicia del Gobierno español [9] las competencias con las que tienen que contar los operadores del derecho deben estar materializadas en los planes de formación, al tiempo que éstas demandan su actualización y revisión periódica para poder mantenerse actualizadas ante los cambios tecnológicos, normativos y las demandas emergentes del sector.

C. Grosso [10] por su parte, brinda una clasificación de las áreas en las que se produce impacto en la actividad del operador del derecho, entre las que considera a las herramientas de organización, de información, de gestión judicial, contexto de los clientes y herramientas de formación. Refiere además el autor, que las competencias de un profesional del Derecho hoy más que nunca no pueden limitarse al conocimiento de la ley y la memorización de



conceptos y agrega, citando a Bilinkis, que si se cree que educar es dar conocimiento técnico y disponer enseñanza para el cumplimiento de normas, en realidad se está preparando a la persona para el pasado y no para el futuro. Siendo así, Pasvenskienė y Astromskis [11] enfatizan que las deficiencias en la formación jurídica, pueden afectar de manera muy significativa a la capacidad de los futuros abogados para desarrollar relaciones con el mundo exterior, ya que éstas pueden conducir a limitaciones profesionales y, en consecuencia, podrían limitar el disfrute del derecho al trabajo y del derecho a la vida privada; además, las deficiencias en la educación jurídica podrían ir más allá y extenderse a terceros como podrían ser los clientes a través de juicios, consejos erróneos o mala gestión de la práctica jurídica.

Los autores consideran que para convertir los riesgos de la evolución del Derecho y de la práctica jurídica en oportunidades, existe una demanda creciente de una nueva generación de abogados con formación interdisciplinar en Derecho y Tecnología, y de profesiones híbridas de nueva generación como son los tecnólogos jurídicos y los gestores de proyectos jurídicos; por lo tanto, las cuestiones de la identificación de las lagunas en la educación jurídica actual, los métodos de infusión de los resultados relacionados con la tecnología en todo el plan de estudios, la exposición de las mejores prácticas y la arquitectura óptima de los programas de estudio de Derecho y Tecnología -entre otros- devienen en temas de necesario análisis para el futuro de la educación jurídica y de la profesión de abogado. No obstante, en opinión de los autores, dado el enfoque conservador y tradicional del Derecho, dentro de este campo de investigación faltan razonamientos jurídicos -como serían las investigaciones sistemáticas sobre el estado de los planes de estudios de Derecho y Tecnología que ofrecen las principales universidades- que respalden tales cambios.

Al mismo tiempo refieren que esto lleva a la conclusión de que viabilizar el derecho a la educación requiere hoy en día un justo equilibrio entre las materias y competencias jurídicas tradicionales y un papel adecuado de las nuevas tecnologías en la educación jurídica. De otro lado, sería difícil encontrar argumentos sólidos para un modelo de educación jurídica, y de educación en general, que excluyera completamente el cambio tecnológico y sus oportunidades de las políticas educativas y los planes de estudio; siendo así, consideran que la educación debe reflejar y reaccionar ante los avances tecnológicos no sólo en los cursos específicos de cada materia, sino también en

todos los contextos educativos, incluidos los planes de estudios jurídicos [11].

La enseñanza del Derecho enfrenta el reto de incorporar el estudio y regulación del uso de la tecnología, sin embargo, a esto se suma un componente más, que es la apuesta por las buenas prácticas; es decir, que los individuos definan y normen sus conductas sin necesidad de la tutela del Estado. En la actualidad dicha regulación se inclina por comportamientos cada vez más alejados de la tutela estatal, pero que subsisten al lado de un derecho tradicional.

### **III. LA INCURSIÓN DE LA TECNOLOGÍA EN LA FORMACIÓN ACADÉMICA Y EL DESEMPEÑO PROFESIONAL**

La irrupción de la tecnología en el Derecho se ha dado en diversos niveles y a diferentes escalas; siendo así encontramos tecnologías para el aprendizaje -si bien transversales a todas las áreas del conocimiento debido a que en cierta forma complementan las prácticas educativas tradicionales- que están diseñadas específicamente para la educación legal y permiten generar diversas habilidades y actitudes de los estudiantes ante las diferentes herramientas que permiten la manipulación tecnológica y adaptabilidad de manera gradual.

En este contexto podríamos hablar de dominios digitales generales para la educación jurídica, que van desde los más simples como el empleo de libros interactivos hasta los más complejos como el despliegue en entornos virtuales por diseño; no obstante, por la transversalidad inherente, no será abordada en el presente artículo.

En el Derecho, la tecnología puede ser empleada de diversas maneras; en su forma más elemental la digitalización automatiza procesos que antes requerían un esfuerzo humano significativo, estas soluciones ayudan a los abogados y estudiantes de derecho a realizar una determinada tarea de forma más rápida y eficiente, con mayor calidad y menos costes, en comparación con su realización manual. Existen sin embargo, otras herramientas que desafiarán y cambiarán completamente la forma en que se prestan ciertos servicios legales; no obstante, sea cual fuere la tecnología a emplear es innegable que colectivamente están transformando todo el panorama jurídico.

De otro lado, los cambios que se han producido en el campo del Derecho en los últimos años han evidenciado un alejamiento progresivo de las formas tradicionales en las que se hicieron las cosas por décadas y nos ha situado en un escenario complejo que no sólo demanda

conocimientos especializados en relación a la forma en que el derecho es respuesta para enfrentar el uso y abuso de la tecnología, sino que al mismo tiempo hace necesario conocer cuáles son aquellas tecnologías que al ser coincidentes con la detección de una necesidad específica y cuya potencialidad aparejaría una posible mejora al ser introducida en ciertos campos, se convertirían en herramientas indispensables dentro del sector legal una vez una vez que hayan sido integradas [11].

Esta realidad plantea la necesidad de analizar dos temáticas altamente diferenciadas; de un lado aquella conocida bajo diferentes nomenclaturas pero de contenido símil donde encontramos al llamado Derecho Informático, en tanto de otro lado, tenemos que la década de los 60 marco el desarrollo de varios sistemas que forjaron la entonces denominada “informática jurídica” que en términos prácticos suele definirse como una de las disciplinas de las ciencias de la información que tiene por objeto la aplicación de la informática en el Derecho; así como “LegalTech” que hace referencia al uso de tecnologías para ofrecer servicios jurídicos, siendo el enfoque más sencillo entenderlo como la interacción entre derecho y tecnología. Se trata de un concepto que hasta ahora ha sido usado de forma genérica para incluir cualquier aplicación o herramienta que se pueda implementar en el mundo jurídico.

Podría decirse que el equivalente en ese entonces del Legal Tech en algunos países fue la informática jurídica; siendo así, estaríamos ante el empleo de tecnología viabilizadora del ejercicio del derecho.

La Tecnología Legal o Legal Tech -término como se ha incorporado con fuerza en el mercado legal en los últimos años y que ha gozado de gran acogida- significa esencialmente el uso de la tecnología y el software para proporcionar ayuda en los servicios legales. Cabe señalar, sin embargo; que acorde “avanza” más esta figura en distintos escenarios -la cual aún no cuenta con un concepto único consensuado, ni con una aproximación de respaldo suficiente- se convierte en mayor o menor medida en un término *sui generis*, al devenir en el resultado de recoger temas propios de la Informática Jurídica, del Derecho Informático, la Inteligencia Artificial, la Administración y otras áreas del conocimiento.

En sentido, refiere Barrio [12] que Legal Tech - Tecnología jurídica-, es una combinación de los términos “servicios jurídicos” y “tecnología” y señala que no existe una definición universal al respecto, siendo BLUES uno de los primeros en definir el término con mayor precisión al señalar

que el Legal Tech describe el uso de tecnologías digitales modernas asistidas por ordenador, para automatizar, simplificar y con suerte, mejorar el proceso de búsqueda, aplicación, acceso y gestión de la justicia a través de la innovación.

En consideración de Barrio se pueden distinguir tres tipos de tecnología dentro de Legal Tech, las que facilitan el acceso a los datos y su tratamiento, las herramientas de apoyo y las soluciones de derecho sustantivo que ayudan o sustituyen al asesoramiento jurídico [12].

Así mismo, acorde al estadio actual de desarrollo tecnológico, debemos abordar al propio derecho como tecnología y es donde identificamos el concepto de Law Tech, que si bien se ha venido usando de forma indistinta junto Legal Tech para referirse a la implementación de la tecnología en el entorno jurídico, una de las principales características diferenciadoras de las aplicaciones Legal Tech stricto sensu es que no están diseñadas tanto para sustituir al abogado como para ayudarlo en su desempeño profesional, en tanto en consideración de algunos sectores, Law Tech serviría para denominar a aquellas herramientas que ya no sólo facilitan la función del jurista; sino que la sustituyen al tener integrado un sistema muy sofisticado de IA capaz de memorizar patrones de conducta o incluso ejecutarse de forma autónoma.

En este contexto señala June Wang que en cuanto a la naturaleza de la tecnología, es útil distinguir entre automatización (aplicaciones que nutren la tecnología) y la innovación (aplicaciones disruptivas de tecnología), ya que la automatización mejorará tanto la eficiencia como la precisión, pero la innovación presentará métodos totalmente nuevos de abogacía. Al mismo tiempo refiere que las tecnologías en la educación jurídica nos plantean tres tipos de consideraciones: la adopción y adaptación de las tecnologías a la enseñanza y el aprendizaje; el estudio e investigación de las disrupciones y otros impactos en la sociedad para ayudar a establecer nuevas leyes que las regulen; y la preparación de los futuros abogados; siendo la última la que reviste interés para los efectos del presente artículo y en torno a la cual, el autor precisa que el reto fundamental y difícil de la educación jurídica no consiste en utilizar las tecnologías en la enseñanza, el aprendizaje y la investigación, aunque éstas sean útiles; sino en preparar a los estudiantes de Derecho para la práctica futura mediante la adquisición de conocimientos y habilidades prácticas que impliquen competencias digitales [3].

Siendo así, McKamey [13] precisa que, dadas las tendencias tecnológicas, es difícil

prever otra cosa que no sea un cambio en la forma en que se prestan los servicios jurídicos.

Por su parte, Corrales, Fenwick y Haapio [14] al cuestionarse sobre qué deberán hacer los abogados, señalan que deberán adaptarse y aprovechar las nuevas oportunidades remarcando que hay tres cosas que en este momento los abogados podrían estar haciendo para agregar valor.

En primer lugar, consideran los autores que los profesionales del Derecho necesitan trabajar con las nuevas tecnologías ya que su actual cartera de clientes y los nuevos que tendrán, demandarán de ellos los conocimientos y manejo de éstas para un asesoramiento comercial y legal estratégico; si los abogados no pueden dar una respuesta satisfactoria a sus clientes, corren el riesgo de que cambien a otro bufete de abogados o consultores; en opinión de Corrales, Fenwick y Haapio ser experto en tecnología será esencial para construir y mantener la lealtad a la "marca".

En segundo lugar, los abogados deben encontrar soluciones "inteligentes" y la tecnología digital tiene el potencial de contribuir a un mundo mejor, más saludable y más seguro. Con el fin de encontrar las mejores soluciones posibles es necesario que los abogados -y otros consultores- tengan una comprensión detallada y precisa de las nuevas tecnologías que permitan la identificación de tales soluciones.

Como tercer punto, enfatizan los autores que los abogados deben aprender a trabajar junto con diseñadores y "tecnólogos" y agregan que los abogados proactivos y expertos en tecnología pueden desempeñar un papel crucial en el desarrollo de la economía digital, lo cual no significa "aplicar" pasivamente las reglas y regulaciones actuales a una nueva tecnología para restringir la innovación; sino que requiere habilidades nuevas y diferentes. Los "mejores" abogados del futuro serán aquellos que comprendan la necesidad de trabajar junto con diseñadores y tecnólogos para encontrar soluciones tecnológicas fáciles de usar y que puedan ayudar a generar confianza en la tecnología, así como cumplir con los requisitos normativos [12].

Señala O'Leary que los clientes exigen ahora un enfoque más eficiente y multidisciplinar que a menudo incluye la tecnología [4]; en tanto para Toohey [15] Los abogados y la tecnología mantienen una relación incómoda. Aunque algunos abogados se adaptan pronto, otros se enorgullecen de ignorar la tecnología

Medianik [16] por su parte anota que históricamente el concepto de competencia de los abogados se refería a una comprensión del

abogado de un área particular del derecho; sin embargo, el impacto de la tecnología en el ámbito jurídico profesional ha hecho obsoleta esta noción histórica de competencia en el operador jurídico; así mismo, refiere que el uso de la IA por parte de los abogados es inevitable debido a sus ventajas competitivas, comparativas y diferenciales, al tiempo de señalar que actualmente no existen normas uniformes diseñadas específicamente para regular el uso de la IA por parte de un abogado en su lugar de trabajo.

Brooks, Gherhes y Vorley [17] consideran que los recientes avances tecnológicos en automatización e inteligencia artificial prometen alterar los cimientos de cómo se practica y realiza el trabajo legal.

Alarie, Niblett y Yoon [18] refiere que los verdaderos beneficios de las herramientas artificialmente inteligentes en la profesión jurídica sólo podrán alcanzarse cuando los abogados reconsideren completamente la prestación de servicios legales. Por lo tanto, es esencial comprender cómo la IA y otras presiones tecnológicas se combinan con las tendencias existentes en el mercado para desafiar a las empresas de servicios legales y a las áreas de negocio en donde las IA puede potencialmente contribuir o alterar la actividad actual; en este sentido, agrega que los ALSP (Alternative legal service providers) y las estructuras empresariales alternativas son una fuente potencial de disrupción para los sistemas legales tradicionales.

Por su parte, Okereke [19] señala que ya no es una predicción que la tecnología tendrá impacto en la profesión legal, sino que es una realidad. En esta línea June Wang sostiene que la diferencia entre los que van a prosperar en la futura profesión jurídica y los que lucharán, girará en gran medida en torno a quién se adapta mejor a los cambios tecnológicos y añade que si la abogacía debe adaptarse a los cambios tecnológicos, también debe hacerlo la formación jurídica y a la inversa, ésta también determinará significativamente el futuro de la práctica jurídica [3].

Es probable que el mundo legal del futuro guarde poca semejanza con el del pasado. Las instituciones legales y los abogados tendrán que cambiar radicalmente y reinventarse para no sucumbir ante el arrollador avance tecnológico que ha incursionado en el campo del derecho, con un enfoque prometedor en opinión de algunos y amenazador en consideración de otros.

En este sentido consideramos que surgirán formas completamente nuevas de brindar

servicios legales debido a la amplia gama de tecnologías que perturbarán las prácticas laborales tradicionales de los abogados.

Para convertir los riesgos de la evolución del Derecho y de la práctica jurídica en oportunidades, será necesario una nueva generación de abogados con formación interdisciplinar en Derecho y Tecnología.

#### **IV. INTELIGENCIA ARTIFICIAL Y OTRAS TECNOLOGÍAS**

Existen diversos autores que abordan la visión tecnológica del Derecho desde distintas ópticas y analizando diversas tecnologías.

Susskind [20] afirma que hay al menos 13 tecnologías disruptivas en la ley y sostiene que individualmente, estos sistemas existentes y emergentes desafiarán y cambiarán la forma en que se prestan ciertos servicios legales y colectivamente transformarán todo el panorama legal; siendo así considera los siguientes:

- *La automatización de documentos*: Estos sistemas, generan primeros borradores de documentos relativamente pulidos y personalizados, en respuesta a los requerimientos del usuario.

- *Conectividad implacable*: Los sistemas evitan que los abogados se desvinculan por completo de sus clientes y de su lugar de trabajo.

- *Mercado legal electrónico*: Hace referencia a los sistemas de reputación en línea que permiten a los clientes compartir sus puntos de vista sobre el desempeño y los niveles de servicio de sus abogados-

- *e- Learning*: Existen progresos notables en el desarrollo de instalaciones en línea para apoyar el aprendizaje y la formación jurídica que están desafiando y reemplazando la mayoría de las conferencias de derecho convencionales y en términos más generales, precipitarán una revisión general de los métodos tradicionales de las facultades de Derecho.

- *Orientación legal en línea*: Los sistemas pueden proporcionar información, orientación e incluso asesoramiento legal en Internet; la amenaza y la interrupción para los abogados convencionales aquí es clara: si los clientes pueden obtener orientación legal y documentos legales en línea; entonces esto puede convertirse en un competidor de bajo costo para los abogados cuya vida se realiza de manera tradicional, consultiva y presencial más aún si la ayuda legal sólida y confiable se comercializa y está disponible sin costo para los usuarios.

- *Legal Open- Sourcing*: En consonancia con el movimiento de código abierto en general, el

autor prevé una colaboración masiva en línea sostenida en el campo de la ley, un movimiento dedicado a construir grandes cantidades de materiales legales públicos orientados a la comunidad, como documentos estándar, listas de verificación y diagramas de flujo.

- *Comunidades legales cerradas*: La idea central en torno a este punto es que grupos restringidos de abogados de ideas afines o con intereses comunes se unan y colaboren en línea en redes sociales privadas para que puedan construir conocimiento y compartir experiencias colectivas tendientes a generar otros conocimientos

- *Flujo de trabajo y gestión de proyectos*: Para el trabajo legal repetitivo de gran volumen, los sistemas de flujo de trabajo son como listas de verificación automatizadas que impulsan un proceso estándar de principio a fin.

De otro lado, los sistemas de gestión de proyectos se adaptan mejor a las tareas y actividades legales que son más complejas y menos estructuradas pero sin embargo aún son susceptibles de un manejo más disciplinado que la publicidad que se encuentra en muchas firmas de abogados y departamentos internos.

- *Conocimiento legal incorporado*: Susskind considera que en los años venideros las normas legales estarán profundamente arraigadas en nuestros sistemas y procesos sociales, laborales y de toda índole en relación directa a los diversos aspectos de nuestras vidas.

La interrupción aquí es que donde las reglas están integradas, los abogados ya no son necesarios para llamar la atención de los clientes sobre circunstancias de importancia legal.

- *Resolución de disputas en línea (ODR)*: Cuando el proceso para resolver una disputa legal, buscando especialmente la formulación de una solución se lleva a cabo total o mayormente a través de Internet nos encontramos ante una forma de resolución de disputas en línea.

De otro lado, McGinnis y Pearce [21] señalan que es importante reconocer dos proposiciones centrales sobre el progreso de la Inteligencia Artificial. Primero, antes de que la combinación de hardware, software y conectividad avanzaran hasta el punto en que lo han hecho, la IA no representaba un sustituto para la actividad humana; pero una vez que la inteligencia artificial alcanzó un nivel en el cual no sólo se volvió competitivo con los humanos, sino que continúa mejorando para superar las habilidades humanas; es necesario replantearse muchas cosas. En segundo lugar, debido a que los aumentos en el poder de la computación son exponenciales y no lineales, las computadoras

ahora pueden realizar tareas legales complicadas mucho más rápido de lo que inicialmente les tomó realizar las tareas más simples.

El desarrollo del campo de la IA y el Derecho comenzó con programas que analizaban casos y continuó con tecnologías que hacen que las tareas de los abogados sean eficientes, resuelvan disputas y reemplacen la intervención humana. Al examinar el curso de este desarrollo, se puede predecir que a largo plazo las tecnologías de IA que utilizan técnicas de aprendizaje automático y aprendizaje profundo podrán reemplazar a los abogados, árbitros, mediadores e incluso jueces; los sistemas informáticos podrán hacer el trabajo de un abogado: examinar un caso, analizar los problemas que le plantea, realizar investigaciones legales e incluso decidir una estrategia.

Por su parte Alarie, Niblett y Yoon se cuestionan en torno a cómo el Derecho se verá afectado por la revolución de los grandes datos y la IA y presumen que el crecimiento de Big data, Inteligencia artificial y Aprendizaje automático tendrá efectos importantes que cambiarán fundamentalmente la forma en que se hace, aprende, sigue y practica el Derecho.

Señalan los autores que los sistemas realizarán muchas de las tareas que actualmente realizan los legisladores, jueces y abogados; sin embargo, en lugar de ofrecer una visión distópica de un mundo legal manejado por máquinas, sugieren que los cambios serán principalmente beneficiosos y estos cambios estarán enfocados en la forma como se hacen las leyes, la forma en que las personas las entienden, y los cambios en la industria de los servicios legales [18].

No obstante; la IA y el uso de la tecnología dentro de la profesión legal son tópicos aún muy cuestionables por diversos sectores jurídicos.

En opinión de Nieva [22] aunque el interés por la IA ha sido fluctuante en los últimos cuarenta años, ya se había introducido en los tribunales años atrás, algunas veces de manera muy tímida y con retraso; otras, a través de un simple uso de variables estadísticas que en consideración del autor no hicieron más que desnaturalizar las potencialidades de la IA; agrega el autor que dentro de los juzgados lo habitual es ver únicamente IA en los procesadores de texto y en los buscadores de jurisprudencia; es decir la IA débil. En este sentido Nieva señala que en lo referente a la labor de los juzgados, actualmente la Inteligencia artificial se está empleando en el procedimiento, la prueba y la argumentación.

El cuanto al primer uso señala que gran parte de la labor es mecánica, más aún, considerable

parte del tiempo se invierte utilizando modelos ya existentes y modificando simplemente los datos identificatorios de la causa, el “cortar-pegar” es habitual. En la actualidad pocas sentencias se redactan completamente, por no decir ninguna. La Inteligencia artificial permite obtener mayor variedad de creación de documentos, de copias automáticas de los mismos, así como mayor capacidad de análisis. Combinadas estas tres funcionalidades la IA será increíblemente más rápida que un juez en la resolución de procedimientos previsibles, sobre todo en el análisis de la documentación. Señala el autor además que para que sea posible esto, las partes deberán realizar la interposición de la demanda y su contestación a través de una aplicación y que éste es el campo más sencillo de ingreso de la IA en el sistema de justicia.

En relación a la prueba, considerada por Nieva como el segundo uso actual, algunas herramientas ayudan a reconstruir los hechos basándose en los vestigios ya existentes que en casos anteriores fueron claves en la investigación con ellas se amplía extraordinariamente el campo de investigación, pero a la vez se concreta de una manera eficiente.

La argumentación, es el aspecto en que los resultados de la IA son más espectaculares y prometedores, a pesar de que sus detractores sostengan que argumentar en materia jurídica no es tan fácil porque requiere una importante labor de persuasión que no siempre depende de variables previsibles.

Nissan [23] refiere que desde la década de 1990, la argumentación ha sido un campo muy activo dentro de la IA y el Derecho e históricamente, no todas las técnicas computacionales para manejar la argumentación se han aplicado necesariamente a argumentos legales.

Por su parte Oskamp y Lodder precisan que la investigación dentro del campo de la Inteligencia Artificial está dirigida a usar la Tecnología de la Información para realizar tareas que de otro modo requerirían inteligencia humana. La inteligencia humana no necesariamente se copia exactamente, sino que simplemente se puede simular. No importa cómo un computador realice la tarea, siempre que el resultado final sea comparable o mejor que cuando un ser humano hubiera realizado la tarea.

Al mismo tiempo los autores [1] señalan que la investigación sobre IA se divide en varios subdominios y agregan que desde una perspectiva de investigación, IA y Derecho es casi sinónimo de lo que se llamaba "Tecnología de la información para abogados" y que la

investigación dentro de ésta área es, en gran parte, dirigida hacia el modelado del razonamiento legal y la toma de decisiones legales. Agregan además que el razonamiento legal difiere de otras formas de razonamiento y recientemente en lo que podría llamarse apropiadamente la "Era de la Convergencia", se han desarrollado técnicas para integrar la predicción y la argumentación, con programas capaces de explicar las predicciones y de presentar argumentos legales razonables.

En este contexto, Ashley [24] anota que a diferencia de los sistemas expertos, los dos paradigmas alternativos, el de recuperación de argumentos y el de la computación cognitiva, no apuntan a resolver por sí mismos los problemas legales de los usuarios, sino que ellos extraen la información semántica de los textos jurídicos y la emplean para ayudar a las personas a que resuelvan sus problemas legales y precisa el autor que la recuperación de información conceptual tampoco es nueva y citando a McCarty, indica que éste caracterizó a la argumentación jurídica sobre el significado de un concepto jurídico, como un tipo de construcción teórica.

### Consideraciones Finales

Es indiscutible que en el inconsciente colectivo se ha arraigado e impera el modelo de abogacía dominante actual; en este contexto la renuencia al cambio además de ser fuerte implica la adopción de diversas posturas a la defensiva o en algunos casos hasta despectivas frente a planteamientos que sugieren una nueva forma de ver y hacer el derecho en relación directa con la tecnología como aliada, escenario para el cual los abogados de larga trayectoria nunca fueron preparados.

El futuro de la abogacía exige repensar la forma y el contenido de la formación jurídica ya que se requerirá de abogados con múltiples habilidades y destrezas en el uso de las diferentes herramientas tecnológicas, al tiempo que estos abogados serán más fácilmente identificables en la medida que los análisis legales podrán monitorear su tasa de éxito. No obstante; hay algunas áreas dentro del campo del derecho en las cuales la incursión tomará un tiempo por lo que se necesitarán abogados en esas áreas especializadas.

El impacto es impredecible, pero sin duda significativo, que las nuevas tecnologías tendrán en el Derecho y la sociedad plantea la cuestión de hasta qué punto las instituciones de enseñanza superior tienen la obligación incorporar competencias digitales y cursos cuyo contenido aborde las nuevas tecnologías en sus planes de estudio.

Debe tenerse presente que no se trata de enseñar a los estudiantes de Derecho a ser expertos tecnológicos sino enseñarles a comprender los principios subyacentes a las tecnologías en el marco de una amplia formación en ciencias sociales, al tiempo dotarlos de diversas habilidades prácticas, incluida la competencia tecnológica.

El rol de las tecnologías en la educación está predeterminado por el alcance del desarrollo tecnológico, que de ser en su momento una especialización se convirtió en una condición indispensable en el devenir de la vida cotidiana. Teniendo esto en cuenta, la transformación de los mercados laborales en el futuro requiere una cuidadosa consideración a la hora de diseñar los programas de estudio y el Derecho no es ajeno a esto.

Las tecnologías emergentes desempeñan un papel cada vez más importante y fomentan el debate sobre las repercusiones e implicaciones tecnológicas en el futuro de la vida y el trabajo de los seres humanos; aunque no se sabe aún con certeza si muchos de los ambiciosos objetivos que se pronostican hoy en día se harán realidad gracias a las tecnologías emergentes, no se puede ignorar el cambio tecnológico

Los abogados no sólo deben ser capaces de adaptarse a la evolución de la tecnología y la innovación, sino que también comprender las cuestiones jurídicas y éticas que plantea el uso de las tecnologías modernas.

Los estudios jurídicos deben paulatinamente abandonar el conservadurismo arraigado y ser capaces de adaptarse a las innovaciones tecnológicas a efecto de volverse más competitivos y eficientes.

### V. REFERENCIAS

- [1] A. Oskamp y A. Lodder. "Introduction: Law, Information Technology, and Artificial Intelligence" en *Information Technology and Lawyers: Advanced Technology in the Legal Domain, from Challenges to Daily Routine*, A. Lodder y A. Oskamp, Eds. Países Bajos Springer, 2006, pp. 1-22 [En línea]. Disponible en: [https://link.springer.com/chapter/10.1007/1-4020-4146-2\\_1](https://link.springer.com/chapter/10.1007/1-4020-4146-2_1) [Accedido: 28 – noviembre – 2023]
- [2] C. Vargas Vasserot. "Metodología activas en la enseñanza del derecho: prueba, ensayo y percepción por parte de los alumnos", 2011, pp. 1-137, [En línea]. Disponible en: <https://core.ac.uk/download/pdf/143456169.pdf>
- [3] Z. June Wang. "Between Constancy and Change: Legal Practice and Legal Education in the Age of Technology". *Law in context*, Vol. 36, (issue 1), 2019, pp. 64-79 [En línea]. Disponible en:

[https://www.researchgate.net/publication/336454057\\_Between\\_Constancy\\_and\\_Change\\_Legal\\_Practice\\_and\\_Legal\\_Education\\_in\\_the\\_Age\\_of\\_Technology](https://www.researchgate.net/publication/336454057_Between_Constancy_and_Change_Legal_Practice_and_Legal_Education_in_the_Age_of_Technology)  
[Accedido: 30 – noviembre – 2023]

[4] D. O'Leary. ““Smart” Lawyering: Integrating Technology Competence into the Legal Practice Curriculum”. 19 *U.N.H. L. Rev. Vol. 19, (issue 2)*, 2021, pp. 196-272. [En línea]. Disponible en: [https://scholars.unh.edu/cgi/viewcontent.cgi?article=1403&context=unh\\_lr](https://scholars.unh.edu/cgi/viewcontent.cgi?article=1403&context=unh_lr) [Accedido: 30 – noviembre – 2023]

[5] S. Mironova, T. Bogdanova y S. Simonova. (2019). “The introduction of digital technologies in the educational process of training lawyers”. SHS Web of Conferences. 69. 00079. CILDIAH-2019. Disponible en: [https://www.researchgate.net/publication/336805595\\_The\\_introduction\\_of\\_digital\\_technologies\\_in\\_the\\_educational\\_process\\_of\\_training\\_lawyers](https://www.researchgate.net/publication/336805595_The_introduction_of_digital_technologies_in_the_educational_process_of_training_lawyers)

[6] D. Díaz, y E. Loyola. “Competencias digitales en el contexto COVID 19: Una mirada desde la educación”. *Revista Innova Educación, Vol. 3 (número 1)*, 2021, pp. 120-150. [En línea]. Disponible en: <https://revistainnovaeducacion.com/index.php/rie/article/view/181/212>

[7] M. Arias, T. Torres y J. Yáñez. “El desarrollo de competencias digitales en la educación superior”. *Historia y Comunicación Social, Vol. 19 N° Esp. Enero*, 2014, pp. 355-366. [En línea]. Disponible en: <https://revistas.ucm.es/index.php/HICS/article/view/44963/42340>

[8] K. Galloway. “A Rationale and Framework for Digital Literacies in Legal Education”. *Legal Education Review, Vol. 7 (issue 1)*, 2017, pp.1-26. [En línea]. Disponible en: <http://www5.austlii.edu.au/au/journals/LegEdRev/2017/7.pdf> [Accedido: 4 – diciembre – 2023]

[9] Ministerio de justicia gobierno de España y Centro de estudios jurídicos. “Marco de Competencias Digitales para la formación del personal de Justicia”, 2023, pp. 1-80. [En línea]. Disponible en: [https://www.cej-mjusticia.es/sites/default/files/adjuntos/noticias/Marco%20de%20Competencias%20Digitales\\_v3.pdf](https://www.cej-mjusticia.es/sites/default/files/adjuntos/noticias/Marco%20de%20Competencias%20Digitales_v3.pdf) [Accedido: 3 – diciembre – 2023]

[10] C. Grosso. “Abogacía 4.0 y justicia predictiva” en *Inteligencia Artificial y Derecho, un reto social*, H. Granero, Ed.: UCA, 2020, pp. 13-22.

[11] A. Pasvenskienė y P. Astromskis, “Future of Legal Education: do Law Schools have the Right to be Conservative?”. The introduction of digital technologies in the educational process of training lawyers. SHS Web of Conferences. 69. 00079. [En línea]. Disponible en: [https://www.researchgate.net/publication/349258367\\_The\\_Future\\_of\\_Legal\\_Education\\_Do\\_Law\\_Schools\\_Have\\_the\\_Right\\_to\\_Be\\_Conservative](https://www.researchgate.net/publication/349258367_The_Future_of_Legal_Education_Do_Law_Schools_Have_the_Right_to_Be_Conservative)

[12] M. Barrio. “Legal Tech y la Transformación del Sector Legal”. *Legal Tech: La transformación digital de la abogacía*, M. Barrio, Ed. Wolters Kluwer, 2019, pp. 37-70.

[13] M. McKamey. “Legal Technology: Artificial Intelligence and the Future of the Law Practice (December 6, 2016). APPEAL Review of Current Law and Law Reform – 2017, 22 Appeal 45. [En línea]. Disponible en: SSRN: <https://ssrn.com/abstract=3014408> [Accedido: 7 – diciembre – 2023]

[14] M. Corrales, M. Fenwick y H. Haapio. “Digital Technologies, Legal Design and the Future of the Legal Profession”. *Legal Tech, Smart Contracts and Blockchain*. M. Corrales, M. Fenwick y H. Haapio, Eds. Singapur: Springer, 2019, pp. 1-15. [En línea]. Disponible en: [https://www.researchgate.net/publication/330939617\\_Digital\\_Technologies\\_Legal\\_Design\\_and\\_the\\_Future\\_of\\_the\\_Legal\\_Profession](https://www.researchgate.net/publication/330939617_Digital_Technologies_Legal_Design_and_the_Future_of_the_Legal_Profession) [Accedido: 8 – diciembre – 2023]

[15] T. Toohey. “Beyond Technophobia: Lawyers’ Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks”, *RICH. J.L. & TECH, Vol. 21 (issue 3)*, Rich. J.L. & Tech 9, pp.1-47, 2015. [En línea]. Disponible en: <https://scholarship.richmond.edu/jolt/vol21/iss3/4> [Accedido: 10 – diciembre – 2023]

[16] K. Medianik. “Artificially intelligent lawyers: updating the model rules of professional conduct in accordance with the new technological era”. pp. 1407-1530. [En línea]. Disponible en: <https://cardozolawreview.com/wp-content/uploads/2018/07/MEDIANIK.39.4.pdf> [Accedido: 10 – diciembre – 2023]

[17] Ch. Brooks, C. Gherhes y T. Vorley. “Artificial intelligence in the legal sector: pressures and challenges of transformation”. *Cambridge Journal of Regions, Economy and Society*, pp. 1-18, 2019. [En línea]. Disponible en: [https://www.researchgate.net/publication/338163462\\_Artificial\\_intelligence\\_in\\_the\\_legal\\_sector\\_pressures\\_and\\_challenges\\_of\\_transformation](https://www.researchgate.net/publication/338163462_Artificial_intelligence_in_the_legal_sector_pressures_and_challenges_of_transformation)

[18] B. Alarie, A. Niblett y A. Yoon. “Law in the Future”, pp. 1-6, 2016. [En línea]. Disponible en: SSRN: <https://ssrn.com/abstract=2787473> or <http://dx.doi.org/10.2139/ssrn.2787473>

[19] W. Okereke. “E-Lawyering and Virtual Law Practice: A Paradigm Shift for Law Library System”. *Library Philosophy and Practice (e-journal)*, University of Nebraska, pp. 1-17, 2019. [En línea]. Disponible en: [https://www.researchgate.net/publication/335856918\\_E-Lawyering\\_and\\_Virtual\\_Law\\_Practice\\_A\\_Paradigm\\_Shift\\_for\\_Law\\_Library\\_System](https://www.researchgate.net/publication/335856918_E-Lawyering_and_Virtual_Law_Practice_A_Paradigm_Shift_for_Law_Library_System)

[20] R. Susskind. “Tomorrow’s Lawyers: An Introduction to Your Future” (2a ed.). Oxford: Oxford University Press 2017.



[21] J. McGinnis, y R. Pearce. “The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services”. *Fordham Law Review*, Vol 82 (issue 6), 2014, pp. 3041-3066. [En línea]. Disponible en: <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5007&context=flr> [Accedido: 12 – diciembre – 2023]

[22] J. Nieva. “Inteligencia artificial y proceso judicial”. Marcial Pons, 2018.

[23] E. Nissan, E. “Legal Evidence, Police Intelligence, Crime Analysis or Detection, Forensic Testing, and Argumentation: An Overview of Computer Tools or Techniques”. *International Journal of Law and Information Technology*, Vol 17 (issue1), pp.1-82, 2008.

[24] K.Ashley.” Inteligencia artificial y analítica” Yachay legal, 2023

# Modelo Híbrido de dos niveles para la detección de anomalías con técnicas de Machine Learning en redes IoT

Sebastian Berrios, *Member, Pontificia Universidad Católica de Valparaíso*,  
Pamela Hermosilla, *Member, Pontificia Universidad Católica de Valparaíso*,  
Herminia Beatriz Parra, *Member, Universidad Católica de Salta*,  
Pablo Oñate, *Student, Pontificia Universidad Católica de Valparaíso*.

**Abstract**— La expansión de las redes IoT es una realidad continua, ya que el número de dispositivos conectados a Internet supera a la población mundial. Si bien esto representa un progreso social significativo, también introduce amenazas cibernéticas que pueden afectar la vida diaria de las personas. En respuesta, este estudio tiene como objetivo desarrollar un Sistema de Detección de Intrusos (IDS) utilizando técnicas de aprendizaje automático (ML) para identificar posibles ciberataques en redes IoT. Estas técnicas son expertas en discernir de forma automática y precisa las diferencias clave entre los datos normales y anormales, y su alta generalización les permite detectar ataques previamente desconocidos. Esta investigación incluye un examen de los sistemas IoT y sus protocolos de comunicación, las diversas amenazas a las que se enfrentan, y proporciona una taxonomía de IDS, que describe los métodos de detección y las técnicas de ML más utilizadas. Se propone un modelo de entrenamiento que incorpora diversas técnicas de ML y Deep Learning (DL), que permite evaluar su eficacia en función de los diferentes tipos de anomalías que deben detectarse.

**Index Terms**—IoT; Ciberataques; Machine Learning; Sistemas de Detección de Intrusos.

## I. INTRODUCCIÓN

El uso de redes de internet de las cosas (IoT) crece exponencialmente, siendo cada vez más los dispositivos conectados a internet. El termino IoT hace referencia a los sistemas físicos que reciben y transfieren datos a través de redes inalámbricas con poca intervención humana y esto se debe gracias a la integración de dispositivos informáticos en todo tipo de equipos [1]. El crecimiento de las redes IoT ha conllevado a que sean objetivos de atacantes para que les realicen actividades maliciosas. Los efectos de los ataques cibernéticos se vuelven más destructivos como resultado de que muchas instituciones han experimentado la interrupción de los servicios luego de estos ataques. Debido a esto, se concluye que los dispositivos IoT requerían en estos casos una herramienta más sofisticada para identificar la actividad maliciosa en la infraestructura inteligente. Estos sistemas se conocen como SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS). La complejidad utilizada por los atacantes y el aumento de los ataques de día cero (es un ataque que tiene como objetivo la

ejecución de código malicioso explotando vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto) indican que un IDS basado en anomalías es considerado adecuado para el entorno actual en sistemas IoT, en particular se considera prometedor el uso de herramientas de entrenamiento como la inteligencia artificial [2].

Esta investigación propone un IDS basado en diversas técnicas ML que utiliza un enfoque de selección de características y un clasificador de votos que es un método de conjunto de clasificadores. El marco de detección del IDS basado en ML propuesto, consta de cuatro fases que son: preprocesamiento del conjunto de datos, reducción de la dimensionalidad, entrenamiento de los clasificadores, por último, un reconocimiento de los ataques detectados. Esta publicación surge del trabajo de Tesis de Magister elaborado por Pablo Oñate de la Pontificia Universidad Católica de Valparaíso (PUCV), la cual se encuentra publicada en el repositorio institucional de dicha institución.

En la sección 2 de este artículo, se muestran aspectos metodológicos y características de la problemática de estudio. En la sección 3 se desarrolla el estado del arte, con la inclusión de los documentos más destacados de la revisión bibliográfica que se realizó. En la sección 4 se aborda el marco teórico, desarrollando un análisis exhaustivo de los sistemas de redes IoT. Este análisis abarcará una variedad de aspectos claves, incluyendo los diferentes tipos de redes, las arquitecturas predominantes, los protocolos de comunicación esenciales y las diversas áreas de aplicación de IoT. Posteriormente, en la sección 5 la atención se centrará en la identificación y definición de las amenazas de seguridad, específicamente en una arquitectura IoT de cuatro capas. Esto incluirá el desarrollo de una taxonomía detallada de los Sistemas de Detección de Intrusos (IDS) existentes, así como una clasificación de las técnicas de inteligencia artificial aplicadas en estos sistemas, con especial énfasis en el Aprendizaje Automático (ML). Además, se proporcionará una descripción detallada de los diversos tipos de datasets disponibles hasta la fecha en el ámbito de las redes IoT. En la sección 6, se presentará una solución propuesta, delineando un modelo innovador diseñado para abordar los desafíos identificados en este campo,

mostrando además los resultados logrados para un caso ejemplo. Se finaliza con la sección 7 en el que se destacan las conclusiones de la investigación.

## II. ASPECTOS METODOLÓGICOS Y CARACTERÍSTICAS DE LA PROBLEMÁTICA DE ESTUDIO

Antes de abordar la investigación a pleno, es conveniente describir las cuestiones metodológicas y resumir la problemática de estudio.

### A. Aspectos Metodológicos

El propósito de este proyecto es desarrollar un modelo para el entrenamiento de un sistema de detección de intrusos (IDS) en el contexto de las redes IoT, con el objetivo de lograr una alta precisión en la detección de ataques. Se emplearán diversas técnicas de inteligencia artificial, específicamente en el ámbito del Machine Learning (ML), para mejorar la detección en las redes IoT.

La primera fase se centrará en una revisión exhaustiva de la literatura y el estado del arte en sistemas IoT, amenazas ciberseguridad, técnicas de ML utilizadas en el área y estudios previos sobre IDS en redes IoT. Esto proporcionará una comprensión integral de los desafíos asociados con las amenazas cibernéticas en redes IoT y culminará en la propuesta de un modelo de entrenamiento.

Durante la fase de desarrollo, se seleccionarán los datasets apropiados, se definirá la técnica de preprocesamiento de datos y se escogerá un método de reducción de características. Se construirá el modelo propuesto, probando diferentes técnicas de ML, y se llevarán a cabo pruebas con los datasets tanto individualmente como en conjunto, creando un nuevo dataset combinado.

En la fase experimental, se evaluarán las técnicas de ML para determinar cuáles se ajustan mejor al problema. Se realizarán diversas pruebas para ajustar parámetros, como la proporción de datos utilizados para el entrenamiento y para las pruebas, y se podrán realizar ajustes al modelo basándose en los resultados obtenidos. Se harán comparaciones con estudios previos similares para establecer estándares de calidad mínimos para la propuesta.

Finalmente, en la fase de resultados, se analizarán en detalle los experimentos realizados. Este análisis permitirá extraer conclusiones sobre la eficacia del modelo propuesto, evaluar cuáles técnicas de ML son más efectivas en situaciones de clasificación binaria (tráfico anómalo o normal), y determinar qué técnicas de ML se adaptan mejor a los desafíos específicos del proyecto.

### B. Problemática de Estudio

Los rápidos avances tecnológicos han permitido que existan más de 25 billones de dispositivos conectados alrededor de todo el mundo al internet, llegando a ser tres veces mayor a la población mundial [3]. El internet de las cosas (IoT) ha proporcionado un cambio a la sociedad, alcanzando nuevas capacidades y servicios a las personas, ha permitido hacer realidad ciudades inteligentes, hogares inteligentes, sistemas de transportes inteligentes, abriendo un mundo de oportunidades y funcionalidades para el bien o comodidad de las personas. Los

sistemas IoT actuales son vulnerables a la mayoría de las ciberamenazas, debido a que muchos fabricantes de dispositivos IoT priorizan las funcionalidades técnicas y de bajo costo sobre mecanismos de seguridad [4]. En el 2021, los ataques a dispositivos IoT han incrementado un 1.080 % [5], siendo relevante encontrar estrategias que permitan el análisis del tráfico en sistemas IoT para la detección temprana de estas posibles amenazas utilizando ML. A continuación, se detallarán diferentes conceptos para comprender en plenitud la magnitud y la cobertura del problema. Por tanto, se detallará el entorno de sistemas IoT, los tipos de ciberataques, los sistemas de detección de intrusos (IDS) y técnicas de ML.

## III. ESTADO DEL ARTE

El estudio de la problemática que se describe en este trabajo se abordó desde diferentes puntos o palabras claves, que permitieron hacer una revisión bibliográfica inicial. Aún cuando las secciones que siguen cuentan con la referenciación bibliográfica específica en cada apartado, es conveniente resumir el estado del arte considerando las investigaciones del del período 2019-2023.

Respecto de las cuestiones de ciberseguridad vinculadas a entorno IoT, se tomó en consideración los aportes de [6] en cuanto a la revisión de las amenazas aplicadas a IoT y el aporte de las tecnologías emergentes como Blockchain, Computación en la Niebla (Fog Computing), Computación en el Borde (Edge Computing) y Aprendizaje Automático para mejorar el nivel de seguridad de los entornos IoT. Por otro lado, de la investigación [7] se toma en consideración los aportes referidos a la aplicación de Machine Learning y Deep Learning para colaborar en la identificación de ciberataques dirigidos a los dispositivos IoT. La propuesta de [8] resulta también de interés para el presente trabajo porque plantea estrategias para la identificación de ataques a sistemas ciberfísicos. Por parte, Keshk et al. [9] define un marco de acción para minimizar los riesgos de acceso a datos privados en contextos en los que se utilizan redes eléctricas inteligentes y en [10] el mismo equipo de investigadores aborda las cuestiones de seguridad en los espacios ciberfísicos desde la Ciencia de Datos. En [11] se estudian las posibles soluciones para asegurar la capa de final del sistema IoT (nodo de borde y dispositivo final), considerando especialmente los microcontroladores. En el artículo [12] se propone un sistema de seguridad para entornos IoT que actúa desde la computación en la niebla y aprovecha otros recursos como las VPN para asegurar el canal de acceso a los dispositivos IoT. La investigación [13] es sumamente interesante, basada en una encuesta de datos destacados, los autores desarrollan una taxonomía de amenazas de red y las características principales de cada tipo de ataque.

Entre las investigaciones que recurren a la aplicación de la inteligencia artificial para desarrollar sistemas de detección más confiables, se destacan los siguientes trabajos: el [14] analiza en profundidad la problemática de ataques en la computación en la niebla, y propone un sistema de detección de intrusiones basado en la inteligencia artificial; la investigación [15] propone un modelo de detección de anomalías en la red, definiendo algunas métricas de evaluación (precisión, tasa de

detección, falsos positivo y Fi-Score) recurriendo a técnicas de Deep Learning; el trabajo [16] describen la problemática propia de los algoritmos de Machine Learning y Deep Learning, y presentan una mejora al rendimiento de estos algoritmos mediante la implementación de técnicas de selección, aprendizaje datasets y voting que se aplican sobre datasets preprocesados; y esta misma línea se abordan métricas de evaluación en la investigación [17].

Por último, los trabajos [18] y [19] nos permitieron abordar con más sustento la elección de los datasets así como las técnicas a utilizar para el análisis de los resultados obtenidos.

#### IV. MARCO TEÓRICO

A continuación, se realizará un estudio sobre los diferentes entornos que existen en sistemas IoT, también las posibles amenazas en estos entornos. Se explicarán los IDS que se usan para detectar estas amenazas en la actualidad, así como las técnicas de ML utilizadas para desarrollar IDS. Por último, se realiza una comparación de diversos estudios actuales referentes a IDS creados con diferentes técnicas y su rendimiento.

Con su creciente aplicación en campos tan diversos como lo militar, la agricultura, los sistemas de energía, la educación y el comercio, han fomentado la emergencia de una amplia gama de dispositivos y la adopción de múltiples estándares de comunicación y protocolos. Esta diversidad se refleja también en la arquitectura de las redes IoT, que se ha adaptado para soportar una variedad de necesidades y especificaciones. Las arquitecturas de IoT, comúnmente estructuradas en múltiples capas, se diseñan para gestionar eficientemente la interconexión de estos dispositivos variados, asegurando la comunicación fluida y la integración de datos.

Se presentan los principales aspectos de los tipos de redes y arquitecturas asociadas a los sistemas IoT.

##### A. Tipos de redes

Una red informática se crea cuando dos o más computadoras (o dispositivos) están conectadas para compartir datos y/o recursos. Se estudiarán los diferentes tipos de redes que se pueden encontrar en sistemas IoT, las cuales, se diferencian en base a la distancia y el propósito de su uso.

- Red de área Personal (PAN): Estas redes suelen ser inalámbricas, se establecen bajo demanda o ad-hoc cuando se necesitan para comunicarse entre dos o más dispositivos. Las redes PAN se utilizan entre dispositivos propietarios de dos partes diferentes, o entre dos dispositivos propietarios de una persona, como una PDA y una computadora portátil o un teléfono móvil. Estas redes generalmente se caracterizan como de corto alcance, a menudo limitadas a 10 metros o menos [20, 21].
- Red de área Local (LAN): Una LAN conecta dispositivos de red en una distancia relativamente corta. Un edificio de oficinas, una escuela o un hogar en red generalmente contiene una sola LAN, aunque a veces un edificio contendrá algunas LAN pequeñas) y ocasionalmente una LAN abarcará un grupo de edificios cercanos. Sin embargo, se diferencia de la PAN por su amplio rango de

comunicación y la mayor cantidad de dispositivos que pueden estar conectados [20, 21].

- Red de área Amplia (WAM): Este tipo de red conecta varios dispositivos que se ubican a largas distancias. Así pueden comunicarse de manera remota sin importar qué tan lejos se encuentren. El ejemplo más común este tipo de es la Internet, que conecta millones de dispositivos alrededor del mundo. Por eso, debido a su amplio alcance, la gestión de este tipo de red informática es pública y les corresponde a diversos administradores [20, 21].
- Red de área Metropolitana (MAN): El término Red de área metropolitana (MAN) se usa típicamente para describir una red que abarca un área de toda la ciudad o un pueblo. Las MAN son más grandes que las LAN tradicionales y utilizan predominantemente medios de alta velocidad, como cable de fibra óptica, para sus redes troncales. Los MAN son comunes en organizaciones que necesitan conectar varias instalaciones más pequeñas para compartir información [20, 21].
- Red de área Local Inalámbrica (WLAN): Las redes de área local inalámbricas son muy parecidas a las redes LAN, excepto que no requieren cables de red para conectarse entre sí. Las señales de radio e infrarrojas se usan para la comunicación entre máquinas mientras se utiliza una red de área local inalámbrica. Las redes de área local inalámbricas permiten la movilidad de los dispositivos mientras están conectados a la red. Estas redes utilizan el estándar IEEE 802.11 [20, 21].
- Red de área de Campus (CAN): Las redes de área de campus suelen ser una conexión de muchas redes LAN pequeñas que se utilizan a menudo en campus universitarios y edificios de oficinas. Las redes de área de campus permiten compartir archivos fácilmente entre diferentes departamentos, ya que todos los archivos generalmente se comparten en las máquinas servidor de cada red LAN. Este tipo de red ofrece mucha sencillez en la transferencia y descarga de archivos [20, 21].
- Red de área de Almacenamiento (SAN): Las redes de área de almacenamiento se utilizan principalmente como bases de datos de información. Se utilizan específicamente para el almacenamiento de información y la fácil recuperación de datos específicos cuando sea necesario. Las redes de área de almacenamiento suelen ser utilizadas por sitios web que ofrecen servicios de descarga [20, 21].
- Red de área del Sistema (SAN): Estas son redes orientadas a la velocidad que proporcionan conexiones de Internet de alta velocidad a un grupo de dispositivos. Estos se utilizan principalmente para fines de servidor y permiten que otras computadoras se conecten a estas redes de área del sistema [20, 21].
- Red Privada Virtual (VPN): Una red privada virtual (VPN) es una red de comunicación virtual que utiliza la infraestructura de una red física para asociar sistemas informáticos de manera lógica. En este sentido, se puede tratar de todos los tipos de redes expuestos anteriormente. Lo más común es utilizar Internet como medio de transporte, ya que este permite establecer la conexión entre todos los ordenadores a nivel mundial y, al contrario de lo que ocurre con las redes MAN o WAN privadas, está disponible de forma gratuita. La transferencia de datos

tiene lugar dentro de un túnel virtual erigido entre un cliente VPN y un servidor VPN [20, 21].

### B. Arquitectura IoT

Una arquitectura IoT se compone de objetos físicos integrados en una red de comunicación y respaldados por equipos informáticos para brindar servicios inteligentes a los usuarios. El sistema IoT debería ser capaz de conectar miles de millones de dispositivos heterogéneos a través de Internet, por lo que se necesita una arquitectura flexible y en capas. Existen numerosas arquitecturas y modelos de referencia propuestos por varios autores y organizaciones, pero aún no se ha consensado en un modelo de referencia formalmente reconocido [22,23]. Las arquitecturas y modelos de referencia más comunes se explican a continuación.

La arquitectura de 3 capas es el modelo más común y básico que comprende las capas de percepción, red y aplicación. La capa de percepción también se denomina “capa de dispositivo” e incluye dispositivos físicos y sensores. La capa de red también se denomina “capa de transmisión”, que debe transmitir de forma segura los datos de telemetría de los sensores a los sistemas de procesamiento y análisis de datos.

La arquitectura de 4 capas es una aplicación de IoT en la que se identifican cuatro capas: (1) capa de detección; (2) capa de red; (3) capa de software intermedio; y (4) capa de aplicación, como se observa en la Figura 1. Cada una de estas capas en una aplicación de IoT utiliza diversas tecnologías que generan una serie de problemas y amenazas de seguridad. Esta arquitectura se diferencia de las de tres capas, por la capa intermedia que permite la conexión entre la capa de red y la capa de aplicación [6]. La capa de aplicación ofrece una gestión global de las aplicaciones utilizando los sistemas de la capa de red [6].

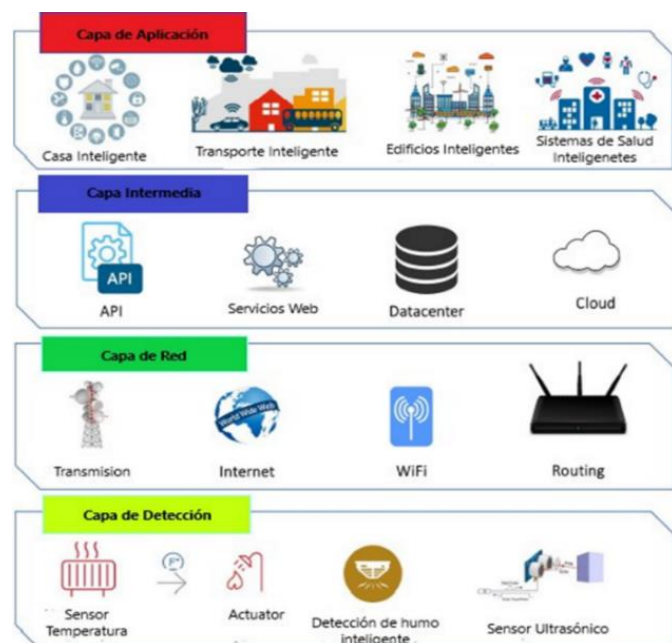


Figura 1: Arquitectura de 4 Capas.

## V. AMENAZAS DE SEGURIDAD EN LAS ARQUITECTURAS IoT

En la sección anterior, se definieron diversas arquitecturas en sistemas IoT, a partir de esto utilizaremos la arquitectura de

4 capas para la división de los posibles ataques en redes IoT como se observa en la Figura 2.

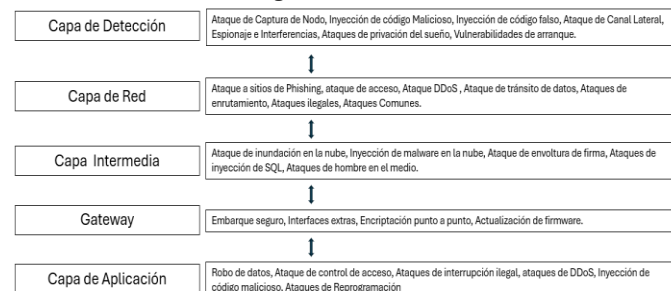


Figura 2: Tipos de Ataques a IoT organizados por la capa afectada [11].

Cada una de las capas utiliza diversos tipos de tecnologías que causan una serie de problemas y amenazas de seguridad. También se agrega el gateway (puerta de enlace), que no es un tipo de capa, pero es un intermediario entre los dispositivos o servicios entre las capas intermedia y la capa de aplicación.

En esta sección se realizará un análisis de las posibles amenazas de las aplicaciones IoT para la arquitectura de 4 capas anteriormente mencionadas.

### A. Amenazas en la capa de Detección

La capa de detección se ocupa principalmente de sensores y actuadores físicos de IoT. Los sensores detectan el fenómeno físico que ocurre a su alrededor y los actuadores realizan una determinada acción en el entorno físico, en función de los datos detectados. Existen una gran diversidad de sensores para detectar diferentes tipos de datos que va desde sensores de cámara hasta sensores de humedad, entre otros, por tanto, se usan diferentes tipos de protocolos como son RFID, GPS, WSN, etc.

En la capa de detección de IoT, se enfrentan varios riesgos de seguridad [6,11], exacerbados por la variedad de dispositivos y protocolos que se utilizan. De la investigación [6] se toman los principales riesgos:

- **Captura de Nodos:** Vulnerabilidad de nodos de baja potencia a ser sustituidos por nodos maliciosos, comprometiendo el sistema IoT. Las aplicaciones IoT se componen de varios nodos de baja potencia, como sensores y actuadores. Estos nodos son vulnerables a una diversidad de ataques, los atacantes pueden intentar capturar o reemplazar el nodo en el sistema IoT por un nodo malicioso. En nuevo nodo puede aparecer como parte del sistema, pero está controlado por el atacante, comprometiendo al sistema completo [6,11].
- **Inyección de Código Malicioso:** Posibilidad de inyectar código dañino en nodos IoT durante actualizaciones de software, facilitando funciones o accesos no autorizados. El ataque involucra al atacante inyectando algún código malicioso en la memoria del nodo. Por lo general, el firmware o el software de los nodos de IoT se actualizan por medio de tecnologías inalámbricas y esto brinda una puerta de entrada a los atacantes para inyectar código malicioso. Esto puede obligar a los nodos a realizar algunas funciones no deseadas o incluso pueden intentar acceder al sistema IoT completo [6].

- **Inyección de Datos Falsos:** Uso de nodos comprometidos para introducir datos incorrectos, causando mal funcionamiento o facilitando ataques DDoS. Una vez que se capturó el nodo, el atacante puede usarlo para inyectar datos erróneos en el sistema IoT. Esto puede dar lugar a resultados falsos y provocar un mal funcionamiento de la aplicación IoT. También se puede utilizar este método para provocar un ataque DDoS, DISTRIBUTED DENIAL OF SERVICE (Denegación de Servicio Distribuido). En un ataque DDoS, múltiples sistemas informáticos comprometidos atacan un objetivo, como un servidor, un sitio web u otro recurso de red, y provocan una denegación de servicio para los usuarios del recurso objetivo [6].
- **Ataques de Canal Lateral (SCA):** Explotación de características como la microarquitectura de procesadores para obtener datos confidenciales, aunque los chips modernos implementan varias contramedidas. Los ataques de canal lateral pueden provocar la filtración de datos confidenciales. Las microarquitecturas de los procesadores, la emanación electromagnética y su consumo de energía revelan información confidencial a los adversarios. Los ataques de canal lateral pueden basarse en consumo de energía, ataques de sincronización o de electromagnéticos. Los chips modernos tienen varias contramedidas para evitar estos ataques de canal lateral mientras implementan los módulos criptográficos [6].
- **Espionaje e Interferencias:** Riesgo de espionaje y captura de datos en nodos IoT desplegados en entornos abiertos, particularmente durante la transmisión de datos o la autenticación. Las aplicaciones IoT a menudo consisten en varios nodos implementados en entornos abiertos, dando como resultado que estén expuestas a los atacantes en cualquiera de las fases de trabajo, como la de transmisión de datos o la de autenticación [6].
- **Ataques de Privación del Sueño:** Estrategias para agotar la batería de dispositivos IoT de baja potencia, conduciendo a una denegación de servicio. En este tipo de ataques, se intenta agotar la batería de los dispositivos periféricos IoT de baja potencia. Esto conduce a una denegación del servicio de los nodos en la aplicación IoT debido a una batería descargada. Esto se puede realizar ejecutando bucles infinitos en los dispositivos perimetrales mediante un código malicioso o aumentando artificialmente el consumo de la energía [6].
- **Ataques de Arranque:** Vulnerabilidades durante el proceso de arranque de dispositivos periféricos, un momento crítico cuando los procesos de seguridad aún no están activos. Los dispositivos perimetrales son vulnerables a varios ataques durante el proceso de arranque. Esto se debe a que los procesos de seguridad incorporados no están habilitados en ese momento. Los atacantes pueden aprovechar esta vulnerabilidad e intentar atacar los dispositivos del nodo cuando se reinician. Es importante tomar las precauciones dado que muchos dispositivos suelen tener poca potencia y, en ocasiones, pasan por ciclos de sueño y vigilia, es esencial asegurar el proceso de arranque en estos [6].

## B. Sistema de Detección de Intrusos (IDS)

Un IDS es una aplicación de seguridad informática cuyo objetivo es detectar una gran variedad de violaciones de

seguridad, que van desde intentos de intrusión externos hasta penetraciones en el sistema y abusos por parte de personas internas [24]. Las principales funciones de los IDS son monitorear hosts y redes, analizar el comportamiento de los sistemas informáticos, generar alertas y responder a comportamientos sospechosos. Debido a que monitorean las redes y host relacionados, los IDS generalmente se implementan cerca de los nodos de red protegidos, siendo los lugares con mayores tráficos de red [25].

La mayoría de los IDS tienen una estructura común que incluye:

1. Un módulo de recopilación de datos que posiblemente contenga evidencia de un ataque,
2. Un módulo de análisis que detecta ataques después de procesar esos datos, y
3. Un mecanismo para informar un ataque.

En el módulo de recopilación de datos, los datos de entrada de cada parte de los sistemas IoT se pueden recopilar y examinar para encontrar el comportamiento normal de interacción, detectando así el comportamiento malicioso en las primeras etapas. El módulo de análisis se puede implementar utilizando varias técnicas y métodos, sin embargo, los métodos basados en ML son más adecuados y dominantes para la tarea de aprender comportamientos benignos y anómalos en función de cómo los dispositivos y sistemas de IoT interactúan entre sí en entornos de IoT. Además, los métodos ML pueden predecir nuevos ataques, que a menudo son diferentes de los ataques anteriores, porque los métodos ML pueden predecir de forma inteligente futuros ataques desconocidos aprendiendo datos previamente existentes [8].

Algunos IDS open source que se pueden utilizar de forma gratuita son los siguientes:

- **Snort:** La primera versión se desarrolló por 1998 y cabe mencionar que en aquel momento no se contempló como IDS puro, pero fue evolucionando hasta ese punto.
- **Suricata:** Es un sistema de detección de intrusiones avanzado que permite multihilos, aceleración mediante hardware, entre otros.
- **Kismet:** Es un IDS Wireless enfocado en la red.

## C. Métodos de Detección de IDS

Los métodos de detección usados por IDS se pueden dividir en cuatro tipos de metodologías que se explica a continuación.

Las **técnicas de detección basadas en firmas** contienen un depósito de firmas de ataques y comparan el tráfico de red o las acciones del sistema con este depósito de firmas. Tan pronto como se encuentra una coincidencia, se genera una alerta de detección. Aunque es suficientemente precisa contra ataques conocidos para los que existen firmas en el repositorio, esta técnica no puede detectar ataques de día cero (nuevos). Incluso si no es efectivo contra mutaciones de un ataque existente [7,9,26].

Algunas investigaciones, como [27], propusieron medios para superar esta deficiencia de técnicas basadas en firmas mediante el uso de un Sistema Inmune Artificial (AIS). Esta técnica diseñó detectores que se basan en firmas/patrones de ataques utilizando el modelo de células inmunitarias, que pueden detectar si un paquete es normal o malicioso a través de

su clasificación como elemento propio o no propio. El sistema tiene la capacidad de adopción de nuevos patrones a partir del monitoreo continuo del sistema. Sin embargo, la viabilidad de tal técnica de detección en un entorno de IoT con recursos limitados es cuestionable [7].

Los autores de [28] resolvieron las limitaciones de recursos en los IDS basados en firmas mediante la utilización de una máquina Linux independiente con una versión adaptada del IDS de firmas basado en Suricata [28] sin embargo, los autores no proporcionaron ninguna pista sobre la actualización de las firmas de ataque. Los autores en [29] ampliaron el trabajo publicado en [28] al proponer modificaciones en las técnicas de coincidencia de firmas. Otra investigación de [10] abordó las limitaciones de potencia de procesamiento de los sistemas IoT mediante el uso de valores de cambio auxiliares con un algoritmo de detección de patrones múltiples, lo que permite una reducción en la cantidad de operaciones de coincidencia requeridas entre las firmas de ataque y los paquetes de tráfico de red. El sistema utilizó repositorios de firmas del IDS de código abierto (Snort) y del antivirus de código abierto (ClamAV) [7].

Las **técnicas de detección basadas en anomalías** se basan en un perfil de comportamiento normal de referencia para el entorno supervisado [26,30]. Esta línea de base normal se usa luego para comparar las acciones del sistema en cualquier momento dado. Cualquier desviación fuera de los límites del umbral permitido se informa generando una alerta sin proporcionar ninguna clasificación para el tipo de ataque detectado. También hay intentos de usar modelos de aprendizaje automático que aprenden eventos normales y de anomalías como modelos de detección de comportamiento. En comparación con las técnicas de detección basadas en firmas, las técnicas de detección basadas en anomalías son más eficaces para descubrir nuevos ataques. Un inconveniente de esta técnica es la dificultad para construir el perfil de referencia de comportamiento normal, lo que da lugar a un aumento de las tasas de falsos positivos [31,32,33]. Las técnicas de detección basadas en anomalías se basan en algoritmos de ML para crear un perfil normal básico de los sistemas supervisados. El uso de tales técnicas de ML en entornos de IoT con recursos y energía limitados sigue siendo un desafío, debido a los altos recursos computacionales necesarios para entrenar y validar las técnicas de ML [2].

Las **técnicas de detección basadas en especificaciones** tienen el mismo principio básico de las técnicas de detección basadas en anomalías, donde el comportamiento normal de un sistema se perfila a través de algún medio y se compara con las acciones actuales del sistema para detectar desviaciones fuera de rango. Sin embargo, en las técnicas basadas en anomalías, el comportamiento normal se aprende a través de ML, mientras que, para las técnicas basadas en especificaciones, un experto humano debe especificarlo manualmente a través de un repositorio de reglas y rangos asociados de desviaciones [34]. Esto permite reducir las tasas de falsos positivos en comparación con las técnicas de detección basadas en anomalías [31]. Con la ventaja de no requerir ninguna fase de aprendizaje después de especificar un conjunto de reglas [34],

estas técnicas adolecen de falta de adaptabilidad a entornos variados y son propensas a errores en las especificaciones [7,35].

Las **técnicas de detección basadas en híbridos** emplean una combinación de las técnicas mencionadas anteriormente para compensar las deficiencias y optimizar las ventajas de detectar ataques nuevos y existentes. Los autores en [36] propusieron SVELTE, que es un IDS para sistemas IoT conectados a IP que utilizan RPL como protocolo de enrutamiento en redes 6LoWPAN. Este IDS se diseñó utilizando un híbrido de técnicas de detección basadas en anomalías y firmas para obtener un equilibrio entre los requisitos de almacenamiento y procesamiento de cada una de estas dos técnicas. Intentaron equilibrar el costo de almacenamiento de la detección basada en firmas y el costo informático de las técnicas basadas en anomalías [7].

#### *D. Taxonomía de ML para Seguridad IoT*

En la era actual de la tecnología, la seguridad de las redes de Internet de las Cosas (IoT) se ha convertido en un campo de importancia crítica. La proliferación de dispositivos conectados ha traído consigo nuevos retos de seguridad, impulsando la necesidad de soluciones más avanzadas y adaptativas. En este contexto, las técnicas de Machine Learning y Deep Learning emergen como herramientas poderosas, ofreciendo enfoques novedosos y eficientes para detectar y prevenir amenazas de seguridad en redes IoT. Esta introducción presenta una taxonomía detallada de estas técnicas, destacando cómo se aplican en diferentes escenarios de seguridad de redes IoT. Se exploran diversas metodologías y algoritmos, desde enfoques clásicos de Machine Learning hasta arquitecturas complejas de Deep Learning, proporcionando una visión integral de cómo estas tecnologías están modelando el futuro de la seguridad en el IoT. A través de esta revisión, se busca no solo entender las capacidades actuales de estas técnicas, sino también anticipar futuras direcciones y desafíos en este campo en rápida evolución.

##### *D.1 Técnicas de Machine Learning para IDS*

Las técnicas de Machine Learning (ML) en sistemas de detección de intrusiones (IDS) para entornos IoT, destacan tres clasificadores principales:

- Naive Bayes (NB), que usa el teorema de Bayes para clasificar tráfico basándose en observaciones previas, pero con limitaciones en la precisión debido a la falta de consideración de interdependencias entre características [37,38];
- K-Nearest Neighbor (KNN), que clasifica datos usando la distancia euclidiana sin parámetros adicionales, con la eficacia dependiente del número de vecinos más cercanos (k), siendo la selección de k crucial para la precisión [39,40]; y
- Árboles de Decisión (DT), que organizan un árbol basado en las características extraídas, enfrentando desafíos en almacenamiento y complejidad computacional [12,13,41,42].
- Máquinas de Vectores de Soporte(SVM), son modelos de aprendizaje supervisado que se utilizan para realizar tareas



de clasificación y regresión. Se basan en el concepto de encontrar el hiperplano que mejor separa las clases en el espacio de características. Este hiperplano se elige de manera que maximice el margen entre las clases, donde el margen se define como la distancia mínima entre el hiperplano y los puntos más cercanos de cada clase, conocidos como vectores de soporte. [56,57]

- El clasificador de Bosque Aleatorio (RF, por sus siglas en inglés de *Random Forest*) es un método de aprendizaje ensamblado para clasificación (y también puede ser utilizado para tareas de regresión), que opera construyendo múltiples árboles de decisión durante el entrenamiento y outputting la clase que es el modo de las clases (clasificación) o predicción media (regresión) de los árboles individuales. Los Bosques Aleatorios corrigen el hábito de los árboles de decisión de sobreajustar a su conjunto de entrenamiento, proporcionando así una mayor precisión general mediante la agregación de los resultados de múltiples árboles.[57]
- El Clasificador SGD (Descenso de Gradiente Estocástico) es un método de optimización y aprendizaje automático que utiliza el gradiente de la función de pérdida para encontrar el mínimo de esta función, actualizando los parámetros del modelo de forma iterativa. A diferencia del descenso de gradiente tradicional, que calcula el gradiente utilizando todo el conjunto de datos (lo cual puede ser muy costoso computacionalmente para grandes volúmenes de datos), el SGD actualiza los parámetros utilizando solo un subconjunto de los datos (un lote) en cada iteración, lo que resulta en una convergencia más rápida y eficiente.[58]

Se destaca la importancia de los IDS en la detección de amenazas, incluyendo ataques de día cero, y se menciona un modelo híbrido de dos niveles para redes IoT, con enfoque en el balance de datos y selección de características para mejorar el desempeño del modelo. En la solución propuesta que se describe en las siguientes secciones se planea probar el modelo en distintos datasets y escenarios para validar su rendimiento y abordar la detección de anomalías desconocidas.

### D.2 Técnicas de Deep Learning para IDS

Los algoritmos DL superan a los algoritmos ML en aplicaciones que involucran grandes conjuntos de datos. DL se vuelve más relevante en las aplicaciones de seguridad de IoT, ya que los entornos de IoT se caracterizan por la producción de grandes cantidades y una variedad de datos. Además, DL es capaz de modelar automáticamente conjuntos de características complejas a partir de los datos de muestra. Otra ventaja de los algoritmos DL es su capacidad para permitir enlaces profundos en redes IoT. Esto permite interacciones automáticas entre sistemas basados en IoT en ausencia de intervención humana para realizar funciones de colaboración asignadas [43].

Debido a su capacidad para extraer representaciones de características jerárquicas en una arquitectura profunda compleja, DL se puede clasificar como una rama de los algoritmos de ML que utiliza múltiples capas no lineales de procesamiento para extraer conjuntos de características. Estos conjuntos de características se utilizan luego para la abstracción y la detección de patrones después de las transformaciones necesarias DL puede usarse en modo generativo con

aprendizaje no supervisado, modo discriminativo con aprendizaje supervisado o un enfoque híbrido mediante la combinación de ambos modos [43].

Los diversos algoritmos de Deep Learning (DL) aplicados en sistemas de detección de intrusiones (IDS) para entornos IoT:

- Las Redes Neuronales Recurrentes (RNNs) son eficaces en el procesamiento secuencial de datos, especialmente en la detección de intrusos en la red, con investigaciones previas destacando su utilidad [14,44].
- Las Redes de Memoria a Largo Plazo (LSTM), una variante de RNN, son adecuadas para analizar datos temporales en detección de anomalías [45,46,47].
- Las Redes Neuronales Convolucionales (CNN) son útiles para la extracción de características de datos, aunque su alta demanda computacional plantea desafíos en IoT [15,48,49].
- Los Perceptrones Multicapa (MLP) se utilizan en funciones no lineales para clasificación o regresión.
- Los Autoencoders Profundos (AEs) se aplican en la detección de malware, mostrando mayor precisión que otros métodos [50,51].
- Las Máquinas de Boltzmann Restringidas (RBM) y las Redes de Creencias Profundas (DBN) enfrentan retos en su implementación en IoT por su alta demanda de recursos, pero se han utilizado en sistemas IDS [52,53].
- Las Redes Antagónicas Generativas (GAN) y los Conjuntos de Redes DL (EDLN) también se exploran para mejorar la precisión y el rendimiento en la seguridad de IoT [16,54,55].

## VI. SOLUCIÓN PROPUESTA

En esta sección se describe la modelización de la solución propuesta, los resultados obtenidos de un caso ejemplo y se resumen las principales conclusiones de dichos resultados.

### A. Modelo Propuesto

Este modelo se centra en la utilización de técnicas avanzadas de selección de características y la aplicación de un clasificador de votación, un enfoque de múltiples clasificadores que ha demostrado ser efectivo en la mejora de la precisión y eficacia del IDS.

La selección de características se abordará mediante métodos más sofisticados que los tradicionalmente utilizados, buscando optimizar el conjunto de datos para que el modelo de ML pueda identificar patrones de intrusión de manera más efectiva. En cuanto a las técnicas de ML, se explorarán algoritmos más avanzados y posiblemente personalizados para adaptarse mejor a las características únicas de los datos de intrusión, superando así las limitaciones de los métodos convencionales.

Este enfoque renovado no solo busca mejorar la precisión en la detección de intrusiones sino también aumentar la eficiencia operativa del IDS, reduciendo la tasa de falsos positivos y adaptándose dinámicamente a las nuevas amenazas en constante evolución [17].

El método consta de las siguientes seis fases principales:

1. Dataset: Se dividirá el conjunto de datos en entrenamiento y testeo con una proporción del 80% y 20% respectivamente.
2. Reducción de dimensionalidad: Se divide en dos etapas que son preprocesamiento de los datos y la selección de características.
  - 2.1. Preprocesamiento de los datasets: Consiste en transformar los datos sin procesar en un formato adecuado para el análisis mediante la aplicación de procesar los datasets originales. Por ejemplo, la eliminación de redundancia, la normalización de los datos en un formato más estándar o la eliminación de valores faltantes.
  - 2.2. Selección de características: para superar el problema de los conjuntos de datos de alta dimensión, se utiliza el enfoque de selección de características para reducir la dimensionalidad de los conjuntos de datos y seleccionar las características más relevantes para la clasificación.
3. Balanceo de datos: Consiste en tres etapas en paralelos que son:
  - 3.1. Sin balancear: Los datasets están desequilibrados, haciendo que la proporción de datos de cada clase no sea equitativa.
  - 3.2. SMOTE: Es una técnica de sobre muestreo que permite balancear los datasets y se aumenta la cantidad de datos de la clase minoritaria.
  - 3.3. RUS: Es una técnica de submuestreo que permite balancear los datasets y se disminuye la cantidad de datos de la clase mayoritaria.

El uso de estas tres etapas permitirá evaluar el mejor rendimiento de los modelos y su comportamiento según la cantidad de datos usados.
4. Entrenamiento del clasificador: Con el propósito de mejorar la precisión del IDS, se entrenan a varios clasificadores individuales basados en ML y DL y se construye un clasificador en conjunto basados en ellos.
5. Reconocimiento de ataques: el rendimiento de los modelos se prueba utilizando las métricas antes explicadas y la técnica de voting se utiliza para combinar las distribuciones de probabilidad de los modelos base con la regla de votos por mayoría para tomar decisiones de clasificación.
6. Resultados: Basado en las métricas de evaluación se evalúa el rendimiento de los clasificadores.

El modelo propuesto para la clasificación binaria en el contexto de la detección de ataques cibernéticos incorpora una metodología basada en el uso combinado de clasificadores Gradient Boosting (GB) y K-Nearest Neighbors (KNN). Estos clasificadores fueron seleccionados debido a su destacado rendimiento en pruebas experimentales previas, lo que indica su eficacia en la diferenciación precisa entre actividades normales y maliciosas dentro de los sistemas de red. Posteriormente, para mejorar la robustez y la precisión de la detección, se implementa un modelo de votación. Este enfoque de votación consolida los resultados de los clasificadores GB y KNN, permitiendo una decisión final basada en la mayoría, lo que mejora significativamente la capacidad del sistema para reconocer y clasificar correctamente los ataques, minimizando tanto los falsos positivos como los negativos. Este enfoque

integrado aprovecha las fortalezas individuales de cada clasificador y proporciona un mecanismo resiliente y adaptativo para la detección de intrusiones en entornos de red dinámicos.

### B. Fase Experimentación

Se realizaron las pruebas por cada clasificador por separado, utilizando el modelo de Voting, mencionado en el punto anterior, en la etapa de entrenamiento del clasificador y en la etapa de reconocimiento de ataque se quita la toma de decisiones. Se evaluarán diferentes modelos con las métricas de evaluación, que permitirán cuantificar el rendimiento de los clasificadores, estos son: *accuracy*, *precision*, *recall* y *f1-score*. Para el modelo propuesto, en la clasificación binaria, se utilizan los clasificadores GB y KNN. En la clasificación multiclase se utilizan los clasificadores KNN y RF.

Los datasets utilizados para el entrenamiento de los clasificadores fueron IoTID20, MQTT-IoT-IDS2020 y IoT-DS-2, utilizando un 80 % para el entrenamiento y un 20 % para el testing de los modelos.

- IoTID20: El banco de pruebas para el conjunto de datos IoTID20 [2] es una combinación de dispositivos IoT y estructuras de interconexión. Se implementó en un entorno doméstico inteligente que consiste en un dispositivo doméstico inteligente SKTNGU y una cámara Wi-Fi EZVIZ para generar el conjunto de datos IoTID20. Estos dos dispositivos IoT están conectados a un enrutador Wi-Fi doméstico inteligente. Otros dispositivos conectados al enrutador doméstico inteligente incluyeron computadoras portátiles, tabletas y teléfonos inteligentes. El SKT NGU y la cámara Wi-Fi EZVIZ fueron dispositivos víctimas de IoT y todos los demás dispositivos en el banco de pruebas fueron los dispositivos atacantes.
- Conjunto de datos MQTT-IoT-IDS2020: Fue creado por Hindy et al [18]. Desde la plataforma de red MQTT, este conjunto de datos consiste en tráfico de red regular y ataques de fuerza bruta. La red consta de 12 sensores MQTT, un intermediario, un dispositivo para replicar un flujo de cámara y un atacante. El conjunto de datos incluye los ataques y escenarios MQTT más populares para analizar dispositivos IoT del mundo real. El conjunto de datos MQTT-IoT-IDS2020 contiene cuatro categorías de ataque [19].
- Conjunto de datos IoT-DS-2: Incluye 15 clases de ataque y 1 clase normal. Se puede acceder a la recopilación de datos IoT-DS-2 en [19].

### C. Tratamiento de los Dataset

Esta fase se inicia con el preprocesamiento de los datasets, las instancias duplicadas se eliminarán de todos los conjuntos de datos. Después, se normalizarán cada una de las características utilizando el escalado de variables (Escala MinMax). De este proceso resultan datos que se encuentran en rango específico (0, 1), lo cual, elimina valores extremos y acelera significativamente los cálculos.

Después de realizar la normalización, se realiza un reemplazo de los valores Missing Values (Valores no identificados) con 0, en caso de que el proceso previo, haya creado valores inconsistentes. Por último, para las columnas no numéricas (Label y Cat) se reemplazarán su valores de cadena

de caracteres (string) a números enteros (number). En el caso de la columna Label las anomalías están representada por un valor de 1, mientras que un valor normal está representado por 0 en la clasificación binaria.

Para balancear los datasets se utiliza la técnica SMOTE, la cual realiza un sobremuestreo de minorías sintéticas (Synthetic Minority Over-sampling Technique - SMOTE) [19] permite aumentar el número de muestras tomando como referencia la clase minoritaria, generando nuevas instancias de las clases. SMOTE no cambia la cantidad de datos de la clase mayoritaria. La creación de las nuevas instancias no son un duplicado de las ya existentes, lo que hace el algoritmo es tomar una muestra al azar del espacio de características de la clase y de sus vecinos más cercanos. Después, se crea un ejemplo sintético en un punto seleccionado al azar entre las dos muestras en el espacio de características. Finalmente, permitiendo el aumento de las muestras para cada clase y hace que las muestras sean más generales.

#### D. Entorno Experimental

Se utilizaron tres entornos distintos para la parte experimental, los cuales, tienen distintas características computacionales.

En la parte de preprocesamiento de los datos, se utilizó un computador personal con las siguientes capacidades:

- Procesador (CPU): Intel I5-7200U
- Núcleos: 2
- RAM: 12 Gigabytes
- Sistema Operativo: Windows 10

En la etapa experimental se utilizó un servidor externo con las siguientes características:

- Núcleos: 8
- RAM: 15,19 Gigabytes
- Sistema Operativo: Centos

Se utilizó el lenguaje de programación Python 3.8.

#### E. Resultados

En los resultados **Clasificación Binaria Balanceada** (ver Tabla 1), los mejores clasificadores son RF, GB y KNN los que obtienen un f1 score sobre el 99% en todas sus métricas, siendo muy confiables para el dataset IoTID20.

En el dataset MQTT-IoT-IDS2020 los resultados demuestran que el mejor clasificador por lejos es GB con un 98.48% de f1 score, siendo el modelo más confiable. En el dataset IoT-DS-2 los resultados, muestran que la mayoría de los modelos han dado muy buenos resultados, siendo el peor NB con un 86,55% y el mejor GB con un 99.98% de f1 score.

Las demás métricas nos demuestran que los modelos realmente no sufrieron un mayor sobreajuste, dando unos modelos muy confiables y eficientes, mostrando lo eficaz del balanceo de datos con una gran cantidad de datos.

El modelo propuesto con voting obtiene un f1 score promedio en los tres datasets de 95.69%, siendo un modelo confiable con un mayor f1 score del 99.53%. Pero a pesar de ser buen modelo GB tiene un mejor rendimiento en general que el modelo propuesto, dando como resultado un f1 score de 99.7%, 98.48% y 99.98%, siendo más confiable para su uso en clasificación binaria balanceada

| Clasificador | Data    | Accuracy | Precision | Recall | F1 score | Tiempo [s] |
|--------------|---------|----------|-----------|--------|----------|------------|
| ADABOOST     | IoTID20 | 0.9504   | 0.9505    | 0.9504 | 0.9504   | 523.51     |
| ADABOOST     | MQTT    | 0.7966   | 0.8554    | 0.7964 | 0.7877   | 1926.77    |
| ADABOOST     | IoTDS2  | 0.9324   | 0.9399    | 0.9324 | 0.9322   | 1252.06    |
| DT           | IoTID20 | 0.8043   | 0.9367    | 0.6519 | 0.7688   | 9.95       |
| DT           | MQTT    | 0.7698   | 0.9996    | 0.5395 | 0.7008   | 36.43      |
| DT           | IoTDS2  | 0.9258   | 0.9823    | 0.8672 | 0.9211   | 24.41      |
| GB           | IoTID20 | 0.9970   | 0.9965    | 0.9974 | 0.9970   | 113.77     |
| GB           | MQTT    | 0.9850   | 0.9995    | 0.9705 | 0.9848   | 263.49     |
| GB           | IoTDS2  | 0.9998   | 0.9999    | 0.9998 | 0.9998   | 624.41     |
| KNN          | IoTID20 | 0.9947   | 0.9957    | 0.9935 | 0.9946   | 0.41       |
| KNN          | MQTT    | 0.8636   | 0.8935    | 0.8253 | 0.8581   | 1.39       |
| KNN          | IoTDS2  | 0.9631   | 0.9973    | 0.9287 | 0.9618   | 1.17       |
| NB           | IoTID20 | 0.5756   | 0.9362    | 0.1607 | 0.2744   | 0.95       |
| NB           | MQTT    | 0.7853   | 0.9847    | 0.5794 | 0.7296   | 5.35       |
| NB           | IoTDS2  | 0.8786   | 0.968     | 0.7822 | 0.8655   | 2.50       |
| RF           | IoTID20 | 0.9971   | 0.9955    | 0.9987 | 0.9971   | 2572.12    |
| RF           | MQTT    | 0.7939   | 0.9836    | 0.5974 | 0.7433   | 13692.35   |
| RF           | IoTDS2  | 0.9347   | 0.9998    | 0.8695 | 0.9301   | 5419.03    |
| SGD          | IoTID20 | 0.5893   | 0.5518    | 0.9429 | 0.6962   | 3.10       |
| SGD          | MQTT    | 0.6923   | 0.9700    | 0.3964 | 0.5628   | 25.37      |
| SGD          | IoTDS2  | 0.8792   | 0.9722    | 0.7805 | 0.8659   | 42.38      |
| Voting       | IoTID20 | 0.9953   | 0.9953    | 0.9953 | 0.9953   | 19.72      |
| Voting       | MQTT    | 0.9118   | 0.9250    | 0.9117 | 0.9111   | 74.48      |
| Voting       | IoTDS2  | 0.9643   | 0.9667    | 0.9643 | 0.9643   | 112.35     |

Tabla 1: Resultados Clasificación Binaria Balanceada

Los resultados de **Clasificación de multiclase** (ver Tabla 2) se muestran que los modelos RF y KNN tienen el mejor rendimiento con un 97% de F1 Score pero solo en el dataset IoTID20, pero al calcular el promedio del rendimiento de estos clasificadores da 75,91% y 83,28, obteniendo KNN un mejor rendimiento general.

| Clasificador | Data    | Accuracy | Precision | Recall | F1 score | Tiempo [s] |
|--------------|---------|----------|-----------|--------|----------|------------|
| ADABOOST     | IoTID20 | 0.7297   | 0.7378    | 0.7296 | 0.7298   | 582.46     |
| ADABOOST     | MQTT    | 0.3616   | 0.4114    | 0.3614 | 0.3063   | 2074.39    |
| ADABOOST     | IoTDS2  | 0.1527   | 0.2518    | 0.1525 | 0.0840   | 3410.84    |
| DT           | IoTID20 | 0.4755   | 0.4879    | 0.4749 | 0.3907   | 10.60      |
| DT           | MQTT    | 0.4978   | 0.4528    | 0.4979 | 0.4268   | 38.44      |
| DT           | IoTDS2  | 0.2352   | 0.0707    | 0.2348 | 0.1043   | 72.45      |
| GB           | IoTID20 | 0.6327   | 0.7451    | 0.6325 | 0.6313   | 13376.06   |
| GB           | MQTT    | 0.4392   | 0.6719    | 0.4396 | 0.3968   | 20117.72   |
| GB           | IoTDS2  | 0.3451   | 0.3727    | 0.3449 | 0.3094   | 9592.04    |
| KNN          | IoTID20 | 0.9785   | 0.9788    | 0.9785 | 0.9785   | 0.40       |
| KNN          | MQTT    | 0.6947   | 0.7589    | 0.6947 | 0.7009   | 1.52       |
| KNN          | IoTDS2  | 0.8104   | 0.8385    | 0.8103 | 0.8189   | 1.58       |
| NB           | IoTID20 | 0.5840   | 0.6731    | 0.5841 | 0.5784   | 1.10       |
| NB           | MQTT    | 0.4986   | 0.6409    | 0.4986 | 0.4273   | 4.68       |
| NB           | IoTDS2  | 0.4835   | 0.5808    | 0.4830 | 0.4391   | 7.71       |
| RF           | IoTID20 | 0.9799   | 0.9804    | 0.9798 | 0.9799   | 2485.16    |
| RF           | MQTT    | 0.6489   | 0.7361    | 0.6488 | 0.6489   | 9685.09    |
| RF           | IoTDS2  | 0.6509   | 0.9351    | 0.6504 | 0.6485   | 13326      |
| SGD          | IoTID20 | 0.4130   | 0.5472    | 0.4132 | 0.2910   | 76.51      |
| SGD          | MQTT    | 0.4058   | 0.4659    | 0.4059 | 0.3408   | 322.45     |
| SGD          | IoTDS2  | 0.4027   | 0.3662    | 0.4024 | 0.3183   | 1453.06    |
| Voting       | IoTID20 | 0.9617   | 0.9633    | 0.9617 | 0.9616   | 2524.21    |
| Voting       | MQTT    | 0.6876   | 0.7500    | 0.6876 | 0.6928   | 10507.97   |
| Voting       | IoTDS2  | 0.7000   | 0.8493    | 0.6996 | 0.6921   | 13012.95   |

Tabla 2: Resultados Clasificación de multiclase

Los resultados de cada uno de los modelos disminuyeron drásticamente, siendo posible un error de configuración con SMOTE. El rendimiento de los modelos definitivamente no es óptimo, por tanto, es necesario replantear la técnica de balanceo utilizada o buscar otra configuración de los parámetros de los clasificadores.

#### F. Síntesis de los Resultados

Al realizar el análisis de resultados de la primera etapa experimental al clasificar los datos no balanceados con clase

binaria, se puede deducir que los modelos tienen un alto rendimiento, pero en algunos casos sufren de sobreajustes por el desbalanceo de clases. Los dos mejores modelos en base a sus métricas son GB y KNN, que son utilizados como clasificadores del modelo propuesto, pero el mejor modelo fue GB, obteniendo un mejor rendimiento en los tres datasets. Al clasificar los datos balanceados con SMOTE con clase binaria, el rendimiento de los clasificadores bajo en comparación a la clasificación binaria sin el balanceo de datos.

Los clasificadores que más destacaron fueron GB y KNN, que son utilizados como clasificadores del modelo propuesto con voting, pero se repite que GB sobresale a los demás en la clasificación binaria. Al clasificar los datos no balanceados multiclase, el rendimiento de los modelos empezó a disminuir, una de las causas puede ser el desbalanceo de las clases, habiendo clases que están muy poco representadas en los datasets. A pesar de esto, los clasificadores RF y KNN destacaron, pero solo en el dataset IoTID20, siendo utilizados como clasificadores del modelo propuesto con voting, pero en general KNN tiene un mejor rendimiento. Al clasificar datos balanceados con SMOTE multiclase, el rendimiento en general de los clasificadores disminuyó drásticamente. Esto puede deberse a una mala configuración de los parámetros en los modelos para una clasificación multiclase o a la técnica de balanceo SMOTE que hizo que se solaparan ciertos tipos de datos, haciendo que los clasificadores tengan un bajo rendimiento al no clasificar correctamente. El modelo que destacó fue KNN teniendo el mejor rendimiento de todos.

## VII. CONCLUSIONES

El crecimiento exponencial de las redes IoT ha impulsado significativos avances en diversos sectores de la sociedad, integrándose como un componente esencial en nuestro presente y futuro. Sin embargo, esta integración masiva también introduce múltiples vectores de amenazas, demandando soluciones innovadoras para garantizar la seguridad de estas redes. Los Sistemas de Detección de Intrusos (IDS) basados en técnicas de Aprendizaje Automático (ML) y Aprendizaje Profundo (DL) emergen como soluciones prometedoras, dada su capacidad para no solo detectar amenazas conocidas sino también adaptarse y reconocer nuevas vulnerabilidades, como los ataques de día cero.

El documento establece una metodología de investigación rigurosa, reportando un avance completo en la revisión del estado del arte. Se exploran las distintas arquitecturas IoT, destacando la ausencia de un estándar universal y la diversidad de protocolos y tecnologías que facilitan la interconexión de dispositivos. Se identifican las amenazas prevalentes en un marco de arquitectura IoT de cuatro capas y se profundiza en la taxonomía de los IDS, incluyendo una revisión de las técnicas de ML y DL aplicables, los conjuntos de datos relevantes para IoT y un análisis de investigaciones previas que abordan la detección de intrusos en este contexto.

El enfoque inicial de votación no cumplió las expectativas, pero orientó la formulación de una metodología efectiva evaluada mediante los conjuntos de datos IoTID20, MQTT-IoT-IDS2020, e IoT-DS-2. Se propone un modelo híbrido

bifásico: la primera fase emplea un clasificador de Gradiente Boosting (GB) para filtrar actividades normales de las anomalías, alcanzando altas puntuaciones F1 en los conjuntos de datos probados. Las anomalías detectadas avanzan a una segunda fase para una clasificación detallada, utilizando técnicas avanzadas como RFECV para la selección de características y SMOTE para el equilibrio de datos, culminando en la clasificación mediante KNN. Este modelo híbrido demuestra un desempeño sobresaliente en la detección y clasificación de anomalías.

La consistencia en el desempeño entre los conjuntos de datos sugiere la robustez del modelo, aunque se identificaron limitaciones en la calidad de los datos de MQTT-IoT-IDS2020. La eficacia del sobremuestreo (SMOTE) en la clasificación multiclase contrasta con el submuestreo (RUS), que, pese a simplificar el entrenamiento, compromete la precisión del modelo. Investigaciones futuras se enfocarán en validar el modelo con conjuntos de datos adicionales, explorar otras técnicas de equilibrio de datos, integrar métodos de selección de características y modelos de clasificación alternativos, y finalmente, implementar y verificar el modelo híbrido en escenarios reales para abordar la detección de anomalías desconocidas de manera efectiva.

Como futuras líneas de investigación, se propone la validación del modelo propuestos con otros casos de uso pertenecientes a contexto de uso más sensible, como es el caso de los sistemas ciberfísicos aplicados al área de la salud. También sería de mucho interés, el análisis detallado de los algoritmos ML y DL utilizados, a fin de mejorar su performance y efectividad.

## VIII. REFERENCIAS

- [1] Flores F. and Cossio E. Aplicaciones, enfoques y tendencias del internet de las cosas (IoT): revisión sistemática de la literatura. *Academia Journals*, 2021. <http://ciateq.repositorioinstitucional.mx/jspui/handle/1020/543>
- [2] Ullah Imtiaz and Mahmoud Qusay. A scheme for generating a dataset for anomalous activity detection in iot networks. pages 508–520, 2020. Department of Electrical, Computer and Software Engineering, Ontario Tech University, Oshawa, ON L1G 0C5, Canada.
- [3] Hasan Alkahtani and Theyazn H. H. Aldhyani. Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms. *Complexity*, 2021(Article ID 5579851):18, 2021. <https://doi.org/10.1155/2021/5579851>.
- [4] Yang Li, Manias Dimitrios Michael, and Shami Abdallah. Pwpae: An ensemble framework for concept drift adaptation in IoT data streams. 2021 IEEE Global Communications Conference (GLOBECOM), page 6, 2021. <http://dx.doi.org/10.1109/GLOBECOM46510.2021.9685338>.
- [5] V. Ishanoglu, C. Covarrubias, R. Rivera, H. Espinoza, and J. Millán. Panorama de las Smart Cities y la ciberseguridad. *CSIRT*,13:32,2021. <https://www.csirt.gob.cl/media/2022/01/CSIRT-CiberSucesos-2021-11-12.pdf>.
- [6] Doohwan Oh, Deokho Kim, and Won Woo Ro. A malicious pattern detection engine for embedded security systems in the internet of things. *Sensors (Basel, Switzerland)*, 14:24188–24211, 12 2014.
- [7] Marwa Keshk, Nour Moustafa, Elena Sitnikova, and Benjamin Tum-bull. Privacy-preserving big data analytics for cyber-physical systems. *Wireless Networks*, 28, 04 2022.
- [8] Robert Mitchell and Ing-Ray Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, 46, 03 2014.
- [9] Debar, H. (2000). An introduction to intrusion-detection systems. *Proceedings of Connect*, 2000.

- [10] Anoop and Sunil Rai. A COMPARATIVE STUDY OF DIFFERENT TYPES OF NETWORKS IJIRT, 1:5, 2014. [https://ijirt.org/master/publishedpaper/IJIRT101024\\_PAPER.pdf](https://ijirt.org/master/publishedpaper/IJIRT101024_PAPER.pdf).
- [11] M. Benaiah Deva Kumar and B. Deepa. Computer Networking: A Survey. IJTRD, 2(5):5, 2015. [https://www.researchgate.net/publication/317101504\\_ComputerNetworking\\_A\\_Survey](https://www.researchgate.net/publication/317101504_ComputerNetworking_A_Survey)
- [12] Ashraf Javed, Moustafa Nour, Khurshid Hasnat, Debie Essam, Haider Waqas, and Wahab Abdul. A review of intrusion detection systems using machine and deep learning in Internet of things: Challenges, solutions and future directions. Electronics, 9, 07 2020.
- [13] Karen Scarfone and Peter Mell. Guide to Intrusion Detection and Prevention Systems (IDPS), volume 800. 01 2007. Nist National Institute of Standards and Technology.
- [14] João P. Amaral, Luís M. Oliveira, Joel J. P. C. Rodrigues, Guangjie Han, and Lei Shu. Policy and network-based intrusion detection system for ipv6-enabled wireless sensor networks. In 2014 IEEE International Conference on Communications (ICC), pages 1796–1801, 2014.
- [15] Sethi Pallavi and Sarangi Smruti. Internet of things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017:1–25, 01 2017.
- [16] Ashraf Javed, Moustafa Nour, Khurshid Hasnat, Debie Essam, Haider Waqas, and Wahab Abdul. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics, 9, 07 2020.
- [17] Ismail Butun, Salvatore Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys Tutorials, PP:266 – 282, 05 2013.
- [18] Shahid Raza, Linus Wallgren, and Thiemo Voigt. Svelte: Real-time intrusion detection in the internet of things. Ad Hoc Networks, 11, 05 2013.
- [19] G. D’Agostini. A multidimensional unfolding method based on bayes’ theorem. Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 362(2):487–498, 1995.
- [20] Andrew Ng and Michael Jordan. On discriminative vs. generative classifiers: A comparison of logistic regression and naive bayes. In T. Dietterich, S. Becker, and Z. Ghahramani, editors, Advances in Neural Information Processing Systems, volume 14. MIT Press, 2001.
- [21] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access, PP:1–1, 06 2019.
- [22] P. Soucy and G.W. Mineau. A simple KNN algorithm for text categorization. In Proceedings 2001 IEEE International Conference on Data Mining, pages 647–648, 2001.
- [23] Xue-wen Chen and Jong Cheol Jeong. Enhanced recursive feature elimination. In Sixth International Conference on Machine Learning and Applications (ICMLA 2007), pages 429–435, 2007.
- [24] Sotiris Kotsiantis. Supervised machine learning: A review of classification techniques. Informatica (Slovenia), 31:249–268, 01 2007.
- [25] Wenliang Du and Zhijun Zhan. Building decision tree classifier on private data. 01 2003.
- [26] J. R. Quinlan. Induction of decision trees. Mach. Learn., 1(1):81–106, March 1986.
- [27] Salem Alharbi, Peter Rodriguez, Rajaputhri Maharaja, Prashant Iyer, Nivethitha Subaschandrabose, and Zilong Ye. Secure the internet of things with challenge response authentication in fog computing. In 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), pages 1–2, 2017.
- [28] Hanan Hindy, David Brosset, Ethan Bayne, Amar Kumar Seeam, Christos Tachtatzis, Robert Atkinson, and Xavier Bellekens. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access, 8:104650–104675, 2020.
- [29] Pablo Torres, Carlos Catania, Sebastian Garcia, and Carlos Garcia Garino. An analysis of recurrent neural networks for botnet detection behavior. In 2016 IEEE Biennial Congress of Argentina (ARGEN-CON), pages 1–6, 2016.
- [30] Mudar Almi’ani, Alia Abughazleh, Amer Al-rayahfeh, Saleh Atiewi, and Abdul Razaque. Deep recurrent neural network for IoT intrusion detection system. Simulation Modelling Practice and Theory, 101:102031, 11 2019.
- [31] Tian Guo, Zhao Xu, Xin Yao, Haifeng Chen, Karl Aberer, and Koichi Funaya. Robust online time series prediction with recurrent neural networks. In 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), pages 816–825, 2016.
- [32] Yao Qin, Dongjin Song, Haifeng Cheng, Wei Cheng, Guofei Jiang, and Garrison Cottrell. A dual-stage attention-based recurrent neural network for time series prediction. 04 2017.
- [33] Pankaj Malhotra, Lovekesh Vig, Gautam Shroff, and Puneet Agarwal. Long short-term memory networks for anomaly detection in time series. 04 2015.
- [34] Niall McLaughlin, Jesus Martinez del Rincon, BooJoong Kang, Suleiman Yerima, Paul Miller, Sakir Sezer, Yeganeh Safaei, Erik Trickle, Ziming Zhao, Adam Doupé, and Gail Joon Ahn. Deep android malware detection. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, CODASPY ’17, page 301–308, New York, NY, USA, 2017. Association for Computing Machinery.
- [35] Sudeendra Kumar K, Sauvagya Sahoo, Abhishek Mahapatra, Ayas Kanta Swain, and K.K. Mahapatra. Security enhancements to system on chip devices for iot perception layer. In 2017 IEEE International Symposium on Nanoelectronic and Information Systems (INIS), pages 151–156, 2017.
- [36] D.E. Denning. An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2):222–232, 1987.
- [37] Wei Wang, Ming Zhu, Xuewen Zeng, Xiaozhou Ye, and Yiqiang Sheng. Malware traffic classification using convolutional neural network for representation learning. In 2017 International Conference on Information Networking (ICOIN), pages 712–717, 2017.
- [38] Hongyu Liu and Bo Lang. Machine learning and deep learning methods for intrusion detection systems: A survey. Applied Sciences, 9:4396, 10 2019. Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani. A survey of machine and deep learning methods for Internet of things (IoT) security. IEEE Communications Surveys Tutorials, 22(3):1646–1685, 2020.
- [39] Sahil Garg, Kuljeet Kaur, Neeraj Kumar, Georges Kaddoum, Albert Y. Zomaya, and Rajiv Ranjan. A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Transactions on Network and Service Management, 16(3):924–935, 2019.
- [40] Mahmood Yousefi-Azar, Vijay Varadharajan, Len Hamey, and Uday Tupakula. Autoencoder-based feature learning for cyber security applications. In 2017 International Joint Conference on Neural Networks (IJCNN), pages 3854–3861, 2017.
- [41] Yisroel Mirsky, Tomer Doitshman, Yuval Elovici, and Asaf Shabtai. Kitsune: An ensemble of autoencoders for online network intrusion detection. CoRR, abs/1802.09089, 2018.
- [42] Mayuranathan Mani, Murugan Mahalingam, and V. Dhanakoti. Best features-based intrusion detection system by rbm model for detecting ddos in cloud environment. Journal of Ambient Intelligence and Humanized Computing, 12, 03 2021.
- [43] Ugo Fiore, Francesco Palmieri, Aniello Castiglione, and Alfredo Santis. Network anomaly detection with the restricted boltzmann machine. Neurocomputing, 122:13–23, 12 2013.
- [44] Marwa Keshk, Elena Sitnikova, Nour Moustafa, Jiankun Hu, and Ibrahim Khalil. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. IEEE Transactions on Sustainable Computing, 6(1):66–79, 2021.
- [45] Yuanfang Chen, Yan Zhang, and Sabita Maharjan. Deep learning for secure mobile edge computing. CoRR, abs/1709.08025, 2017.
- [46] Yuancheng Li, Rong Ma, and Runhai Jiao. A hybrid malicious code detection method based on deep learning. International Journal of Software Engineering and Its Applications, 9:205–216, 05 2015.
- [47] Robert E. Hiromoto, Michael Haney, and Aleksandar Vakanski. A secure architecture for IoT with supply chain risk management. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), volume 1, pages 431–435, 2017.
- [48] Yuyang Zhou, Guang Cheng, Shanqing Jiang, and Mian Dai. Building an efficient intrusion detection system based on feature selection and ensemble classifier. Computer Networks, 174, 06 2020.
- [49] Hanan Hindy, Ethan Bayne, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, and Xavier Bellekens. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoTIDS2020 Dataset), pages 73–84. 01 2021.
- [50] I. Ullah and Q.H. Mahmoud. In IoT Intrusion Detection Datasets., 2021. Disponible online: <https://sites.google.com/view/iotdataset1> (Accedido el 6 de Julio del 2023).
- [51] Kevin W. Bowyer, Nitesh V. Chawla, Lawrence O. Hall, and W. Philip Kegelmeyer. SMOTE: synthetic minority over-sampling technique. CoRR, abs/1106.1813, 2011.
- [52] Marwa Keshk, Benjamin Turnbull, Nour Moustafa, Dinusha Vatsalan, and Kim-Kwang Raymond Choo. A privacy-preserving-framework-



based blockchain and deep learning for protecting smart power networks. IEEE Transactions on Industrial Informatics, 16(8):5110–5118, 2020.

- [53] Caiming Liu, Jin Yang, Run Chen, Yan Zhang, and Jinqian Zeng. Research on immunity-based intrusion detection technology for the internet of things. In 2011 Seventh International Conference on Natural Computation, volume 1, pages 212–216, 2011.
- [54] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, and Mark Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pages 600–607, 2013.
- [55] Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, and Maurizio Spirito. Demo: An iids framework for internet of things empowered by 6lowpan. pages 1337–1340, 11 2013.
- [56] Arenas-Hoyos, S.A., Bernal-Noreña, Á. Support vector machines implementation over integers modulo-M and Residue Number System.
- [57] Longfei Sun;Yanhui Liu;Yuanjian Wang;Qinghao Dong;Wanjie Zhao, Analysis of characteristic index and prediction of river bottom tearing scour in the Yellow River.
- [58] S. Gomez, M. Martinez, y J. Lopez, "Eficiencia del clasificador SGD en grandes conjuntos de datos," *Journal of Machine Learning Research*, vol. 15, no. 4, pp. 1123-1145, Jul. 2023.

## IX. BIOGRAFÍAS



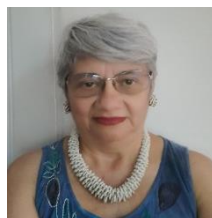
**Dr.(c)Sebastián Berrios** nacido el 7 diciembre de 1986. Actualmente candidato a doctor en Ingeniería informática en la Pontificia Universidad Católica de Valparaíso. Graduado de Ingeniería Civil en Computación e Informática en la Universidad De Las Américas. Magíster en Ciencias de la Ingeniería y Magíster en Ingeniería en Informática en la Pontificia Universidad Católica de Valparaíso. Actualmente docente del área de Ciberseguridad y Administrador de TI de la escuela de ingeniería informática de la Pontificia Universidad Católica de

Valparaíso. Cursando un Diplomado de Inclusión en Educación en la Pontificia Universidad Católica de Valparaíso, con una duración de 140 horas. Además, se cursó un Diplomado en Seguridad de la Información de 132 horas en la Universidad de Chile y un Diplomado en Ciberseguridad de 96 horas en la misma universidad. También se obtuvo un Diplomado en Ciberseguridad de 100 horas en el Instituto Profesional IACC.



**Pamela Hermosilla** nacida en Valparaíso, Chile, el 8 de octubre de 1974. Graduada de Universidad Técnica Federico Santa María (UTFM Ingeniero Civil en Informática (UTFSM), Diplomada en Comercio Electrónico y Logística Empresarial (UTFSM), Auditor Interno ISO 9001 (Brain & Cia Consultores), MBA of Chief Information Officer CIO (Abet Open University), Diplomada en Docencia Universitaria de la Pontificia Universidad

Católica de Valparaíso (PUCV), Diplomada en Formación Virtual Universitaria (PUCV), Symposium for Entrepreneurship Educators (Luksic Scholars – Babson College). Asesorías: miembro del Consejo Público Privado de la red Fortalece Pyme, Valparaíso - Corfo, integrante del Board de Directores, de la incubadora Chrisalys PUCV. Desarrollo profesional en áreas de Aseguramiento de calidad en gestión de proyectos, Planificación estratégica organizacional, Rediseño curricular basado en competencias, Habilidades de Innovación y emprendimiento en estudiantes de ingeniería, Gamificación en el proceso de enseñanza y aprendizaje.



**Herminia Beatriz Parra de Gallo**, Especialista en Informática Forense, Dra. en Ingeniería Mención Sistemas de Información, Master en Administración de Negocios, Ingeniería en Computación. Con una extensa carrera académica como docente e investigadora en la UCASAL reviste la categoría de INVESTIGADOR INDEPENDIENTE “B” (CI-UCASAL), y es Directora del Grupo de I+D+i de Forensia Digital de esa institución, grupo abocado al desarrollo de

proyectos de i+d interinstitucionales con universidades nacionales y latinoamericanas. Es además, Directora del Instituto de Estudios Interdisciplinarios de Ingeniería de la Facultad de Ingeniería de la UCASAL y Directora de la carrera de Especialización en Administración de Bases de Datos. Participa en la formación de recursos humanos impartiendo cursos de posgrado y como docente de carreras de grado y posgrado en UFASTA (Argentina), UTN-FRSF (Argentina), UTN-FRC (Argentina), UNIVA (México), UNISANGIL (Colombia), Universidad Católica de Colombia (Colombia), UniTECH (España). Perito Informático de Parte. Consultora en Proyectos Tecnológicos Críticos. Sus temáticas de interés son: Forensia Digital, Educación en Ingeniería y Ética en la Ingeniería.



**Pablo Oñate** Ingeniero civil informático con el grado de magister en ingeniería informática en la Pontificia Universidad Católica de Valparaíso, cuenta con amplio conocimiento de machine learning y matemática estadística para el análisis de datos y creación de modelos predictivos.

# ¿Podemos considerar persona a la IA?

Antonela D’Onofrio, Lucía Algieri, Ana Haydée Di Iorio, Bruno Constanzo

**Abstract**--El auge de la Inteligencia Artificial y sus usos cada vez más difundidos, en áreas de conocimiento y profesiones inesperadas, causan sorpresa y confusión por parte de éstas. El no conocer cómo funcionan, sumado al halo místico con que empresas y desarrolladores rodean a estos sistemas, ocasiona que surjan situaciones donde se le otorgan cualidades y características propias de los seres vivos e incluso las personas humanas. En este trabajo se debate sobre los aspectos tecnológicos, técnicos, jurídicos y filosóficos con los cuales se puede enfocar la cuestión de la Inteligencia Artificial, para llegar a debatir la cuestión de si es posible o no considerar persona a los modelos de IA, y las consecuencias legales y jurídicas que esto puede desencadenar.

**Palabras Clave**--Inteligencia Artificial, Derecho, Sujeto de Derecho, Persona, Encuadre jurídico.

## I. INTRODUCCIÓN

EL devenir de los avances tecnológicos han introducido nuevas y disruptivas herramientas que acompañan las tareas cotidianas de los seres humanos. Sin lugar a dudas, la incorporación de tecnologías de Inteligencia Artificial en diversos aspectos de la sociedad y profesiones que tenían poco contacto con la informática ha generado grandes aportes a la humanidad. Ahora bien, dicha incorporación ha generado grandes discusiones respecto a su alcance, limitación y regulación. También han aparecido múltiples posturas que van desde planteos válidos y racionales hasta extremos anclados únicamente en la imaginación y la ficción, muchas veces enraizados en un entendimiento básico o nulo de cómo funcionan estas tecnologías. No ayuda que muchos proponentes de las mismas son vagos al respecto, y constantemente envuelven los productos en halos de misterio, tratando de dotarle cualidades de los seres vivos en general, y de los seres humanos en particular a cuanto producto nuevo comercializan con el “*sticker*” de Inteligencia Artificial. Las diversas posturas pueden pasar de ser extremo apocalípticas a indiferentes, de regulaciones puntillosas a falta absoluta de regulación.

El presente trabajo es un punto de partida en la discusión que nos convoca: es necesario desmitificar la humanización de la tecnología. En pos de ello, haremos un abordaje de la verdadera naturaleza de la IA, basándonos en las miradas científica-tecnológica y jurídico-filosófica para establecer qué elementos del derecho pueden configurar a la Inteligencia Artificial, y en última instancia, concluir si debiera o no ser considerada un sujeto de derecho y por qué.

## II. MARCO TEÓRICO

Para realizar un estudio lo más acabado posible es necesario abordar la presente cuestión desde dos miradas igual de importantes y complementarias entre sí: por un lado, una

mirada científico-tecnológica y, por otro, una mirada ius-filosófica.

### A. Aspectos Científico-Tecnológicos

La Inteligencia Artificial es una rama de la ciencia que busca imitar el comportamiento de seres vivos en búsqueda de lograr algoritmos<sup>1</sup> que tengan algún grado de inteligencia.

Entendemos por algoritmo a una secuencia ordenada y finita de instrucciones que permite resolver un problema. La cuestión de la inteligencia es más ambigua de definir, pero se pueden mencionar algunas categorías de algoritmos de IA que permiten hacerse una idea:

- Algoritmos de clasificación, que pueden determinar a qué categoría o clase pertenece un dato.
- Algoritmos de agrupamiento, que pueden reunir datos en grupos de acuerdo con características comunes a los mismos.
- Algoritmos de regresión, que pueden aproximar curvas, superficies, o funciones matemáticas en general, en base a puntos que formen parte o se encuentren en la cercanía de esta.
- Algoritmos de búsqueda de caminos, que permiten elegir un camino entre nodos de un grafo o un espacio geométrico.
- Algoritmos de aprendizaje automático que pueden ajustarse a dar una respuesta adecuada en base a ejemplos que se muestran en una etapa de “entrenamiento” o “aprendizaje”.
- Algoritmos de optimización, que permiten explorar soluciones a problemas que se pueden definir en términos de una función de puntaje objetivo, y buscan soluciones que maximicen (o minimicen) el valor de la misma.

Estas categorías son generales, y varios algoritmos pertenecen a más de una de estas categorías: es posible entrenar una red neuronal para clasificar imágenes con un entrenamiento de descenso del gradiente estocástico, optimizando su entrenamiento con una “función de error” especializada, o utilizar un algoritmo genético para ajustar los

---

<sup>1</sup> Elegimos hablar de algoritmos en general, ya que estos pueden representarse tanto como ecuaciones matemáticas, código, o circuitos. Es decir, un algoritmo es un ente abstracto que describe la solución a un problema, que podemos particularizar como fórmulas matemáticas, o tanto como software o hardware que lo implemente. Estas distintas representaciones del algoritmo tienen ventajas y desventajas: la formulación matemática puede ser interesante para buscar relaciones con otros problemas o simplificaciones desde lo teórico, el software puede llevarse a cualquier dispositivo computacional compatible, mientras que una implementación en hardware será extremadamente eficiente en rendimiento, pero poco flexible comparada con el software.



pesos sinápticos de la red, con una función de *scoring* adecuada al problema que se busca resolver. También se debe mencionar que hay algoritmos de otras ramas de la matemática o la informática que resuelven estos problemas, pero no son considerados algoritmos de Inteligencia Artificial.

Por ejemplo, el método de Mínimos Cuadrados es un algoritmo que puede considerarse tanto de regresión como de optimización, ya que permite tanto la aproximación de funciones como la búsqueda de parámetros óptimos para un problema. Sin embargo, no se lo considera un algoritmo de inteligencia artificial, como sí se considera a las redes neuronales o los algoritmos evolutivos. Esto sucede, entre otras razones, porque hay soluciones matemáticas directas que expresan el problema de manera determinada, y la solución al mismo consiste en completar las ecuaciones correspondientes y calcular el resultado. Tampoco se puede negar que el nombre del algoritmo tiene una cierta influencia, ya que tanto “redes neuronales” como “algoritmos evolutivos” evocan a cuestiones de la biología, en las cuales estos otros algoritmos están inspirados.

### B. Definiciones científicas de Inteligencia Artificial

Si bien Alan Turing en la década del 50 formuló la pregunta de si eventualmente las máquinas podrían emular el pensamiento [1], el concepto de Inteligencia Artificial tomó relevancia en la siguiente década gracias a gracias referentes como McCarthy, Shannon, Minsky, Papert, Rosenblatt, Widrow, Hoff, Weizenbaum, Sussman, por nombrar algunos. El Dr. Frank Rosenblatt fue uno de los pioneros en el tema de redes neuronales, partiendo del modelo de neurona de McCulloch-Pitts [2] y llevando adelante el desarrollo del Perceptrón [3], una implementación concreta de aquel modelo matemático de neurona, resultando en un clasificador binario o discriminador lineal capaz de generar una predicción basándose en un algoritmo simple: si el resultado de sumar el valor de todas las entradas de una neurona multiplicadas por los pesos sinápticos asociados a cada<sup>2</sup> una supera un valor umbral, entonces la neurona debe activarse. Una idea matemáticamente simple, elegante, y con un gran potencial.

Una característica fundamental de este momento histórico fue el gran optimismo de los investigadores. Los grandes avances iniciales y la formulación de soluciones a diversos problemas de esta naciente disciplina impulsó a creer que se iban a poder desarrollar sistemas de enormes capacidades en la siguiente década. La falta de cumplimiento ante las promesas de desarrollos cada vez más complejos y de enorme capacidad técnica, llevó eventualmente a lo que se denominó “invierno de la IA”. Esto volvería a pasar en los años 90. Pareciera ser una costumbre de la disciplina prometer soluciones a todos los problemas de un momento histórico en base a desarrollos (técnicamente impresionantes), y luego al no poder cumplir con las expectativas, generar el rechazo de las industrias, gobiernos e inversores. A estos múltiples desencantos también le debemos la multiplicidad de nombres con los que nos

referimos a estas técnicas: inteligencia artificial, inteligencia computacional, machine learning, deep learning, programación diferenciable, etc. Si bien pueden tener un significado técnico específico, muchas veces se usan como sinónimos para ocultar que en realidad estamos hablando de inteligencia artificial, con toda su historia de éxitos y fracasos, y también la experiencia que viene con ella.

De las varias definiciones de Inteligencia Artificial que se han propuesto a lo largo del tiempo, hemos seleccionado las siguientes para discutir los aspectos más relevantes que cada una destaca:

- Shirai y Tsujii indican que “El objetivo de la investigación sobre inteligencia artificial es conseguir que un ordenador llegue a realizar las importantes funciones de la inteligencia humana.” [4]. De la presente definición se resalta la vocación aspiracional de la Inteligencia Artificial: llegar a realizar las funciones de la inteligencia humana.
- Según Schalkoff, la Inteligencia Artificial es “Un campo de estudio que se enfoca a la explicación y emulación de la conducta inteligente en función de procesos computacionales.” [5]. La presente definición incorpora 2 elementos muy interesantes: la idea de emulación y el concepto de procesos computacionales. En razón de ella se podría concluir que la Inteligencia Artificial es un algoritmo que pretende imitar la conducta inteligente.
- Bartneck et al. definen a la Inteligencia Artificial como “la capacidad de un sistema para simular y realizar tareas que usualmente requerirían de la inteligencia humana, entre ellas, el razonamiento lógico, el aprendizaje y la resolución de problemas” [6]. De la presente definición es interesante resaltar que la pretensa emulación radica sobre el razonamiento lógico, el aprendizaje y la resolución de problemas; quedando fuera, por ejemplo, la inteligencia emocional y la capacidad de discernir, ambas propias de la inteligencia humana.
- Chollet define a la IA en general como “...un campo antiguo y amplio que generalmente puede entenderse como ‘todos aquellos intentos para automatizar procesos cognitivos humanos’” [7]. Luego desarrolla “*Machine learning* es un subcampo de la IA que apunta a automáticamente desarrollar programas (llamados *modelos*) puramente por exposición a datos de entrenamiento”. Finalmente define “*Deep learning* es una de las varias ramas del *machine learning* donde los modelos son largas cadenas de transformaciones geométricas, aplicadas una a continuación de la otra”. En esta definición, que puede parecer excesivamente simple, en realidad se hace evidente la crítica de Chollet a la exageración de los proponentes de la “IA para

---

<sup>2</sup> Toda esta operación, larga de describir en palabras, matemáticamente se resume en el concepto de producto punto entre dos vectores o matrices.

todo”. En concreto Chollet resalta la naturaleza matemática del *machine learning* en general y el *deep learning* en particular, criticando de lleno la humanización indebida de estas técnicas<sup>3</sup>.

- Por su parte, la OMPI (Organización Mundial de Propiedad Intelectual) define a la Inteligencia Artificial indicando que “generalmente, se considera una disciplina de la informática cuyo objetivo es el desarrollo de máquinas y sistemas que puedan llevar a cabo tareas para las que se prevé la necesidad de intervención de inteligencia humana” [8]. Por un lado, de dicha definición es interesante resaltar el término “generalmente”, lo cual da un indicio de que no hay unanimidad de criterios para definir a la Inteligencia Artificial. Por otro lado, de la definición surge el concepto de “máquina”, incorporando de esta manera, por ejemplo, a la robótica. También hace la siguiente mención, compleja y poco clara: “llevar a cabo tareas para las que se prevé la necesidad de intervención de inteligencia humana”; de esta última, quedan más preguntas que respuestas: ¿la Inteligencia Artificial es de naturaleza instrumental? ¿la Inteligencia Artificial sustituye a la Inteligencia Humana? ¿qué pasa con el desarrollo, el entrenamiento y la supervisión?

De las definiciones enumeradas podríamos concluir que la Inteligencia Artificial es una rama de la ciencia que busca imitar el comportamiento de los seres humanos mediante la implementación de algoritmos que tengan algún grado de inteligencia.

Cabe destacar que la descripción anterior recepta 3 conceptos que, a nuestra consideración, son esenciales respecto a su configuración y su finalidad.

- Hablamos de **algoritmos** de Inteligencia Artificial. Según la Real Academia Española, un algoritmo es un “Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema”<sup>4</sup>. En este sentido, la idea de “algoritmo” es un concepto más abarcativo que máquina u ordenador (aunque las regulaciones y bibliografías más modernas y actuales optan en su mayoría por el término “máquina”). La idea de algoritmo mantiene la idea de desmaterialización propia del software de computadoras. El concepto algoritmo también evita la idea de humanización de las máquinas o la reducción del pensamiento humano al concepto de inteligencia-máquina.

- La Inteligencia Artificial busca **emular o imitar** algunas de las funciones de la Inteligencia Humana, no todas. Al menos por ahora, como dice Bartneck et al. [6] o Fabio Morandín-Ahuerma [9] realiza las funciones del “razonamiento lógico, el aprendizaje y la resolución de problemas”. La Inteligencia Artificial carece de herramientas de inteligencia emocional, tampoco puede realizar valoraciones de bondad o maldad de los actos. La Inteligencia Artificial no cuenta con discernimiento. Por ello, la frase “algún grado de inteligencia”.
- Su naturaleza es **instrumental**. La Inteligencia Artificial es una herramienta al servicio de la humanidad, creada, modelada, entrenada y supervisada por personas humanas. En este mismo orden de ideas, y conforme lo esbozado por Borda, quien plantea que el “destinatario último y verdadero de los derechos y obligaciones es siempre el hombre” [10], podemos entender a la Inteligencia Artificial como una creación del hombre para que sea utilizada por el hombre, un bien de naturaleza instrumental, una herramienta.

### C. Persona y Sujeto de Derecho

Es de notorio conocimiento que cuando mencionamos el término “persona” nos referimos a aquel sujeto con la capacidad jurídica de adquirir derechos y contraer obligaciones.

Tradicionalmente este concepto fue vinculado al hombre, entendiéndolo como aquel ser gregario, “*Zoon Politikón*”<sup>5</sup>, que necesita de un otro para su crecimiento y desarrollo personal. Dicha necesidad se refleja en la tendencia natural del hombre a asociarse con otros, conformando así sociedades. De aquí surge la premisa de que no hay derecho sin un otro, un alter.

Con la evolución de la sociedad el concepto de persona también evolucionó, incorporando al concepto tradicional de persona a las organizaciones, las cuales son entendidas como aquel conjunto de personas que se reúnen con un fin u objetivo común. Así es que se da lugar al surgimiento de la persona jurídica o de existencia ideal.

Así es que actualmente que en nuestro ordenamiento jurídico encontramos 2 tipos de personas:

- Personas de existencia visible o personas humanas.
- Personas de existencia ideal o personas jurídicas.

Según el antiguo Código Civil Argentino, en su artículo 51, son personas de existencia visible “*todos los entes que presentasen signos característicos de humanidad, sin distinción de cualidades o accidentes*”, por su parte el artículo 19 nuestro actual Código Civil y Comercial y el artículo 4° de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), establecen que la persona humana comienza a ser centro de imputación de

---

<sup>3</sup> Invitamos a los lectores a leer en su totalidad el Capítulo 14 del libro “Deep Learning with Python”, 2da edición, donde Chollet no sólo desarrolla su crítica a esta mirada humanizante de la IA, sino que también demarca sus limitaciones, y esboza un camino hacia cómo podrían evaluarse en el futuro sistemas que exhiban formas más generales de inteligencia. Es de destacar que incluso los grandes modelos de lenguaje más avanzados a la fecha no logran obtener buenos puntajes en el benchmark “*Abstraction and Reasoning Corpus*” propuesto por Chollet.

<sup>4</sup> Consultado online en Enero 2024, link: <https://dle.rae.es/algoritmo>.

---

<sup>5</sup> Concepto creado por Aristóteles cuyo significado literal de la expresión es «animal político» o «animal cívico» y hace referencia al ser humano.

efectos jurídicos desde el momento de la concepción, entendida como la unión del gameto femenino y masculino.

Por su parte, las personas de existencia ideal son entes a los cuales el ordenamiento jurídico les confiere aptitud para adquirir derechos y contraer obligaciones para el cumplimiento de su objeto y la consecución de sus fines. En ningún caso serán constituidas para violar la ley, el orden público o la buena fe o para vulnerar derechos de cualquier persona.

Ahora bien, como menciona Borda [10]:

*“La persona no nace porque el derecho objetivo le atribuya capacidad para adquirir derechos y contraer obligaciones, sino que le reconoce esa capacidad porque es persona. En otras palabras, la persona no es un producto del Derecho, no nace por obra y gracia del Estado; es el “hombre de carne y hueso, el que nace, sufre y muere —sobre todo muere— el que come y bebe y juega y duerme y piensa y quiere”. Aun en las “personas jurídicas” el destinatario último y verdadero de los derechos y obligaciones es siempre el hombre porque el derecho no se da sino entre hombres. Por eso es que el Derecho, que no crea esas personas, tampoco podría desconocerlas ni menos aún crear arbitrariamente otras que no fueran el hombre o las entidades en que él desenvuelve sus actividades y sus derechos.”*

En este sentido, como afirma el autor antes citado el Estado mediante su ordenamiento jurídico no podría, o al menos no debería, crear arbitrariamente ficciones en las que el hombre no fuese el centro.

En este sentido, autores como Aftalión, establecen que sólo mediante un capricho del legislador podría atribuirse la calidad de persona a cosas, bienes o animales [11]; y refuerza *“haciendo ontología jurídica, se advierte que esa adjudicación de derechos es meramente nominal y que, siendo el derecho algo esencialmente humano, sólo los hombres son en verdad personas (sujetos de derecho)”*. La aclaración entre paréntesis pertenece a los autores.

Desde una mirada iuspositivista todo concepto de persona o sujeto de derecho es una creación legal normativa, una ficción. En dicha razón se fundamenta la posibilidad de establecer que ciertos objetos, elementos o bienes como ríos, ecosistemas, animales puedan ser considerados sujetos de derecho, “personas no humanas”.

Por su parte, desde una mirada iusnaturalista, el concepto de persona/sujeto de derecho es inescindible del ser humano, ya que existe una vinculación ontológica entre ellos, una cuestión sustancial. Así es que según Boecio retomando las ideas de Santo Tomás de Aquino define a la persona como *“unidad sustancial de naturaleza racional”*. De dicha definición surgen todas las dimensiones del ser humano, entre ellas, la socialidad, es decir: la necesidad de vivir en sociedad para resolver sus carencias y también perfeccionarse, principios fundantes del derecho.

#### D. Atributos de la personalidad

Desde una perspectiva normativa, de la definición de persona o sujeto de derecho definida en el título anterior se desprenden los atributos de la personalidad, es decir, aquellas cualidades, propiedades o características que distinguen a una persona física o jurídica de otra, brindando individualidad y

singularidad a cada una de ellas.

Entre los atributos de la personalidad encontramos aquellos comunes entre las personas físicas y jurídicas como el nombre, el domicilio, el patrimonio y la capacidad; y, por otro lado, el estado civil que sólo le es propio a las personas de existencia visible.

#### E. La capacidad

Ahora bien, a los efectos del presente trabajo es sumamente importante abordar el atributo de la capacidad, **cualidad inseparable de las personas**.

Se ha dicho con razón que es el más típico atributo de las personas: el que sirve precisamente para definir las como tales, desde el ángulo del derecho, porque es el único atributo que no sólo hace a la naturaleza sino también a la esencia de la personalidad.

A grandes rasgos existen dos tipos de capacidad: la capacidad de hecho o ejercicio, y la capacidad de derecho. La capacidad de derecho es aquella capacidad de adquirir derechos y contraer obligaciones; y, la capacidad de hecho o de ejercicio, que es la aptitud para ejercer por sí mismo los derechos.

Conforme menciona Lambías [12]: *“Sea que se trate de una u otra clase de capacidad, es siempre una aptitud del sujeto destinada a actuarse (actualizarse), es decir, a pasar de la potencia al acto”*.

#### F. ¿Qué implica ser capaz?

Según Llambías *“la capacidad se apoya en el discernimiento”*. Ahora bien, según la Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, Ciudad Autónoma de Buenos Aires, Sala E, en el caso “J.M. c/ G. de S., F. s/ Divorcio” (30/10/1991)<sup>6</sup>: *“No debe confundirse la capacidad con el discernimiento. La primera es la aptitud del sujeto para ser titular de relaciones jurídicas o para ejercer por sí mismo los derechos propios. El discernimiento es la cualidad o facultad del sujeto por la cual conoce y distingue lo bueno de lo malo, lo justo de lo injusto, lo conveniente de lo inconveniente. La capacidad sólo incide en la validez o invalidez del acto jurídico, en tanto que el discernimiento opera en un plano de mayor generalidad: su ausencia impide la imputación misma del acto el agente que si es su autor material, no resulta ser su autor moral”*.

El término discernimiento se forma a través del sufijo en latín *mentum* que significa “medio o instrumento” y discernir que también proviene del latín *discernere* y expresa “distinguir o separar”.

El discernimiento es el juicio por cuyo medio percibimos y declaramos la diferencia que existe entre varias cosas. El acto de discernir es una virtud ligada a un juicio moral que permite al individuo valorar si una acción es buena o mala. El discernimiento como juicio moral es la habilidad o capacidad que posee una persona para certificar o negar el valor moral de una determinada situación.

---

<sup>6</sup> El sumario de fallo puede ser accedido online en la siguiente URL: <http://www.saij.gob.ar/actos-juridicos-capacidad-discernimiento-suc0007378/123456789-0abc-defg8737-000csoiramus>.

Según Gonzalo Quintero [13], existe una tesis mayoritaria que considera que entre la inteligencia artificial y la inteligencia humana hay una diferencia ontológica insalvable, y lo que hacen las máquinas es imitar o simular procesos de razonamiento humano, y que en su más alto grado de desarrollo, no dejan de ser ingenios creados por la voluntad de las personas, por lo tanto, serían objeto pero no sujeto del derecho, y su presencia en el sistema legal se ha de acomodar a esa condición.

Ahora bien, es importante destacar, conforme lo mencionado, que la imitación que realiza la tecnología de los comportamientos humanos no es equivalente a la capacidad de pensar desde la teoría y la práctica experimentada por el hombre, mucho menos el discernimiento. *“El calificativo más cercano que se le podría añadir al tema de tecnología con autonomía es el de autómatas, lo que se refiera a un proceso que desde la tecnología imita la figura y los movimientos de un ser animado”*.

Por ello se puede afirmar que: *“los sistemas de inteligencia artificial como tecnologías en sí son amorales, no tienen capacidad para distinguir entre el bien y el mal, asumen la naturaleza de sus creadores. No será la tecnología en sí, la que acabará con las miserias humanas, tampoco dominarán el mundo, y mucho menos desde una visión catastrofista acabarán con el planeta, Internet de las Cosas no es quien pondrá en riesgo la privacidad del individuo, las armas y los denominados sistemas autónomos e inteligentes, son programados por el ser humano”* [14].

Según Ramos [15], *“la Inteligencia Artificial no tiene ni tendrá conciencia de sus actos, responsabilidad en el sentido humano, ni tampoco tendrá conciencia de sí misma, ni podrá percibir el sentido de los símbolos que une siguiendo una lógica para generar frases con sentido lógico como lo hace la inteligencia humana”*.

Si la Inteligencia Artificial contara con discernimiento que la asistiera en la comprensión de la bondad o maldad de los actos que realiza, esto podría acarrear la eventual reprochabilidad de su conducta y su consecuente responsabilidad, tanto civil como penal.

Así es que actualmente no existen condenas penales ni civiles que le atribuyan responsabilidad a la Inteligencia Artificial.

Como antecedente, siguiendo la presente línea de pensamiento, se encuentra el caso en Arizona, Estados Unidos en que un vehículo autónomo de Uber atropelló y quitó la vida a una persona que se encontraba cruzando la calle, en este caso la justicia acusó de homicidio culposo a la mujer que iba dentro del vehículo ya que la consideró “operadora de seguridad”. La fiscal del caso Rachel Mitchell consideró que *“Ponerse al volante de un automóvil es una responsabilidad seria. Independientemente de la tecnología que esté disponible para los conductores, la seguridad de todos en la calle y en el vehículo siempre debe ser la primera prioridad del conductor”*.

En esta línea de argumentación, el filósofo francés Eric Sadin establece que: *“la IA no es propiamente una inteligencia. El primer error que se comete habitualmente,*

*sostiene, es llamar inteligencia a lo que no lo es, esto es sólo un modo de racionalidad basado en esquemas restrictivos y que apuntan a satisfacer todo tipo de intereses”* [16]. Conforme expresa Ramos respecto de los dichos del filósofo: *“Sadin tiene razón porque la primera tarea que hay que emprender en el análisis de la IA es precisamente no dar por supuesto que el nombre implica una semejanza tal que, desde el vamos, se pueda confundir lo que una y otra forma de inteligencia realizan. Los que se plantean la posibilidad de aquella razón sea reemplazada por superada por esta nueva forma de construir conocimiento deberían comenzar por explicar lo que una y otra producen”*.

En conclusión, como dice Bartneck la Inteligencia Artificial procura imitar alguna de las funciones que realiza la Inteligencia humana, no todas. La Inteligencia Artificial nunca podrá tener sentimientos ni distinguir la maldad o bondad de sus actos, como dice Ramos “(...) la inteligencia humana tiene como tarea resolver cuestiones existenciales de mucho más valor”.

### III. DISCUSIÓN

#### A. Encuadre jurídico de la IA: ¿Bien que no es cosa?

En razón de la evolución económica y el surgimiento de la Industria 4.0, se ha concretado un proceso de desmaterialización plasmado en la economía de la información o del conocimiento, la cual ha dado lugar a la aparición y auge de los bienes “intangibles”.

Los bienes inmateriales, desde una perspectiva netamente económica, son un tipo de activo intangible con valor económico, es decir, son recursos inmateriales que una empresa adquiere para generar ganancias. Entre ellos identifica a los derechos emanados de la propiedad intelectual, como también los conocimientos técnicos y las habilidades estratégicas.

Por otro lado, desde una perspectiva netamente jurídica, los comentarios realizados al artículo 16 del Código Civil y Comercial de la Nación Argentina que refieren a los bienes intangibles como “Bienes que no son cosas”, establecen que: *“En la economía se ha verificado, en las últimas décadas, un fenómeno de desmaterialización, por el que los grandes negocios no se refieren ya a cosas, sino a “intangibles”, a valores económicos no materiales —como, por ejemplo, los derechos sobre determinada idea útil para la producción de bienes y servicios—. También en el Código Civil y Comercial se regulan las obligaciones relativas a bienes que no son cosas (art. 764 y concs. CCyC) y los contratos habitualmente empleados para su transmisión (por ejemplo, cesión, factoraje, etc.)”*. De dichas afirmaciones se puede concluir que se mantiene la clasificación tradicional de bienes, otorgándole al concepto de “cosa” la característica atributiva de la materialidad o tangibilidad, y al “bien que no es cosa” la característica atributiva de la “desmaterialización” o intangibilidad.

Los denominados “bienes intangibles” o “bienes que no son cosas” son aquellos que no son cosas materiales y se encuentran enmarcados dentro de las diversas normativas de Propiedad Intelectual.

Según *World Intellectual Property Organization* (WIPO-OMPI): “La propiedad intelectual se refiere al conjunto de derechos legales que protegen las creaciones de la mente humana, tales como invenciones, obras literarias y artísticas, diseños y símbolos, nombres y emblemas utilizados en el comercio”.

La Inteligencia Artificial, conforme fue definida en el apartado científico-tecnológico, es un algoritmo que pretende imitar algunas de las funciones de la inteligencia humana. Un Algoritmo que se traduce en un sistema operativo, un software, un programa de computadora, es decir: un bien inmaterial, un intangible, un bien que no es cosa.

La Inteligencia Artificial, como todo bien intangible es susceptible de ser abordada, protegida y enmarcada dentro de las diversas normativas de Propiedad Intelectual vigentes tanto a nivel nacional, regional como internacional.

En este sentido, a continuación, detallaré aquella normativa que enmarcaría a la Inteligencia Artificial dentro de los plexos normativos antes señalados de la Propiedad Intelectual:

- El Convenio de Berna de 1971 para la Protección de las Obras Literarias y Artísticas regula el caso de los Programas de ordenador. Los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2° del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión.
- El Acuerdo de Aspectos de los Derechos de Propiedad Intelectual relacionados al Comercio (ADPIC/TRIPS) de 1994 retoma el abordaje del Convenio de Berna y regula en su Artículo 10: “Programas de ordenador y compilaciones de datos. 1. Los programas de ordenador, sean programas fuente o programas objeto, serán protegidos como obras literarias en virtud del Convenio de Berna (1971). 2. Las compilaciones de datos o de otros materiales, en forma legible por máquina o en otra forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, serán protegidas como tales. Esa protección, que no abarcará los datos o materiales en sí mismos, se entenderá sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales en sí mismos”.
- Tratado de la OMPI sobre Derecho de Autor (WCT) del año 1996 trata la protección de las obras y los derechos de sus autores en el entorno digital siguiendo la línea del artículo 2° del Convenio de Berna y, especialmente en su artículo 4°, regula a los “programas de computadora, con independencia de su modo o forma de expresión como a las compilaciones de datos u otros materiales (“bases de datos”)” como bienes intangibles susceptibles de ser protegidos por el derecho de autor.
- Por su parte nuestro Régimen de Propiedad

Intelectual, normado mediante la ley N°11.723, en su artículo 1° enumera los bienes susceptibles de protección por derecho de autor: “A los efectos de la presente Ley (...) las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales; (...) en fin, toda producción científica, literaria, artística o didáctica sea cual fuere el procedimiento de reproducción.”

- Por otro lado, la ley de Patentes de Invención y Modelos de Utilidad de Argentina, en su artículo 6°, establece que: “No se considerarán invenciones para los efectos de esta ley: (...) c) Los planes, reglas y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económico-comerciales, así como los programas de computación (...)”.

Conforme lo expuesto podemos concluir que la Inteligencia Artificial dada su caracterización científico-tecnológica y los institutos jurídicos y normativa vigente, es un bien intangible susceptible de ser protegido y regulado mediante el derecho de autor.

Como menciona Diego Alejandro Morales Oñate (2021): “son dos los requisitos para que las creaciones del intelecto puedan ser consideradas obras: a) la originalidad;12 y, b) que sea susceptible de ser expresada, reproducida o divulgada por cualquier forma o medio conocido o por conocerse. Al respecto, se puede considerar que el algoritmo se encuentra plasmado en un soporte reproducible, divulgable, como podría ser la misma documentación técnica base de un programa; en este caso, se consideraría al algoritmo una obra protegible por el derecho de autor” (...) “El algoritmo, para ser considerado como obra debe ser original y susceptible de expresión; por tanto, si el algoritmo es apto de ser reproducido o divulgado puede ser considerado como obra protegible por sí mismo, de manera independiente”.

Conforme lo plasmado, a la Inteligencia Artificial, como bien intangible protegido por el derecho de autor, le serán aplicables todos los principios rectores de dicho instituto: su caracterización, la atribución de la titularidad, los derechos y obligaciones emergentes para sus titulares, la duración del monopolio legal creado a los efectos de su explotación, las excepciones y flexibilidades, y también las responsabilidades emergentes por su uso y goce.

#### IV. CONCLUSIONES Y TRABAJO FUTURO

Entonces, ¿puede la inteligencia artificial, en sus múltiples formas, ser considerada persona o sujeto de derecho? ¿O tal vez alguna variante lo suficientemente compleja?

En principio, consideramos que no debiera considerarse persona o sujeto de derecho a la IA, y esta afirmación no se basa en ninguna medida o métrica de complejidad. La Inteligencia Artificial actual, en todas sus formas y variantes, no es más que una imitación simplista de la inteligencia humana (o biológica, si consideramos algunas variantes).

Las redes neuronales, por razones históricas, llevan un



nombre grandioso para lo que es tan sólo un burdo modelo matemático de sus contrapartes biológicas: simplemente resumen todas las cuestiones biológicas, químicas y físicas implicadas en su funcionamiento en un producto punto entre vectores. En realidad, lo más sorprendente de las redes neuronales<sup>7</sup> es que aún en la simplicidad de sus fundamentos técnicos y teóricos, gracias a la escala a la que el *hardware* moderno y la enorme disponibilidad de datos de entrenamiento nos permiten entrenar y operar estos modelos, logran exhibir un comportamiento tan complejo que es capaz de confundir a una gran parte de la sociedad.

Si en lugar de redes neuronales la discusión fuera sobre “aprendizaje por representaciones jerárquicas” o “transformaciones geométricas encadenadas” (sinónimos sugeridos por François Chollet), difícilmente podría realizarse el salto de imaginación requerido para atribuirle atributos o capacidades humanas a una gran pila de fórmulas y parámetros ajustados de acuerdo con el descenso por el gradiente de una superficie multidimensional, descrita de manera ruidosa por una interminable cantidad de ejemplos de entrenamiento, o variantes aumentadas de los mismos.

Enfrentados contra esta realidad excesivamente matemática de la “inteligencia de las máquinas” (o acaso la mejor aproximación de eso que hemos logrado desarrollar hasta ahora), debiera ser cada vez más evidente que ésta carece de consciencia, discernimiento y capacidad en términos jurídicos.

No hay en estos ninguna aptitud jurídica que les permita adquirir derechos o contraer obligaciones. Estas aptitudes solo le son propias, directa o indirectamente, a los seres humanos. De momento consideramos que la naturaleza jurídica de la Inteligencia Artificial es configurarse como un bien intangible, que puede ser protegido por la propiedad intelectual, y es de carácter instrumental.

No creemos haber encontrado una solución definitiva y duradera al debate que hemos planteado en este trabajo, pero si buscamos despejar algunas cuestiones que se tratan de imponer como novedosas cuando en realidad ya contamos no sólo con el conocimiento científico para discutirlos en un marco teórico adecuado, sino también con andamiaje jurídico suficiente para enmarcarlas adecuadamente.

Sin duda el desarrollo de la tecnología, la reacción de la sociedad a la incorporación creciente de Inteligencia Artificial en cada vez más ámbitos, el avance y resolución de casos emblemáticos respecto de IA y diversos aspectos del derecho, y la eventual reglamentación de este tipo de sistemas en cada vez más países del mundo, nos aseguran que será necesario, más temprano que tarde, volver a discutir los temas que se plantearon en este trabajo.

## V. AGRADECIMIENTOS

Agradecemos a la Universidad FASTA, y el Ministerio Público Fiscal de la Provincia de Buenos Aires, por su apoyo

constante al Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, sin el cual este trabajo no hubiera sido posible, en particular a Roberto Giordano Lerena y Mónica Pascual.

Agradecemos los aportes, ideas, discusiones e intercambios con los integrantes del proyecto de Sistematización y Producción de Conocimiento en Inteligencia Artificial y Evidencia Digital (SPICA), en particular Josefina Riva Posse, Valentina Fernández, Enzo Nogueira, Santiago Trigo, Leonela Pancani y Juliana Huarte. Agradecemos también a Juan Ignacio Iturriaga por sugerencias e intercambios que ayudaron a mejorar este trabajo.

## VI. REFERENCIAS

- [1] A. M. Turing. (1950, Octubre). Computing Machinery and Intelligence. Mind, Volumen LIX, Nro. 236, ps. 433–460, DOI: <https://doi.org/10.1093/mind/LIX.236.433>.
- [2] W. S. McCulloch, W. Pitts (1943). A logical calculus of the ideas immanent in nervous activity. Bulletin of Mathematical Biophysics 5, ps. 115–133. DOI: <https://doi.org/10.1007/BF02478259>.
- [3] F. Rosenblatt, “The Perceptron A Perceiving and Recognizing Automaton (Project PARA)”. Cornell Aeronautical Laboratory, Inc. Buffalo, N.Y., Enero 1957.
- [4] Y. Shirai, J. Tsujii, *Artificial Intelligence: Concepts, Techniques and Applications*, Wiley (1984), traducción de la edición original de Japón (1982).
- [5] R. J. Schalkoff, *Artificial Intelligence: An Engineering Approach*, McGraw-Hill Education (1990).
- [6] C. Bartneck, C. Lütge, A. Wagner, S. Welsh, “What is AI?,” in *An Introduction to Ethics in Robotics and AI*, 1ra ed., SpringerBriefs in Ethics, Suiza, 2021, c. 2, sec. 1, pp. 7–12.
- [7] F. Chollet, *Deep Learning with Python, 2<sup>nd</sup> Edition*, Manning Publications Co. (2021).
- [8] *Preguntas Frecuentes: IA y Políticas de PI*, Organización Mundial de la Propiedad Intelectual. Accedido en Enero 2024, disponible online: [https://www.wipo.int/about-ip/es/artificial\\_intelligence/faq.html](https://www.wipo.int/about-ip/es/artificial_intelligence/faq.html).
- [9] F. Morandín-Ahuerma. (2022). ¿Qué es Inteligencia Artificial?. Int. J. Res. Publ. Rev, Vol. 3, Nro. 12, ps. 1947-1951.
- [10] G. A. Borda, “Tratado de Derecho Civil. Parte General, Tomo I”. Abeledo-Perrot, 1999.
- [11] E. R. Aftalión, J. Villanova, J. Raffo, “Introducción al Derecho”, Abeledo-Perrot, 1972.
- [12] J. J. Llambías, “Tratado de Derecho Civil. Parte General. Tomo I.” Editorial Emilio Perrot, 1960.
- [13] G. Quintero Olivares, “La robótica ante el Derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas”. Revista Electrónica de Estudios Penales y de la Seguridad, n.º 1, 2017.
- [14] J. Bossman, “Top 9 ethical issues in artificial intelligence”, World Economic Forum, Octubre 2016. Disponible online: <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/>.
- [15] A. Ramos. (2022). ¿Inteligencia Artificial vs Inteligencia Humana?. In *Itinere*, Vol. 12, Nro. 1.
- [16] E. Sadin, “La artificial o el desafío del siglo”, Caja Negra, 2020.

## VII. BIOGRAFÍAS



**Antonela D'Onofrio** es Abogada y Profesora de Nivel Superior por la Universidad FASTA, y actualmente se encuentra finalizando una Maestría en Propiedad Intelectual en FLACSO. Es investigadora del InFo-Lab, y tiene una extensa carrera académica como investigadora en temas de Derecho y Tecnología, y actualmente está participando en investigaciones sobre Inteligencia Artificial y Derecho.

<sup>7</sup> Y todas las variantes modernas como las redes convolucionales, *autoencoders* varios, GANs, LSTM, redes recurrentes, modelos de difusión, y Transformers. Esta enumeración dista de ser exhaustiva, meramente enunciamos los modelos que en los últimos meses han estado en boga.

**Lucía Algieri** es Licenciada en Criminalística por la Universidad FASTA, y se encuentra terminando sus estudios de Abogacía en la misma Universidad. Desde el año 2018 forma parte del InFo-Lab donde investiga temas de Informática Forense y Evidencia Digital. Actualmente está participando en grupos de investigación donde se investiga y desarrollan aplicaciones de Inteligencia Artificial para analizar y procesar Evidencia Digital, y la interacción de estas nuevas tecnologías con el Derecho y la Justicia.



**Ana Haydée Di Iorio** es Ingeniera en Informática por la Universidad FASTA y Especialista en Gestión de la Tecnología y de la Innovación por la Universidad Nacional de Mar del Plata. Desde el año 2014 dirige el InFo-Lab y tiene una extensa carrera como Perito Informática, y como investigadora académica en temas de Informática Forense. Ha dirigido y participado múltiples proyectos de I+D+i en Informática Forense, Evidencia Digital, Informática y Derecho, entre otras temáticas.



**Bruno Constanzo** es Ingeniero en Informática por la Universidad FASTA. Desde el año 2014 forma parte del InFo-Lab donde investiga temas de Informática Forense, Evidencia Digital, y el uso de Inteligencia Artificial para pericias y análisis de evidencia digital. Cuenta con una extensa carrera como investigador académico en estos temas, y ha participado en múltiples proyectos de I+D+i en la temática. Ha realizado aportes a librerías y proyectos de software libre ampliamente utilizados en el área de informática forense.





# PRIVACIDAD DE DATOS EN APLICACIONES DE SISTEMAS IOT PARA SMART CITIES: UNA REVISIÓN SISTEMÁTICA

Pamela Hermosilla, *Miembro, Pontificia Universidad Católica de Valparaíso*, Ivo Cattarinich, *Miembro, Pontificia Universidad Católica de Valparaíso*, Ignacio Rojas, *Miembro, Pontificia* and Sebastián Berrios, *Miembro, Pontificia Universidad Católica de Valparaíso*.

**Abstract-** The Internet of Things (IoT) is a rapidly evolving technology that interconnects physical objects through communication networks, facilitating data collection and sharing for improved decision-making and efficiency across sectors. However, the extensive collection of personal data without consent raises privacy concerns and exposes individuals to data misuse. This systematic review aims to determine the most suitable technologies for protecting personal data, identifying vulnerabilities in the application of IoT systems in the context of smart cities. To achieve this, existing literature on data privacy in IoT systems was analyzed, based on searches in the WoS and Scopus databases, and 15 relevant studies addressing different aspects of data privacy were selected. The review's findings revealed that data privacy in IoT systems is an active and evolving research area. Various techniques and approaches were found to protect data privacy in IoT environments. Finally, key considerations related to data privacy protection in implementing IoT systems were identified, such as managing large volumes of data generated by IoT devices, system interoperability, and the reconciliation between privacy and data utility. This review can serve as a foundation for future research and developing more effective solutions for protecting data privacy in IoT systems.

**Keywords:** IoT, privacy, smart cities, data protection, data collection.

## I. INTRODUCTION

La necesidad de crear un mundo conectado que ofrezca servicios y procesos más eficientes nos ha llevado a compartir un gran volumen de datos de forma poco consciente en determinadas situaciones. Los nuevos sistemas de organización del transporte público, el control del tráfico vehicular o la eficiencia energética en edificios, tienen como factor común la recopilación de datos personales. Los sensores que miden y controlan la actividad en las ciudades trabajan bajo el concepto de Internet de las Cosas (IoT), que recopilan información y la envían a un sistema centralizado en la nube donde se procesan y toman decisiones en tiempo real.

La tecnología IoT es utilizada como base fundamental del funcionamiento de las ciudades inteligentes o Smart Cities. Se considera a una ciudad como inteligente cuando ha integrado

una infraestructura de tecnologías de información y comunicaciones (TIC), el análisis de datos y el control en tiempo real [1]. En una ciudad inteligente los dispositivos y sensores proporcionan datos que permiten conocer el comportamiento de una ciudad y los movimientos que se presentan en ésta. Un tratamiento adecuado de los datos permitiría adaptar y potenciar bienes y servicios requeridos para cubrir las necesidades de las personas. En el caso de Las Vegas, Estados Unidos, han trabajado en potenciar principalmente el ámbito del transporte, el uso de las energías, las obras áreas públicas y la seguridad, lo cual sustenta mediante la transmisión de datos por medios abiertos, realizando análisis de datos en tiempo real, lo que permite apoyar de manera eficiente y expedita la toma de decisiones oportuna. Este enfoque establece una alianza del sector público-privado, para resguardar tanto la seguridad de personas como de la información y su disponibilidad [2].

La ciberseguridad en IoT es una preocupación creciente, ya que los dispositivos IoT se conectan cada vez más a Internet. Estos dispositivos recopilan y comparten una gran cantidad de datos personales, que pueden ser vulnerables a ataques cibernéticos.

Los riesgos de ciberseguridad en IoT incluyen el robo de datos, los ataques DDoS, el acceso no autorizado, la manipulación de dispositivos y las vulnerabilidades de software. Estos riesgos pueden afectar a las personas de diversas maneras, desde la pérdida de privacidad hasta la seguridad física. Para mitigar estos riesgos, es importante que las organizaciones que desarrollan y utilizan sistemas IoT implementen medidas de seguridad básicas, como el cifrado de datos, la autenticación multifactor y las actualizaciones de software. También es importante que los usuarios estén informados de los riesgos de ciberseguridad y de las medidas de protección que pueden adoptarse.

Por lo cual sistemas IoT presentan riesgos de ciberseguridad que pueden afectar a las personas, desde la pérdida de privacidad hasta la seguridad física. Es importante que las organizaciones y los usuarios implementen medidas de seguridad para mitigar estos riesgos.

En Asia, en la ciudad de Seúl, en Corea del Sur, es posible apreciar una serie de iniciativas que han permitido ir incorporando TIC en distintos ámbitos de su quehacer, lo que la llevado a reconocerla como Smart Seoul Network (S-Net), este sistema se caracteriza por el acceso a Internet de todos sus ciudadanos, a través de la implantación de una banda ancha impartida por los municipios, potenciando las redes Wi-Fi de libre acceso. Se ha requerido de una infraestructura tecnológica adecuada para consolidar la integración a través de los dispositivos Long Range (LoRa), tecnología ideada para conexiones a grandes distancias en redes de IoT en las que se necesiten sensores que no dispongan de corriente eléctrica de red [3]. A nivel sudamericano, la ciudad de Rio de Janeiro (Brasil) el plan de implementación reúne estratégicamente proyectos que fortalecen la integración de los ciudadanos y el gobierno, considerado servicios que se enmarcan en un centro de operaciones local, el que entrega monitoreo, inclusión digital, lo que se traduce en un indicador clave para conocer y medir la brecha y analfabetismo digital principalmente de los sectores más desprovisto de TIC [4]. A partir de los antecedentes presentados, no se ha observado un planteamiento claro para el tratamiento de datos y el resguardo de la privacidad de las personas, al integrar tecnologías en el desarrollo de ciudades inteligentes, lo que representa un espacio de contribución interesante en cuanto a la arquitectura tecnológica adecuada y un marco de trabajo estándar para el tratamiento de datos y la protección de la privacidad. Además, la complejidad de los sistemas de ciudades inteligentes y la rápida evolución de las tecnologías utilizadas, representan la necesidad de crear estándares de buenas prácticas entre los diferentes actores involucrados, en cuanto a la recopilación y procesamiento de los datos.

Las Smart Cities, ya sea construidas desde sus inicios o adaptadas a la tecnología actual, basan su funcionamiento en IoT, por lo que se hace necesario abordar en su diseño y planificación aspectos de privacidad, identificando los sensores que en definitiva captarán los datos, para definir las tecnologías requeridas para el resguardo de éstos. Por lo tanto, se ha planteado para esta revisión responder la siguiente pregunta que guiará el estudio, y que dice relación con determinar ¿Cómo resguardar la privacidad de los datos recopilados por los sistemas basados en IoT en una ciudad inteligente?

El propósito de esta revisión es determinar las tecnologías disponibles para la protección de los datos personales a partir de la identificación de puntos vulnerables en la aplicación de sistemas IoT. Se busca evaluar las medidas de seguridad existentes y determinar qué soluciones pueden ser aplicadas para salvaguardar la privacidad de los usuarios. Esta revisión permitirá establecer un marco de referencia para el desarrollo de estrategias de protección de datos en el contexto de los sistemas IoT, promoviendo así la confianza y seguridad en el uso de estas tecnologías. Esta revisión se centra en dar respuesta a la interrogante de investigación planteada a través de una revisión sistemática, para lo cual se han considerado como referencia 15 artículos publicados entre 2018 y 2023 en

las plataformas WoS y Scopus bajo conceptos como privacidad de datos en Smart Cities, recolección de datos en sistemas IoT y protección de datos. La revisión tendrá un enfoque de análisis descriptivo el que permitirá indagar en el área de estudio y realizar una síntesis cualitativa de los aspectos más relevantes identificados. El estudio se estructura comenzando con una descripción detallada de la metodología empleada para esta revisión, abarcando desde la recolección hasta la selección de artículos, siguiendo las pautas de Prisma 2020 [5]. Este proceso metodológico nos lleva a la identificación de los elementos clave relacionados con las interrogantes planteadas en la investigación. Como consecuencia, se destacan los aspectos cruciales para la implementación de sistemas IoT que priorizan la protección de la privacidad de los usuarios, subrayando la importancia del enfoque de privacidad desde el diseño, técnicas de anonimización y la capacidad de los individuos para gestionar sus propios datos.

## II. METODOLOGÍA

La metodología de investigación establecida para esta revisión busca dar respuesta a las principales interrogantes que guían este estudio, las que se enmarcan en indagar y responder siguientes preguntas de investigación (PI):

- PI 1: ¿Qué sistemas IoT para Smart Cities recopilan datos personales?
- PI 2: ¿A qué tipos de riesgos se exponen las personas al interactuar con sistemas IoT?
- PI 3: ¿Qué tecnologías son utilizadas para resguardar la privacidad de los datos personales?

Se entenderá como datos personales los que se refieren a antecedentes propios de cada individuo, relacionado con el nombre y apellidos, dirección, número de documento de identidad, dirección de protocolo de internet (IP), número de teléfono, correo electrónico, orientación sexual, origen racial o étnico, datos genéticos o biométricos y geolocalización.

Para abordar adecuadamente las interrogantes planteadas, se han identificado dos etapas, la primera de ellas se enfoca en definir los conceptos claves que permitirán seleccionar el conjunto de artículos que serán sometidos a revisión, mientras que la segunda etapa considera un análisis realizado por el equipo de investigación, para determinar los principales aspectos en materia de privacidad de datos para aplicaciones de sistema IoT. En la

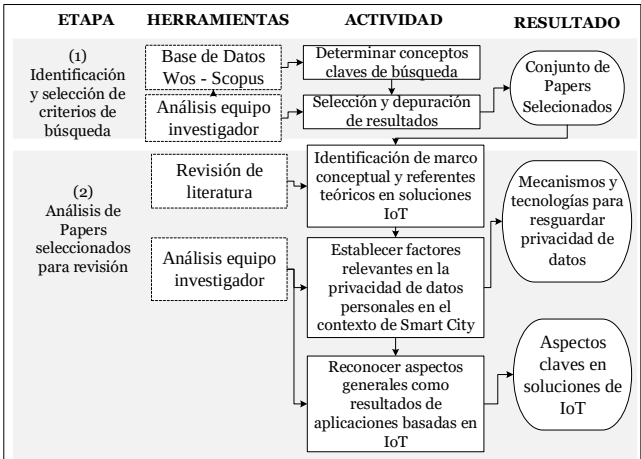


Figura 1 se puede apreciar la representación de la metodología de investigación propuesta, en la cual es posible identificar las etapas con sus herramientas, actividades y resultados. A partir de la indagación de los artículos revisados se establecen los aspectos relevantes de privacidad para la implantación de sistemas IoT y se plantean aspectos generales de los resultados, logrando establecer categorías para comparar alcances y aportes interpretando similitudes y diferencias.

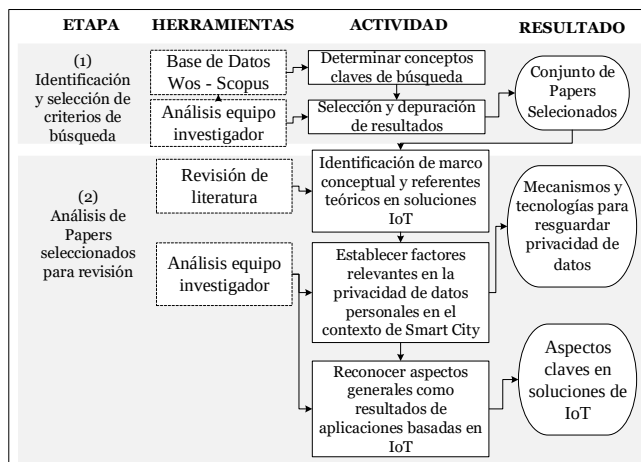


Figura 1. Metodología de Investigación

La metodología de investigación de esta revisión sistemática se ha basado en PRISMA 2020, la cual es una guía actualizada diseñada para mejorar la transparencia y claridad en la publicación de revisiones sistemáticas y metaanálisis. PRISMA, que significa "Preferred Reporting Items for Systematic reviews and Meta-Analyses", cuyo objetivo es ayudar a los autores a documentar de manera detallada y transparente el proceso de revisión, incluyendo la justificación, metodología, y hallazgos. La versión de 2020 actualiza y reemplaza la declaración PRISMA de 2009, reflejando los avances en la metodología y terminología de las revisiones sistemáticas. Incluye un conjunto de elementos basados en evidencia para el reporte en revisiones sistemáticas y metaanálisis, enfocándose principalmente en la evaluación de efectos de intervenciones. PRISMA 2020 introduce nuevas orientaciones para el reporte que abarcan los avances en los métodos para identificar, seleccionar, evaluar y sintetizar estudios.

### III. ESTRATEGIA DE BÚSQUEDA

#### A. Criterios de Búsqueda

Para la selección de los artículos científicos se utilizaron las bases de datos WoS y Scopus, realizando diversas consultas para la búsqueda de artículos que revisan los conceptos relevantes que contribuyan a responder las preguntas de investigación presentadas, y que entreguen antecedentes importantes, relacionados a la recopilación y protección de datos en sistemas IoT.

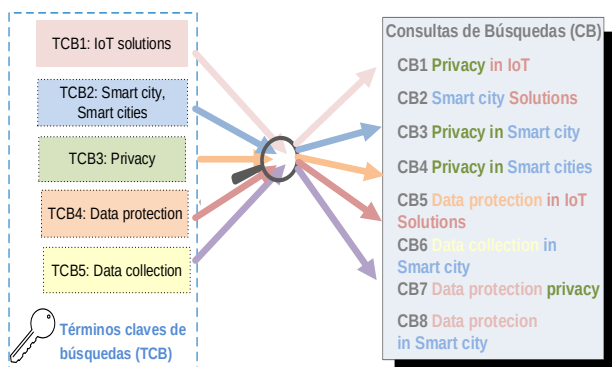


Figura 2. Términos clave de búsqueda – Consultas de búsquedas

Para focalizar las búsquedas a realizar, se definieron primeramente términos claves de búsquedas (TCB), los cuales se combinaron para generar las consultas de búsquedas (CB), las que finalmente guiaron la búsqueda en las bases de datos mencionadas. En figura 2 es posible distinguir los términos clave y criterios de búsqueda utilizados para el desarrollo de esta revisión.

A partir de lo anterior, para una primera iteración de búsquedas, se definieron los siguientes criterios inclusión (CI) y criterios de exclusión (CE):

|    |   |                       |                                                                                                                                                                                                                                                                                                                          |
|----|---|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CI | 1 | Área de conocimiento: | Computer Science Information Systems or Computer Science Artificial Intelligence or Automation Control Systems or Computer Science Hardware Architecture or Engineering Electrical Electronic or Ethics or Green Sustainable Science Technology or Information Science Library Science or Robotics or Telecommunications |
| CI | 2 | Idioma:               | Inglés                                                                                                                                                                                                                                                                                                                   |
| CI | 3 | Tipo de documento:    | Article, Conference papers                                                                                                                                                                                                                                                                                               |
| CE | 1 | Año:                  | <=2018 (5 años de vigencia)                                                                                                                                                                                                                                                                                              |
| CE | 2 | Palabras clave:       | "Ethics", "law", "laws", "legislation"                                                                                                                                                                                                                                                                                   |

Como resultado de las primeras búsquedas, para cada uno de los sets de artículos encontrados en base de datos WoS y Scopus, se aplicó un algoritmo para eliminar los registros repetidos, no obstante, se obtuvieron cantidades de artículos superiores a las requeridas para este estudio, por lo que se aplicó un nuevo refinamiento que consideró: eliminación de artículos con utilización de encuestas, se acotó el periodo de años de 10 a 5, se excluyeron los referidos al ámbito de salud por considerarse muy específico para el objetivo de esta investigación, por otro lado se consideraron principalmente los que fueran open Access y los que contuvieran los términos security o privacy en el título.

Finalmente, aplicando estos últimos criterios de exclusión anteriormente, se ordenaron los artículos resultantes según la cantidad de citaciones de éstos, de los cuales se seleccionaron para la revisión los 15 más citados, y se dejan los primeros de 7 Scopus y los 8 primeros WoS, de tal forma de cubrir ambas fuentes de datos de forma balanceada y representativa. La Figura 2 representa el esquema general de búsqueda y selección de artículos considerados para el desarrollo de esta revisión, donde se puede apreciar el detalle de lo mencionado y las cantidades de artículos obtenidos.

#### B. Categorías de Análisis

Para llevar a cabo la revisión de los artículos seleccionados, es importante establecer las categorías de análisis que se utilizarán. Estas categorías se basarán en las preguntas que guían este estudio de investigación. El propósito de estas categorías es dirigir y estructurar el proceso de análisis,

enfocándolo en la búsqueda de respuestas específicas. Esto permitirá una organización más efectiva de la información recopilada y facilitará la extracción de conclusiones relevantes.

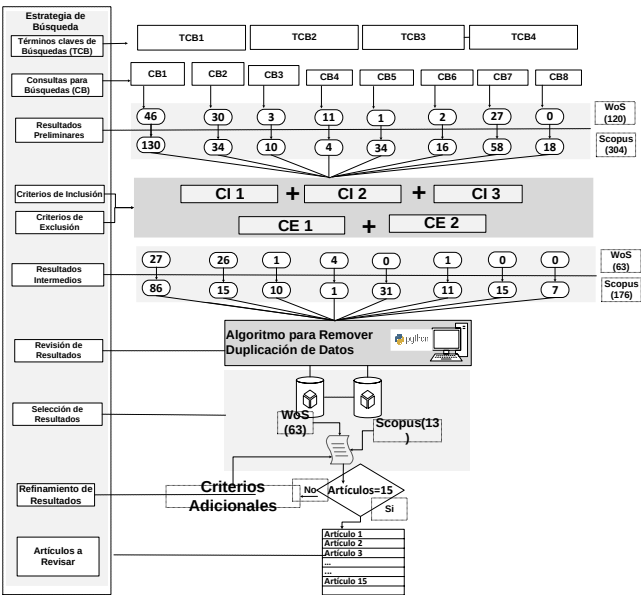


Figura 2.Estrategia de búsqueda y selección de artículos.

Se identificaron 4 categorías de análisis: aplicaciones de IoT, riesgos asociados a la recopilación de datos en sistemas IoT, tecnologías para la protección de datos y modelos de tratamiento de datos. La primera categoría busca explorar los diferentes campos de aplicación de los sistemas IoT para tener una visión general de su alcance y uso. Sin embargo, estas aplicaciones también plantean riesgos en términos de seguridad y privacidad, ya que los sistemas IoT pueden ser vulnerables a ataques cibernéticos, robo de datos personales y violaciones de la privacidad, lo cual será analizado en la segunda categoría. Por otro lado, la tercera categoría se enfoca en investigar las tecnologías disponibles para proteger los datos recopilados y transmitidos por los dispositivos IoT, como técnicas de cifrado, autenticación, control de acceso y gestión de claves. Por último, la cuarta categoría aborda la necesidad de establecer modelos de tratamiento de datos que permitan a los usuarios tener un mayor control sobre su información, garantizando un uso adecuado de los datos recopilados. Estos modelos consideran tecnologías para resguardar la privacidad de los datos en los dispositivos IoT, así como en su transmisión, almacenamiento y posterior procesamiento. Lo anterior se representa en el esquema de la siguiente figura.

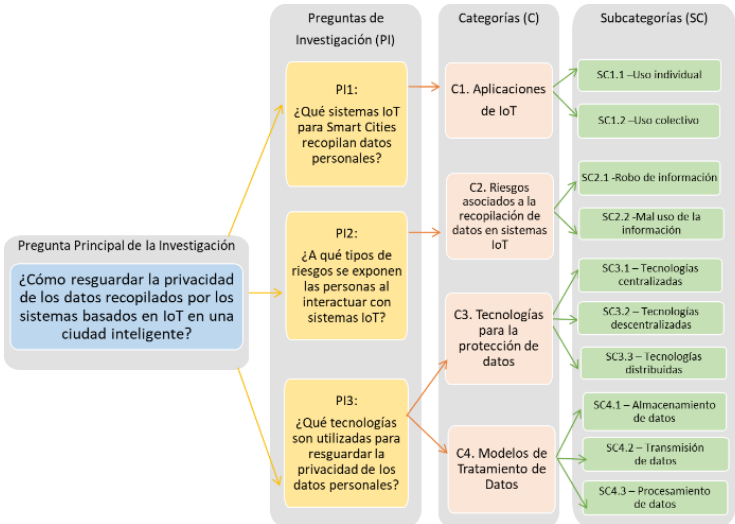


Figura 3. Esquema de categorías y subcategorías según preguntas de investigación.

#### IV. RESULTADOS

En esta sección se presentarán inicialmente los resultados en cuanto a las características generales de los artículos revisados, de forma de tener una visión general de la cobertura demográfica y temporal de lo abordado en esta revisión. Posteriormente, se señalarán los principales hallazgos identificados a partir del análisis de las categorías mencionadas previamente, estableciendo además aspectos transversales en lo revisado, en cuanto a las subcategorías identificadas. Finalmente, se entregará una síntesis de este apartado, señalando lo más relevante de los hallazgos de esta investigación.

##### A. Principales características de artículos seleccionados

En este apartado se muestran los principales resultados de los 15 artículos sometidos a revisión en este estudio [6-20] **Error! Reference source not found.**, para lo cual se identificó inicialmente sus principales características, luego se describen los hallazgos más relevantes acorde a las categorías de análisis definidas anteriormente. Finalmente se entrega una síntesis del resultado de esta investigación.

TABLA 1: Listado de papers revisados

| Título                                                                                                                | País/Año        |
|-----------------------------------------------------------------------------------------------------------------------|-----------------|
| Protecting Location Privacy in IoT Wireless Sensor Networks through Addresses Anonymity [6]                           | China/ 2022     |
| Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments [7] | China/ 2022     |
| Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hash Function [8]                             | Australia/ 2022 |
| Realizing Efficient Security and Privacy in IoT Networks [9]                                                          | China/ 2020     |
| Method to implement K-NN machine learning to classify data privacy in IoT environment [10]                            | IRAQ/ 2020      |
| A Trust-based Security System for Data Collecting in Smart City [11]                                                  | China/ 2020     |
| Searchable Encryption Scheme for Personalized Privacy in IoT-Based Big Data [12]                                      | China/ 2019     |
| Authentication and Key Management in Distributed IoT using Blockchain Technology [13]                                 | India/ 2021     |
| A Regulatory View on Smart City Services [14]                                                                         | Croacia/ 2019   |
| Security and privacy for mobile IoT applications using blockchain [15]                                                | Portugal/ 2021  |
| An efficient dummy-based location privacy-preserving scheme for internet of things services [16]                      | China/ 2019     |
| Smart City IoT Services Creation Through Large-Scale Collaboration [17]                                               | Italia/ 2020    |
| A Methodological Framework for the Selection of Key Performance Indicators to Assess Smart City Solutions [18]        | Grecia/ 2019    |
| Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures [19]       | Corea/ 2019     |
| MicroServices Suite for Smart City Applications [20]                                                                  | Italia/ 2019    |

Realizando un análisis preliminar de las palabras clave de los artículos identificados en la **Error! Reference source not found.**, se tiene el siguiente esquema de red, realizado con la herramienta VOSviewer, el que permite identificar nodos como los elementos principales y los enlaces de cómo se relacionan entre ellos. Figura 4.

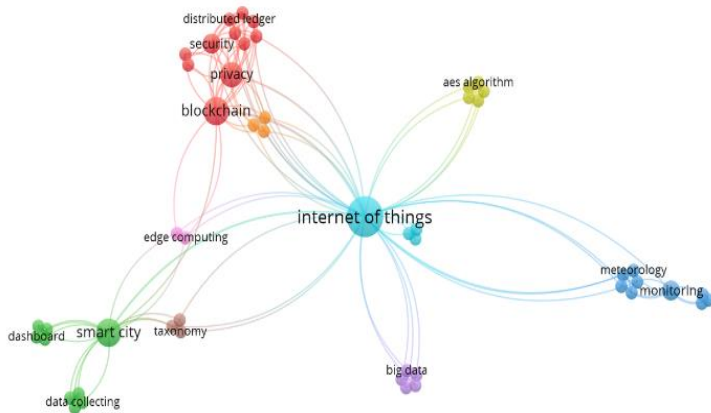


Figura 4. Esquema de red para palabras clave de los artículos seleccionados.

El esquema de red de esta investigación permite visualizar que los principales aspectos abordados por los artículos son: internet of things, smart city, blockchain y privacy, lo que se relaciona directamente con las categorías identificadas y el propósito de esta investigación. La estructura de las interacciones muestra una fuerte relación del nodo central como elemento clave del tema en estudio. Además, es posible apreciar algunos grupos enfocados en aplicaciones (nodos azules a la derecha), recolección y visualización de datos asociados a smart city (nodos en verde, lado inferior izquierdo) y aspectos de protección de datos (nodos color rojo,

lado superior izquierdo).

Adicionalmente, se realizó un análisis de la distribución geográfica y temporal de los artículos seleccionados, siendo China el país con mayor cantidad de investigación relacionada. Este análisis permitió examinar la procedencia de los estudios y su evolución a lo largo del tiempo.

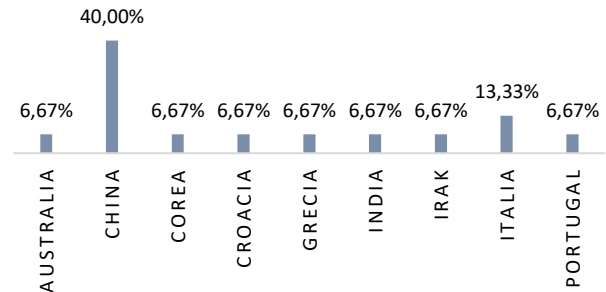


Figura 5. Gráfica distribución de los artículos según país.

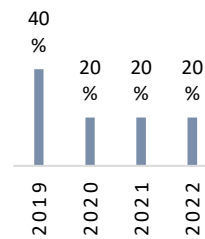


Figura 6. Gráfica distribución de los artículos según fecha de publicación.

## B. Hallazgos por categorías de análisis

En esta sección se presentan los resultados y descubrimientos específicos relacionados con cada una de las categorías y subcategorías de análisis, definidas previamente. Se proporcionan los principales hallazgos relevantes, los cuales se organizan y presentan de manera estructurada para facilitar la comprensión y el análisis de los resultados.

### B.1 Aplicaciones de IoT

#### ✓ Aplicaciones individuales

En la revisión realizada fue posible identificar aplicaciones utilizadas en dispositivos móviles que usan los servicios de ubicación en su funcionamiento [15], las que pueden entregar información personal delicada, como la dirección particular, lugares frecuentes de visita, condiciones de salud, etc. Siguiendo el mismo concepto de aplicaciones móviles, Los autores de [9] enfocan su investigación en la protección de la transmisión de datos a través de la red celular de quinta generación (5G) y en [8] se menciona la utilización de los sistemas de geo-localización y uso de redes sociales.

Las aplicaciones de IoT (Internet de las cosas) en el contexto de las smart cities ofrecen una amplia gama de posibilidades para mejorar la eficiencia, la sostenibilidad y la calidad de vida en las ciudades [19]. Al conectar dispositivos, sensores y sistemas de información, se crea una red inteligente que permite recopilar y analizar datos en tiempo real para tomar

decisiones más informadas y eficientes. Esta red de aplicaciones considera ámbitos de gobierno, transporte, servicios a la comunidad, salud, sustentabilidad con el medio ambiente, entre otras. El potencial de IoT es amplio y su implementación puede adaptarse a las necesidades específicas de cada ciudad para mejorar la calidad de vida de sus habitantes, promover la sostenibilidad y optimizar la gestión urbana.

✓ Aplicaciones colectivas

En [15] y [11] se describen algunos escenarios de aplicación específicos como es el caso de los vehículos inteligentes con capacidades de movilidad, para lo cual se implementó y evaluó experimentalmente la arquitectura y los mecanismos propuestos como una prueba de concepto. Para este caso, es necesario compartir datos relacionados con la identidad y ubicación del usuario de manera segura y privada, protegiendo la privacidad de la persona y asegurando la integridad de los datos durante la transmisión y el procesamiento.

## ***B.2 Riesgos asociados a la recopilación de datos en sistemas IoT***

✓ Robo de información

La recopilación y transmisión de datos a través de sistemas IoT en smart cities plantea riesgos significativos para la privacidad y la seguridad de los ciudadanos. A medida que los dispositivos conectados se multiplican, se recopila una gran cantidad de información personal que puede ser objeto de abuso o uso indebido [6] [7] [8] [9] [10] [11] [13] [14] [16].

Uno de los riesgos es la vulnerabilidad de los datos. La información recopilada, como la ubicación, los patrones de comportamiento y las preferencias de los ciudadanos, puede ser interceptada o accedida por personas no autorizadas. Esto podría conducir al robo de identidad, la suplantación de identidad o la exposición de información sensible. [16]

Además, los sistemas IoT en las smart cities también enfrentan riesgos de seguridad cibernética. La interconexión de dispositivos y sensores abre la puerta a posibles ataques y manipulaciones maliciosas. Los hackers pueden explotar las vulnerabilidades de seguridad para interrumpir servicios críticos, como el suministro de energía o el control del tráfico, lo que afecta la vida cotidiana de los ciudadanos. Para disminuir estos riesgos, es fundamental implementar medidas de seguridad sólidas. Esto implica adoptar prácticas de encriptación robustas para proteger los datos en tránsito y en reposo [9]. Además, se deben establecer políticas claras de privacidad que informen a los ciudadanos sobre qué datos se recopilan, cómo se utilizan y cómo pueden ejercer su derecho a la privacidad [14].

Asimismo, se requiere una colaboración estrecha entre gobiernos, empresas y expertos en ciberseguridad para identificar y abordar las vulnerabilidades en los sistemas IoT. Es esencial realizar evaluaciones periódicas de seguridad, actualizar regularmente el software y brindar educación y

concienciación sobre los riesgos a los ciudadanos [18].

✓ Mal uso de la información

En los artículos analizados no se evidenció investigación asociada al mal uso de los datos personales, la mayor parte de ellos están enfocados en el robo de la información y como evitarlos, aplicando técnicas de seguridad en el almacenamiento y transmisión de los datos. Es importante considerar que para este caso el usuario del sistema IoT entrega el consentimiento de uso de la información para el objetivo en el que fue concebido, por lo tanto, se entiende por mal uso a la práctica indebida de recopilar, almacenar, procesar o divulgar información personal de los ciudadanos para fines no autorizados.

## ***B.3 Tecnologías para la protección de datos***

✓ Centralizadas

- Bloqueadores de red y mecanismos de interferencia [9]. En estos sistemas se introduce intencionalmente una señal de radiofrecuencia (RF) para distorsionar la red de transmisión, con esto, el canal de comunicación se mantiene ocupado evitando el ingreso indeseado de atacantes.
- Machine learning para métodos de encriptación según la clasificación del dato [10]. Este sistema utiliza los métodos de reconocimiento de patrones K -vecinos cercanos (K-NN, K-Nearest Neighbor) para asignar relevancia a los datos clasificándolos como de baja, media y alta sensibilidad. Este algoritmo permitirá asignar los recursos computacionales necesarios para el cifrado y descifrado de los datos haciendo el proceso más eficiente en cuanto al consumo energético.
- Edge computing, también conocido como computación en el borde, es un enfoque de procesamiento de datos y ejecución de aplicaciones en dispositivos ubicados en el borde de la red, cerca de donde se generan los datos. A diferencia del procesamiento tradicional en la nube, donde los datos se envían a centros de datos remotos para su procesamiento, el edge computing permite realizar el procesamiento y análisis de datos de manera local, lo que reduce la latencia y mejora la eficiencia en la transmisión de datos. El edge computing permite llevar la capacidad de cómputo más cerca de la fuente de datos, lo que brinda beneficios como mayor privacidad y seguridad de los datos, mayor disponibilidad de servicios y reducción de la carga en las redes de comunicación [19].

✓ Descentralizadas

- K-anonimato para aplicaciones que operan con servicios basados en la ubicación (LBS, location-based services), a través del uso de GPS integrados en distintos dispositivos



de IoT. Este sistema permite asegurar que la ubicación de un usuario sea identificada con una probabilidad menor o igual a  $1/k$ , donde  $k$  es un parámetro de anonimato. En estos esquemas, se utilizan ubicaciones ficticias o "dummy locations" que son similares a la ubicación real del usuario. Estas ubicaciones ficticias se emplean para formar conjuntos anónimos, dificultando que un atacante pueda distinguir cuál es la ubicación real del usuario dentro de dicho conjunto. Este tipo de ubicaciones presenta ventajas significativas, como no requerir complicados esquemas de cifrado y descifrado, y permitir el ahorro de recursos computacionales en dispositivos del IoT [10] [16].

- Enmascaramiento espacial es utilizada en la protección de datos y la privacidad para ocultar o anonimizar la información de ubicación geográfica, consiste en alterar o distorsionar los datos de ubicación para evitar que se pueda identificar la ubicación real de un individuo o entidad [16].
- Los algoritmos de encriptación cobran vital importancia en el tratamiento y seguridad de la transmisión de datos, como se menciona en [10] [12] es necesario cifrar los datos fuertemente para evitar ataques externos, sin embargo, el proceso de cifrado y descifrado requiere de un consumo de recursos computacionales elevados lo que conlleva a un alto consumo de energía eléctrica.

#### ✓ Distribuidas

- Blockchain permite el anonimato de los usuarios, compartiendo información sin revelar la identidad del propietario. Un sistema de este tipo ofrece mayor resistencia a fallos individuales, donde los nodos participantes se encargan de su correcto funcionamiento y validación, lo que crea una red con propiedades de inmunidad capaces de mitigar acciones maliciosas, como la manipulación de información. Básicamente, blockchain funciona como un registro que almacena información (transacciones) en bloques interconectados de forma secuencial, formando una cadena. Esta característica permite el intercambio de activos criptográficos entre usuarios y también registra y realiza un seguimiento seguro del estado del blockchain [8] [13] [15].
- El desarrollo de una suite de microservicios para aplicaciones de Smart City utilizando Node-RED [20], que permite la creación de una amplia gama de nuevas aplicaciones IoT para ciudades inteligentes.

El artículo destaca los requisitos para las aplicaciones IoT de ciudades inteligentes y presenta un conjunto de microservicios, su ámbito de aplicación y requisitos en relación con las soluciones IoT de ciudades inteligentes.

Para los aspectos mencionados anteriormente es importante tener en consideración a arquitectura de los dispositivos IoT, la cual abarca el diseño y la estructura de los sistemas de IoT, así como la forma en que estos sistemas interactúan entre sí y con otros servicios. Esta arquitectura se compone de diversas capas y componentes, cada uno desempeñando funciones específicas para garantizar el funcionamiento adecuado de los dispositivos IoT. Entre las principales capas de esta arquitectura se encuentran: la capa de percepción o sensor, la capa de red, la capa de middleware y la capa de aplicación [21].

#### • Capa de percepción o sensor

Esta capa desempeña un papel crucial al detectar, recolectar, procesar y transmitir información o datos a través de los dispositivos IoT. Estos dispositivos pueden variar en tipos, incluyendo sensores, actuadores, cámaras, micrófonos y otros. Funcionando como el puente entre el mundo físico y el digital, esta capa suministra datos que reflejan el estado y el comportamiento de objetos y su entorno [22, 23]. Además, tiene la capacidad de ejecutar ciertas funciones de procesamiento local, como el filtrado, la compresión o la agregación de datos, con el propósito de reducir la carga en la red y mejorar la eficiencia. Esta capa actúa como un enlace vital entre el mundo físico y el digital. Esta capa se encarga de la detección, recolección, procesamiento y transmisión de información a través de una variedad de dispositivos IoT, como sensores, actuadores, cámaras y micrófonos. Su función principal es proporcionar datos que reflejen el estado y comportamiento de objetos y su entorno. Además, esta capa posee la habilidad de realizar procesamiento local, incluyendo tareas como el filtrado, la compresión y la agregación de datos, lo cual es fundamental para disminuir la carga en la red y aumentar la eficiencia general del sistema. [24].

#### • Capa de red

Esta capa desempeña un papel fundamental al facilitar la transferencia de datos entre los dispositivos IoT y los servidores o la nube. Utiliza una variedad de medios de comunicación, ya sea a través de conexiones cableadas o inalámbricas, y se apoya en diversos protocolos de red, que pueden incluir tanto IP como otros, para establecer la conectividad y gestionar el enrutamiento de los datos [25]. Además de estas funciones esenciales, esta capa también puede realizar tareas de procesamiento intermedio, como el almacenamiento en caché, la replicación o la transformación de datos, con el objetivo de mejorar la calidad y la disponibilidad de la información [26, 27, 28].

#### • Capa de middleware

Esta capa, posicionada entre la capa de red y la capa de aplicación, opera como un componente de software fundamental. Su propósito es proporcionar servicios comunes y abstractos que simplifican el desarrollo e integración de las aplicaciones IoT. Dentro de su repertorio de servicios se encuentran funciones como la gestión de dispositivos, el manejo de datos, la administración de eventos, la seguridad, la identidad y el contexto, entre otros [29, 30]. Además de estas funciones esenciales, esta capa también puede llevar a cabo tareas de procesamiento avanzado, como el análisis, la minería de datos o el aprendizaje de datos, para extraer información y conocimiento valioso a partir de los datos.

- Capa de middleware

Esta capa tiene la responsabilidad de ofrecer las funcionalidades específicas de las aplicaciones de IoT destinadas a los usuarios finales. Entre las diversas aplicaciones que pueden formar parte de esta capa se encuentran la monitorización, el control, la optimización, la predicción y la automatización [31, 32, 33]. Además de estas funcionalidades clave, esta capa también puede desempeñar funciones de procesamiento final, como la visualización, la presentación y la ejecución de los datos [34]. Además, esta capa gestiona aspectos de seguridad y privacidad, asegurando que los datos de los usuarios estén protegidos y que se cumplan las regulaciones pertinentes.

#### **B.4 Modelo de Tratamiento de datos**

- ✓ Almacenamiento de datos

- El Modelo de Información adicional permite recopilar datos sobre las preferencias de privacidad de los usuarios, como las opciones de consentimiento, las restricciones de divulgación de datos, las preferencias de compartición selectiva, entre otros aspectos relacionados con la gestión de la privacidad [16]. Estos datos adicionales se agregan a la información personal básica para proporcionar un panorama más completo y contextual de las preferencias y requerimientos de privacidad de cada persona.
- El establecimiento de una comunidad técnica de ciudades inteligentes [12][17] minimiza los esfuerzos de implementación de nuevas soluciones, maximizando el intercambio de componentes, estandarizando los modelos de datos en una plataforma común. Se presentan metodologías para motivar a los desarrolladores a idear aplicaciones utilizando un enfoque modular, donde los componentes de una sola función que son reutilizables por otros servicios de la ciudad se empaquetan y publican como componentes independientes, llamados Atomic Services. Los servicios atómicos son componentes de una sola función que son reutilizables por otros servicios de

la ciudad y se empaquetan y publican como componentes independientes [35, 36].

- ✓ Transmisión de datos

- MQTT (Message Queuing Telemetry Transport) [6], integra diversos componentes como protocolos de comunicación el cual utiliza un modelo de publicación y suscripción que almacena mensajes asíncronos y de tamaño pequeño, adecuados para aplicaciones IoT, además considera Storj [7] [37] una plataforma de almacenamiento distribuido que permite la eliminación y modificación de datos bajo demanda.

- ✓ Procesamiento de datos

- Big data analytics desempeña un papel fundamental al permitir el análisis de grandes volúmenes de datos generados en las ciudades. Las ciudades inteligentes generan una gran cantidad de datos a partir de sensores, dispositivos conectados, redes de transporte, sistemas de energía, redes sociales y otras fuentes. Estos datos pueden ser estructurados o no estructurados y contienen información valiosa sobre el funcionamiento de la ciudad, los patrones de comportamiento de los ciudadanos y las tendencias urbanas. Este análisis permite extraer conocimientos y patrones significativos de estos datos para obtener información que puede ser utilizada para mejorar la toma de decisiones en diferentes áreas [19].
- La medición de privacidad basado en entropía representa la incertidumbre de poder identificar la ubicación real del usuario a partir de un conjunto de ubicaciones ficticias. Cuanto mayor sea la entropía, más difícil será determinar la ubicación real del usuario en el conjunto anónimo. La entropía se calcula utilizando la probabilidad de consulta histórica para cada ubicación en el conjunto anónimo [8].
- La Preservación de Privacidad de Ubicación Basado Dummy (DLP) consiste en agregar información ficticia o "dummy" a los datos de ubicación real con el fin de ocultar la identidad y preservar la privacidad de las personas. La idea de DLP de introducir ubicaciones falsas o ficticias en los conjuntos de datos, utilizando algoritmos específicos que preservan la estructura y las características generales de los datos reales, pero sin revelar información personal identificable [16] [38].
- DLP Mejorado selecciona de manera eficiente las ubicaciones ficticias teniendo en cuenta información adicional disponible para un atacante. En la

construcción del conjunto anónimo de ubicaciones ficticias tienen la probabilidad de consulta histórica más similar a la ubicación real del usuario, generando un conjunto anónimo con una entropía lo suficientemente alta utilizando algoritmos específicos que preservan la estructura y las características generales de los datos reales, pero sin revelar información personal identificable [39,40].

Para finalizar esta sección de resultados, se presenta siguiente tabla que relaciona los artículos sometidos a revisión con las correspondientes categorías definidas para esta investigación

TABLA 2  
Papers revisados / Categorías

| Artículos<br>/Subcategorías                    |                                                                                                                   | Uso individual | Uso Colectivo | Robo de información | Mal uso de información | Téc. centralizadas | Téc. descentralizadas | Téc. distribuidas | Almacenamiento de datos | Transmisión de datos | Procesamiento de datos |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|----------------|---------------|---------------------|------------------------|--------------------|-----------------------|-------------------|-------------------------|----------------------|------------------------|
| [6]                                            | Protecting Location Privacy in IoT Wireless Sensor Networks through Addresses Anonymity                           |                |               | x                   |                        |                    |                       |                   |                         | x                    |                        |
| [7]                                            | Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments |                |               | x                   |                        |                    |                       |                   |                         | x                    |                        |
| [8]                                            | Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hash Function                             | x              |               | x                   |                        |                    |                       | x                 |                         |                      | x                      |
| [9]                                            | Realizing Efficient Security and Privacy in IoT Networks                                                          |                |               | x                   |                        | x                  |                       |                   |                         |                      |                        |
| [10]                                           | Method to implement K-NN machine learning to classify data privacy in IoT environment                             |                |               | x                   |                        | x                  | x                     |                   |                         |                      |                        |
| [11]                                           | A Trust-based Security System for Data Collecting in Smart City                                                   |                | x             | x                   |                        |                    |                       |                   |                         |                      |                        |
| [12]                                           | Searchable Encryption Scheme for Personalized Privacy in IoT-Based Big Data                                       |                |               |                     |                        |                    | x                     |                   | x                       |                      |                        |
| [13]                                           | Authentication and Key Management in Distributed IoT using Blockchain Technology                                  |                |               | x                   |                        |                    |                       | x                 |                         |                      |                        |
| [14]                                           | A Regulatory View on Smart City Services                                                                          |                |               | x                   |                        |                    |                       |                   |                         |                      |                        |
| [15]                                           | Security and privacy for mobile IoT applications using blockchain                                                 | x              | x             |                     |                        |                    |                       | x                 |                         |                      |                        |
| [16]                                           | An efficient dummy-based location privacy-preserving scheme for internet of things services                       |                |               | x                   |                        |                    | x                     |                   | x                       |                      | x                      |
| [17]                                           | Smart City IoT Services Creation Through Large-Scale Collaboration                                                |                |               |                     |                        |                    |                       |                   | x                       |                      |                        |
| [18]                                           | A Methodological Framework for the Selection of Key Performance Indicators to Assess Smart City Solutions         |                |               | x                   |                        |                    |                       |                   |                         |                      |                        |
| [19]                                           | Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures        | x              |               |                     |                        | x                  |                       |                   |                         |                      | x                      |
| [20]                                           | MicroServices Suite for Smart City Applications                                                                   |                |               |                     |                        |                    |                       | x                 |                         |                      |                        |
| % de presencia en la revisión de la literatura |                                                                                                                   | 15%            | 10%           | 50%                 | 0%                     | 15%                | 15%                   | 20%               | 20%                     | 10%                  | 15%                    |

### C. Síntesis

La presente revisión sistemática se enfocó en la seguridad y protección de datos para los sistemas IoT en smart cities. A partir de los hallazgos obtenidos, se categorizaron los resultados en cuatro segmentos: aplicaciones de IoT, riesgos asociados a la recopilación de datos en sistemas IoT, tecnologías para la protección de datos y modelos de tratamiento de datos.

De los artículos revisados, es posible señalar en primera instancia que el riesgo eminente al que se exponen los sistemas de IoT se relaciona con la posibilidad de los datos

sean interceptados y utilizados para otros fines distintos a los considerados en su operación normal. La falta de supervisión, en el sentido de implementaciones tecnológicas adecuadas en los sistemas de aplicaciones IoT, puede evidenciar posibilidad de riesgos importantes para las personas y la comunidad, en la que se insertan estas soluciones.

Con respecto al resguardo de la privacidad, se identificaron aportes en la mejora de la eficiencia de las ubicaciones ficticias requeridas para los esquemas de anonimato, considerando además una reducción del tiempo computacional para entregar ubicaciones irreales, lo que permite encontrar fácilmente la ubicación ficticia óptima sin recorrer todas las ubicaciones en el conjunto de candidatos, y con mayor probabilidad de dificultar algún ataque que intente distinguir la ubicación real. No obstante, esta tecnología presenta una deficiencia cuando se trate de ubicaciones que antes no han sido visitadas, pudiendo entregar lugares con probabilidad histórica de 0% como océanos o desiertos, los cuales serían ubicaciones ficticias falsas.

Adicionalmente, la propuesta de utilizar MQTT como complemento para mejorar la interoperabilidad entre dispositivos IoT y la cadena de bloques, evita la sobrecarga computacional de los dispositivos. Los datos se almacenan en un sistema de almacenamiento descentralizado, y no directamente en la cadena de bloques lo que garantiza la posibilidad de modificación y eliminación de datos. Además, proporciona control de privacidad y gestión de datos a los usuarios, incluyendo la capacidad de eliminar o modificar datos.

Respecto de las plataformas de almacenamiento permiten que los mensajes se almacenen en forma de cadena de bloques. Estos mensajes son intercambiados entre nodos autorizados utilizando algoritmos de cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. En cuanto a la seguridad y confidencialidad de los datos, los mensajes intercambiados entre nodos autorizados utilizan algoritmos de cifrado simétrico y asimétrico. El cifrado simétrico utiliza una única clave compartida para cifrar y descifrar los mensajes, mientras que el cifrado asimétrico utiliza un par de claves, una pública y una privada, para cifrar y descifrar los mensajes.

Otro punto importante es la eficiencia del proceso de encriptación y el aumento en la seguridad de los datos utilizando algoritmos más rápidos. Se han propuesto técnicas de procesamiento basadas en machine learning para la clasificación de la sensibilidad de los datos y así generar cifrados más rápidos y con correlaciones más bajas lo que se traduce en una mayor seguridad y privacidad. Al mejorar la eficiencia del proceso de encriptación y aumentar la seguridad de los datos utilizando algoritmos más rápidos y técnicas de procesamiento basadas en machine learning, se logra una mayor protección de la privacidad y la seguridad en los sistemas basados en blockchain.

En resumen, se han realizado avances en la protección de la privacidad y seguridad en aplicaciones IoT, pero aún existen desafíos a superar. La supervisión tecnológica adecuada, la generación de ubicaciones ficticias más precisas y el uso de

algoritmos de cifrado eficientes son aspectos clave para garantizar la integridad y privacidad de los datos en sistemas de IoT.

## V. DISCUSIÓN

Considerando los hallazgos de esta revisión en relación a otras investigaciones del área en estudio, es posible señalar preliminarmente que existen diversas técnicas para resguardar la protección de los datos, las que se basan principalmente en algoritmos que buscan mantener la seguridad de éstos y protegerlos ante eventuales vulnerabilidades. No obstante, no ha sido sencillo inferir cómo se podría operacionalizar su implementación, así como tampoco el identificar claramente en qué capa se integrarían dichas técnicas, entendiendo que la protección de los datos se debe dar tanto en los dispositivos IoT, como en la transmisión del mensaje, almacenamiento y procesamiento [41].

Para abordar de manera más exhaustiva el alcance final de esta investigación, nos referimos a las preguntas que guían este estudio. Estas preguntas proporcionan una guía clara sobre los aspectos que se abordarán y los objetivos que se pretenden alcanzar. Al responder a estas preguntas, se espera obtener una comprensión más profunda y completa del tema en cuestión, lo que permitirá reconocer la implicancia de los hallazgos mencionados y plantear proyecciones para trabajos futuro en el área.

PI 1. ¿Qué sistemas IoT para Smart Cities recopilan datos personales

En cuanto a la recopilación de datos personales a través de los sistemas IoT, la mayoría de los artículos revisados entregan información general del tema en estudio, resultados que se pueden extrapolar a distintas áreas en el contexto de las smart cities, no obstante, en algunos casos fue posible identificar algunos ámbitos de aplicación específica, como los son las aplicaciones móviles que pueden recopilar datos personales, como ubicación, preferencias, hábitos de consumo, información de registro y otros datos relevantes para brindar servicios personalizados a los usuarios, pero que también pueden ser considerado una invasión a privacidad si es acceso a estos datos no es debidamente informado y consensuado por el usuario. Por otro lado, en la indagación inicial de esta investigación se pudo apreciar que, en el contexto de las ciudades inteligentes, los sistemas IoT se utilizan en el sector del transporte para el monitoreo y gestión del tráfico, sistemas de estacionamiento inteligente, seguimiento de flotas y optimización de rutas. Estos sistemas mejoran la eficiencia del transporte, reducen la congestión y brindan una experiencia más fluida para los usuarios. En esta investigación se pudo complementar lo anterior con la revisión de los vehículos inteligentes, llamados también vehículos IoT, que son

automóviles equipados con tecnología avanzada que les permite conectarse a Internet y comunicarse con otros dispositivos y sistemas. Estos vehículos utilizan sensores, redes de comunicación y sistemas de procesamiento de datos para recopilar información y tomar decisiones en tiempo real. En este sentido toman un papel importante los dispositivos de GPS, que proporcionan rutas optimizadas en tiempo real y actualizaciones de tráfico en tiempo real. Esto ayuda a los conductores a evitar congestionamientos y encontrar la ruta más eficiente.

Estos son solo algunos ámbitos de los diversos sectores en los que se aplican sistemas IoT. La tecnología IoT tiene un amplio potencial en varios campos y su adopción continúa creciendo, impulsando la eficiencia, la automatización y la toma de decisiones basadas en datos en diferentes industrias que se encuentran presente en el contexto de las smart cities.

PI 2. ¿A qué tipos de riesgos se exponen las personas al interactuar con sistemas IoT?

Respecto a esta pregunta, es importante mencionar que existen varios riesgos asociados a la seguridad y privacidad de los datos en las aplicaciones de IoT. Uno de los riesgos más destacados es el robo de información. Los datos personales recopilados por los dispositivos de IoT, como la ubicación, los patrones de comportamiento y la información personal identificable, pueden ser objeto de robo por parte de actores malintencionados. Este robo de información puede tener consecuencias graves, como el uso indebido de datos personales, el fraude o el compromiso de la privacidad de las personas.

Además del robo de información, los ataques informáticos son otra preocupación importante, en la que los sistemas de IoT pueden ser vulnerables a ataques como de denegación de servicio (DDoS), inyección de código malicioso, interceptación de comunicaciones y acceso no autorizado a los dispositivos. Estos ataques pueden comprometer la integridad de los datos, la funcionalidad de los dispositivos y la privacidad de los usuarios.

Dentro de los artículos seleccionados, no fue posible identificar estudios o posibles soluciones para el mal uso de la información personal por parte de las empresas. Si bien el usuario entrega su consentimiento para el tratamiento de sus datos como parte de una funcionalidad de un sistema IoT, el reglamento de protección de datos de la unión europea [42] dicta directrices sobre el uso correcto de los datos personales. Como trabajo futuro será necesario extender la investigación a los marcos reguladores y aspectos legales para tener una comprensión clara del problema.

Los sistemas IoT presentan riesgos de ciberseguridad como el robo de datos, ataques DDoS, acceso no autorizado, manipulación de dispositivos y vulnerabilidades de software.

Estos riesgos pueden afectar a las personas de diversas maneras, desde la pérdida de privacidad hasta la seguridad física.

Estos riesgos pueden afectar a las personas de diversas maneras, desde la pérdida de privacidad hasta la seguridad física. Por ejemplo, si los datos de salud de una persona son robados, los atacantes podrían utilizarlos para robar su identidad o cometer fraudes médicos. Si un dispositivo IoT que controla una infraestructura crítica, como una central eléctrica o una red de transporte, es manipulado, podría provocar daños físicos o incluso la pérdida de vidas.

Para mitigar estos riesgos, es importante que las organizaciones que desarrollan y utilizan sistemas IoT implementen medidas de seguridad básicas, como el cifrado de datos y la autenticación multifactor. También es importante que los usuarios estén informados de los riesgos de ciberseguridad y de las medidas de protección que pueden adoptarse.[23][24][25]

De lo anterior, queda de manifiesto que es fundamental implementar medidas de seguridad adecuadas para proteger los datos personales en las aplicaciones de IoT, aspecto que se abordó en la siguiente pregunta.

PI 3. ¿Qué tecnologías son utilizadas para resguardar la privacidad de los datos personales?

Respecto de las tecnologías para resguardar la privacidad de los datos, tanto en el análisis de los artículos sometidos a esta revisión, como en extensa literatura existente en esta área, se pueden encontrar estudios de técnicas de cifrado robustas, la autenticación y autorización de dispositivos, la monitorización constante de la red, la segmentación de la red para limitar el acceso no autorizado y la actualización regular de software y firmware para mitigar vulnerabilidades conocidas.

Se destaca la incorporación de tecnología distribuida como blockchain, que proporciona una forma segura y transparente de almacenar y verificar transacciones. Bajo este enfoque, las transacciones son agrupadas en bloques y enlazadas en una cadena secuencial. Cada bloque contiene un conjunto de transacciones verificadas y selladas criptográficamente. Una vez que un bloque es agregado a la cadena, no puede ser modificado sin alterar los bloques siguientes, lo que garantiza la integridad de los datos. La seguridad de blockchain se basa en algoritmos criptográficos, donde cada participante en la red tiene una copia del blockchain completo, lo que impide la manipulación de datos por parte de un único actor.

La indagación de esta pregunta abarcó diversas técnicas y modelos de protección de datos en aspectos tecnológicos y niveles de profundidad y complejidad algorítmica, por lo que cada una de las tecnologías investigadas podrían ser en sí una

investigación o considerar la opción de plantear una integración de ésta para proporcionar una solución más robusta y segura.

Integrando los aspectos mencionados en las preguntas anteriormente desarrolladas, es posible indicar que la protección de datos personales en el entorno digital es de vital importancia en la actualidad. El auge de las tecnologías como el Internet de las Cosas (IoT) y la digitalización de servicios han incrementado la recopilación de datos personales, aumentando a su vez la necesidad de fortalecer las medidas de seguridad y privacidad.

Junto con lo anterior, y en respuesta a nuestra pregunta de investigación principal, concluimos que resguardar la privacidad de los datos recopilados por los sistemas basados en IoT en una ciudad inteligente requiere una combinación de tecnologías y estrategias. Esto incluye el uso de encriptación para proteger los datos durante la transmisión y el almacenamiento, la implementación de técnicas de anonimización de datos para resguardar la identidad de los individuos y la consideración de tecnologías emergentes como el blockchain.

Además, se identificaron que existen riesgos inherentes asociados con la interacción con los sistemas IoT, como la violación de datos y el uso no consentido. Por lo tanto, además de las soluciones tecnológicas, también es esencial contar con políticas sólidas de privacidad y seguridad de los datos, así como una mayor transparencia en cómo se recogen, almacenan y utilizan estos datos.

## VI. CONCLUSIONES

En conclusión, es posible indicar que para asegurar la privacidad de los datos en las ciudades inteligentes, resulta imperativo establecer una colaboración multidisciplinaria que involucre a tecnólogos, formuladores de políticas, entidades reguladoras y la ciudadanía, con el fin de concebir e implementar estrategias de privacidad que sean tanto efectivas como perdurables. Esta sinergia es fundamental para proteger los datos personales en un contexto de creciente conectividad. Del mismo modo, el análisis realizado subraya que la gestión de la privacidad de los datos trasciende los límites tecnológicos, entrelazándose con dimensiones sociales y humanas. Se evidencia la necesidad de una integración armónica de políticas públicas y privadas que fomenten la adopción segura de tecnologías IoT. Este enfoque holístico es crucial frente al desafío que representa la ciberseguridad en el ámbito del IoT, donde la proliferación de dispositivos conectados incrementa la exposición a potenciales brechas de seguridad. Solo mediante una gestión integrada y considerando las múltiples facetas de la privacidad, se podrá avanzar hacia sistemas IoT robustos y seguros para los usuarios.

## REFERENCIAS

- [1] A. L. Samarakkody, U. Kulatunga y D. Bandara, «What differentiates a smart city? A comparison with a basic city,» de 8th World Construction Symposium, Sri Lanka, 2019.
- [2] Consumer Technology Association, «Innovate Vegas " Six Pillars of smart Vegas",» 19 March 2021. [En línea]. Available: <https://www.ces.tech/articles/2021/march/las-vegas-becoming-a-smart-city.aspx>. [Último acceso: 15 May 2023].
- [3] Ministry of Land, Infrastructure and Transport, «Smart city Korea,» 18 February 2020. [En línea]. Available: <https://smartcity.go.kr/en/2020/02/18/서울시-스마트서울-네트워크s-net-자문위원회-출범/>. [Último acceso: 15 May 2023].
- [4] Rio Prefeitura, «City Hall signs PPP of public lighting,» 28 April 2020. [En línea]. Available: <https://prefeitura.rio/cidade/crivella-assina-ppp-da-iluminacao-publica>. [Último acceso: 10 April 2023].
- [5] M. J. Page y J. E. McKenzie, «Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas,» Revista Española de Cardiología, vol. 74, nº 9, pp. 790-799, 2021.
- [6] Z. Qiong y K. Zhang, «Protecting Location Privacy in IoT Wireless Sensor Networks through addresses Anonymity,» Wiley Hindawi, vol. 2440313, p. 12, 2022.
- [7] W. Tsu - Yang, M. Qian, S. Kumari y P. Zhang, «Rotating Behind Security: A Lightweight Authentication Protocol Based on IoT - Enabled Cloud Computing Environments,» Sensors, vol. 3858, 2022.
- [8] K. Yurika Pant, A. Alsadoon, S. Khurram, A.-K. Ahmad, P. Penatiyana W.C., S. Ur Rehman y I. Rafiqi, «Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hsh Function,» Future Internet, vol. 1477, 2022.
- [9] J. H. Anajemba, Y. Tang, C. Iwendi, A. Ohwoekwwo, G. Srivastava y J. Ohyun, «Realizing Efficient Security and Privacy in IoT Networks,» Sensors, vol. 2609, p. 20, 2020.
- [10] S. QahtanMakki, H. Zaidalaa y A. Alaa Ahmed, «Method to implement K-NN machine Learning to Classify Privacy in IoT environment,» Indonesian Journal of Electrical Engineering and Computer Science, vol. 20, nº 2, pp. 985-990, 2020.
- [11] W. Fang, N. Cui, C. Wei, Z. Wuxiong y C. Yunliang, «A Trust-based Security System for Data Collecting in Smart City,» Transactions on Industrial Informatics, vol. 101109, pp. 1551-3203, 2020.
- [12] S. Li, M. Li, H. Xu y X. Zhou, «Searchable Encryption Scheme for Personalized Privacy in IoT- Based Big Data,» Sensors, vol. 1059, p. 19, 2019.
- [13] P. Soumyashree, J. Debasish, M. Bhabendu Kumar, S. Ramasubbareddy, M. Daneshmand y A. Gandomi, «Authentication and Key Management in Distributed IoT using Blockchain Technology,» Things Journal, vol. 101109, 2021.
- [14] M. Weber y I. Podnar Zarko, «A Regulatory View on Smart City Services,» Sensors, vol. 103390, p. 415, 2019.
- [15] K. Carvalho y J. Granjal, «Security and Privacy for Mobile IoT Applications using blockchain,» Sensors, vol. 5931, p. 21, 2021.
- [16] Y. Du, G. Cai, X. Zhang, T. Liu y J. Jiang, «An efficient Dummy-Based Location Privacy-Preserving Scheme For Internet Of Things Service,» MDPI, vol. 278, p. 10, 2019.
- [17] F. Cirillo, D. Gomez, L. Diez, I. EliceGUI Maestro, T. B. Juel Gilbert y R. Akhavan, «Smart City IoT Service Creation Through Large Scale Collaboration,» IEEE internet of things Journal, vol. 1, pp. 43 - 48, 2020.
- [18] K. Angelakoglou, N. Nikolopoulos, P. Giourka, I. L. Svensson, P. Tzarchopoulos, A. Tryferidis y D. Tzovaras, «A Methodological Framework for the selection of key Performance Indicators to Assess Smart City Solutions,» Smart Cities, vol. 2020018, pp. 269-306, 2019.
- [19] J. Hoon Jo, P. Kumar Sharma, J. Sapalo Sicato y J. Hyuk Park, «Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures,» Journal of Information Processing Systems, vol. 15, nº 4, pp. 765-784, 2019.
- [20] C. Badii, P. Bellinio, A. Difino, P. Nesi y G. Pantaleo, «Microservices Suite for Smart City Applications,» Sensors, vol. 4798, p. 19, 2019.
- [21] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, doi: 10.1109/COMST.2015.2444095.
- [22] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", 2020, [Online].
- [23] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," in Computer Networks, vol. 76, pp. 146-164, 2015, doi: 10.1016/j.comnet.2014.11.008.
- [24] M. A. Razzaque, M. Milojevic-Jevric, A. Palade and S. Clarke, "Middleware for Internet of Things: A survey," in IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70-95, Feb. 2016, doi: 10.1109/IIOT.2015.2498900.
- [25] M. R. Palattella et al., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," in IEEE Journal on Selected Areas in Communications, vol. 34, no. 3, pp. 510-527, March 2016, doi: 10.1109/JSAC.2016.2525418.
- [26] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," in IEEE Internet Computing, vol. 21, no. 2, pp. 34-42, March-April 2017, doi: 10.1109/MIC.2017.37.
- [27] M. A. Alsheikh, S. Lin, D. Niyato and H. Tan, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996-2018, Fourth Quarter 2014, doi: 10.1109/COMST.2014.2320099.
- [28] A. B. Adeel, M. A. Azam, A. Nadeem, M. H. Durad and M. A. Usman, "A Survey on Security and Privacy Issues of Internet of Things," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 2019, pp. 1971-1976, doi: 10.1109/IWCMC.2019.8766648.
- [29] S. B. Mokhtar, A. Ksentini, Y. Hadjadj-Aoul, T. Taleb and D. Benferhat, "A Survey on Security in Internet of Things: Standards, Challenges and Solutions," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1506-1532, thirdquarter 2020, doi: 10.1109/COMST.2020.2984400. A.-a. AFFIA, A. NOLTE y R. MATULEVIČIUS, «IoT Security Risk
- [30] S. Raza, L. Wallgren and T. Voigt, "SVELTE: Real-time intrusion detection on the Internet of Things," 2013 IEEE International Conference on Distributed Computing in Sensor Systems, Cambridge, MA, 2013, pp. 335-342, doi: 10.1109/DCOSS.2013.78.
- [31] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes," in Journal of Network and Computer Applications, vol. 101, pp. 55-82, 2018, doi: 10.1016/j.jnca.2017.12.001.
- [32] Aslan, Ö.; Aktu g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks,

and Solutions. Electronics 2023, 12, 1333.  
<https://doi.org/10.3390/electronics12061333>

[33] J.P. A. Yaacoub, H. N. Noura, O. Salman, A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," in *KeAi Internet of Things and Cyber-Physical Systems*, vol 3, 2023.

[34] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," in *Wireless Networks*, vol. 8, no. 5, pp. 521-534, Sept. 2002, doi: 10.1023/A:1016598314198.

[35] IBM, "Autenticación de nodos", [en línea]. Disponible en: <https://www.ibm.com/docs/es/iad/7.2.x?topic=security-node-authentication>.

[36] M. Salinas Rosales y G. Duchén Sánchez, "Protocolo de autenticación para redes inalámbricas de sensores basado en identidad", *Rev. Fac. Ing. Univ. Antioquia*, no. 52, pp. 203-217, abr. 2010.

[37] J. N. Al-Karaki y A. E. Kamal, "Routing techniques in wireless sensor networks: a survey", *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6-28, 2004, doi: 10.1109/MWC.2004.1368893.

[38] 17. J. Li, X. Chen, M. Li, J. W. Li, P. Lee y W. Lou, "Secure deduplication with efficient and reliable convergent key management", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615-1625, 2014, doi: 10.1109/TPDS.2013.284.

[39] Z. Shelby, K. Hartke y C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, Junio 2014, doi: 10.17487/RFC7252.

[40] S. Khanam, I. B. Ahmedy, M. Yamani, M. Hisham y A. Qalid, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures on the Internet of Things," in *IEEE Access*, vol 8, Nov. 2020

[41] H. Beige, "The Advance of Internet of Things Security Threats and Possible Measures", in *Highlights in Science, Engineering and Technology*, vol 68, 2023.

[42] Management: A Framework and Teaching Approach,» *Informatics in Education*, 2023.



## BIOGRAFIAS



**Pamela Hermosilla** nacida en Valparaíso, Chile, el 8 de octubre de 1974. Graduada de Universidad Técnica Federico Santa María (UTFM Ingeniero Civil en Informática (UTFSM), Diplomada en Comercio Electrónico y Logística Empresarial (UTFSM), Auditor Interno ISO 9001 (Brain & Cia Consultores), MBA of Chief Information Officer CIO (Abet Open University), Diplomada en Docencia Universitaria de la Pontificia Universidad Católica de Valparaíso (PUCV), Diplomada en Formación Virtual Universitaria (PUCV),

Symposium for Entrepreneurship Educators (Luksic Scholars – Babson College). Asesorías: miembro del Consejo Público Privado de la red Fortalece Pyme, Valparaíso - Corfo, integrante del Board de Directores, de la incubadora Chrisalys PUCV. Desarrollo profesional en áreas de Aseguramiento de calidad en gestión de proyectos, Planificación estratégica organizacional, Rediseño curricular basado en competencias, Habilidades de Innovación y emprendimiento en estudiantes de ingeniería, Gamificación en el proceso de enseñanza y aprendizaje.



**Ivo Cattarinich**, nacido en Antofagasta, Chile. El 6 de abril de 1968. Estudio en colegio Salesiano de Valparaíso, Armada de Chile y Universidad Técnica Federico Santa María. Con amplia experiencia en diferentes áreas tales como Marítima, construcción, gas y petróleo. Se ha desempeñado en empresas tales como: Bureau Veritas, Constructora VINCI, Salfa, Besalco, Transmarko, Cpt marítima, Navimag, Humboldt, Transmarchilay, Armada de Chile. Actualmente en formación de Doctorado en Industria

Inteligente, de la Pontificia Universidad Católica de Valparaíso.



**Ignacio Rojas**, nacido en Curicó, Región del Maule, Chile, el 21 de septiembre de 1986. Graduado de Universidad de Talca (Ingeniero en Mecatrónica). 18 años de experiencia en procesos industriales automatizados para la agroindustria, visión artificial, tecnologías láser, cámaras multispectrales, robótica e inteligencia artificial. Investigación basada en inteligencia artificial aplicada a procesos industriales.



**Dr.(c)Sebastián Berrios** nacido el 7 diciembre de 1986. Actualmente candidato a doctor en Ingeniería informática en la Pontificia Universidad Católica de Valparaíso. Graduado de Ingeniería Civil en Computación e Informática en la Universidad De Las Américas. Magíster en Ciencias de la Ingeniería y Magíster en Ingeniería en Informática en la Pontificia Universidad Católica de Valparaíso. Actualmente docente del área de Ciberseguridad de la Pontificia Universidad Católica de Valparaíso.

Administrador de TI de la escuela de ingeniería informática de la Pontificia Universidad Católica de Valparaíso.

Actualmente cursando un Diplomado de Inclusión en Educación en la Pontificia Universidad Católica de Valparaíso, además posee un Diplomado en Seguridad de la Información de 132 horas en la Universidad de Chile y un Diplomado en Ciberseguridad de 96 horas en la misma universidad. También se obtuvo un Diplomado en Ciberseguridad de 100 horas en el Instituto Profesional IACC.

# Protección Digital de Niños, Niñas y Adolescentes: Caso de Estudio en Escuelas de Salta (Argentina)

Maria Inés Gonzalez, Observatorio para la Protección de la Infancia, UCASAL

Micaela Soto Llatser, Observatorio para la Protección de la Infancia, UCASAL

Fernanda Jael Bischoff Herrera, Observatorio para la Protección de la Infancia, UCASAL

Ezequiel Lamas, Facultad de Ingeniería, UCASAL

Herminia Beatriz Parra de Gallo, Facultad de Ingeniería, UCASAL

**Abstract**—El presente trabajo describe los resultados de un proyecto de extensión universitaria, en el que participaron distintos actores institucionales, cumpliendo cada uno de ellos un rol propio y específico. A partir de encuentros desarrollados en escuelas de enseñanza primaria, en los que se trabajó un espacio de discusión y análisis del Grooming, fue posible tomar contacto con Niños, Niñas y Adolescentes (NNyA) quienes plasmaron en una encuesta su visión y vivencia acerca de este delito informático. Esta experiencia, desarrollada a modo piloto en un conjunto pequeño de escuelas primarias y secundarias de la ciudad de Salta (Argentina), permitió obtener un relevamiento de primera fuente que muestra el impacto del Grooming de manera objetiva, cruda y realista. Basado en una metodología sistemática y desarrollado por un equipo multidisciplinario, el proyecto mostró como resultados destacables que es posible encarar la Forensia Digital desde un foco socio-comunitario y desde la responsabilidad social universitaria y desarrollar acciones de alto impacto mediante la vinculación de actores que representen las dimensiones universitarias fundamentales (docencia, investigación y extensión).

**Index Terms**—Grooming, Responsabilidad Social Universitaria, Educación Primaria, Educación Secundaria.

## I. INTRODUCCIÓN

Este trabajo surge como una propuesta de extensión y vinculación con el medio, a partir de una de las actividades de gestión universitaria que la Universidad Católica de Salta (UCASAL), pone a disposición de su propia comunidad educativa: los proyectos de extensión y vinculación con el medio.

En respuesta a la “X Convocatoria de Proyectos de Extensión”, la Facultad de Ingeniería (FI), el Observatorio para la Protección de la Infancia (OPPI), ambos espacios propios de la UCASAL, y la Asociación Civil Grooming Argentina (ACGA)<sup>1</sup>, presentan un proyecto denominado “ProDigNNA – Protección Digital de Niños, Niñas y Adolescentes”.

El Plan Estratégico Institucional 2020-2024 de la UCASAL propone el desarrollo de la función de extensión y vinculación con medio a través del “EJE 4: COOPERAR CON LOS

APORTES DE LA DOCENCIA, INVESTIGACIÓN Y ACTIVIDADES DE EXTENSIÓN A LA CALIDAD DE VIDA DE LA POBLACIÓN, COMUNICANDO EFICIENTEMENTE Y MAXIMIZANDO LA PRESENCIA A NIVEL REGIONAL, NACIONAL E INTERNACIONAL”, que para el caso que nos ocupa, se implementa mediante la convocatoria anual a proyectos de extensión, dirigidos a la comunidad educativa íntegra de la UCASAL, con el objetivo estratégico de potenciar las acciones de extensión relacionadas con el proyecto académico de la UCASAL y que permitan incrementar la vinculación con el medio.

A través de los proyectos de extensión, desde el Vice-Rectorado de Extensión e Integración Universitaria de la UCASAL, se busca resolver problemáticas sociales, promoviendo el trabajo conjunto de docentes, graduados y alumnos de todas las carreras con actores externos provenientes del Estado, empresas y ONGs.

El OPPI de la UCASAL se constituye como un espacio para la observación crítica y la intervención en temas referidos a la infancia, adolescencia y familia. Para ello convoca a las unidades académicas que estudian temas afines, permitiendo ampliar el estudio de problemáticas sociales que le son propias.

Por su parte, la Facultad de Ingeniería de la UCASAL cuenta con el Instituto de Estudios Interdisciplinarios de Ingeniería (I.Es.I.Ing.), que incluye al conjunto de grupos de i+d residentes en dicha unidad académica, y propone entre sus objetivos el de “Fomentar el estudio y la resolución de problemas desde el enfoque interdisciplinario, prestando especial atención a aquellos que involucren a las carreras que se dictan en la facultad”. Desde este lineamiento, el Grupo de I+D+i de FORENSIA DIGITAL Y CIBERSEGURIDAD se interesa en el proyecto ProDigNNA, en coincidencia con la intención de desarrollar a partir del año 2023 acciones tendientes a definir y fomentar la responsabilidad social de la investigación forense que se realiza en dicho espacio.

Como respuesta a estos intereses comunes, desde el OPPI y el I.Es.I.Ing. se presenta el proyecto ProDigNNA, y se invita a la ACGA para que acompañe esta acción.

Este trabajo comprende un conjunto de secciones que le dan forma. En la Sección II se aborda la problemática de estudio, para la cual en la Sección III se presenta el estado del

<sup>1</sup> <https://www.groomingarg.org/>

arte y en la Sección IV la fundamentación del proyecto. La Sección V describe la metodología que permitió desarrollar el proyecto y en la Sección VI se enuncian los resultados obtenidos. Por último, la Sección VII señala las principales conclusiones del trabajo realizado.

## II. PROBLEMÁTICA DE ESTUDIO

Si bien hoy los Niños, Niñas y Adolescentes (NNyA) son nativos digitales y asimilan con mayor rapidez el uso de las TICs, no perciben los riesgos y vulnerabilidades que presenta el sistema. Así, como adultos debemos brindar herramientas para que puedan aprender cómo conocerse, vincularse y comunicarse virtualmente de modo seguro.

El entorno digital permite el desarrollo de una gran gama de nuevos delitos que proliferan bajo la falsa seguridad que se le atribuye, al poder deambular en él desde la comodidad de nuestros hogares. Estos crímenes tienen diversas víctimas, las más vulnerables son los NNyA, quienes utilizan libremente el ciberespacio sin advertir los riesgos que estas interacciones digitales pueden tener, vulnerados por el anonimato característico del internet, su inocencia y la ignorancia de la comunidad.

Según señala la ACGA en su página web, el Grooming es el acoso sexual a niños, niñas y adolescentes a través de medios digitales, consistente en acciones desplegadas generalmente por personas adultas, de cara a establecer contacto con fines sexuales. El término de “grooming” tal como se lo conoce en el habla hispana o “child grooming” en el habla inglesa, es un anglicismo que se traduce en conductas de acercamiento o acicalamiento, configurándose como delito en distintos países de América Latina. Representa una serie de conductas deliberadamente emprendidas por una persona con el objetivo de contactar a un niño, niña y/o adolescente y así ganarse su confianza, estableciendo un vínculo emocional a fin de disminuir sus inhibiciones para luego generar un encuentro personal en el mundo físico, o bien, como en la mayoría de los casos, obtener el material de contenido sexual por parte de la víctima para su comercialización, distribución y/o para satisfacer su perversidad sexual.

Este proceso es ejecutado por el acosador y consta de distintas etapas bien diferenciadas, las cuales podrán ser reemplazadas y/o alternadas entre sí:

- 1) Etapa de enganche o entrapment (atrapamiento): Con el objetivo de ganarse la confianza y establecer un vínculo de amistad, en esta etapa el acosador se acerca al niño, niña o adolescente generalmente falseando su identidad y/o su edad, a través de una conversación donde prevalece el intercambio de gustos, preferencias e intereses.
- 2) Etapa de fidelización: En esta etapa el acosador a sabiendas de los gustos e intereses del niño, niña o adolescente profundiza la relación obteniendo una mayor cantidad de datos personales, donde intentará mantener cautiva la atención procurando fidelizar el vínculo a través del intercambio de secretos, confidencias, promesas, etc.
- 3) Etapa de seducción: En esta etapa el acosador seducirá y sexualizará la conversación, generalmente mediante

preguntas y/o relatos, para generar en el niño, niña o adolescente un compromiso y/o dependencia emocional.

- 4) Etapa de acoso sexual: Esta etapa se caracteriza por una marcada agresión sexual, implícita o explícita, en la cual el acosador manipula a la víctima a través de la solicitud de imágenes y/o videos íntimos, o bien, la propuesta de un encuentro personal. En aquellos casos en los cuales el niño, niña o adolescente no acceda a sus requerimientos, el acosador ejercerá distintas formas de violencia, tales como: chantaje, extorsión, amenazas o coacciones.

Como conclusión, este proceso puede transcurrir durante días, semanas, meses y/o años, transformándose en una nueva modalidad del abuso sexual sin contacto físico contra los NNyA.

La primera intención del trabajo conjunto entre el Grupo de I+D+i de Forensia Digital y el OPPI, fue la formulación de un plan de atención a la problemática del Grooming, con características de integralidad (niños, padres, docentes), y multiespacio (escuela, familia, sociedad) que el tema requería, pero habiendo tomado contacto con las instituciones y organizaciones que se dedican a la atención de esta problemática (Poder Judicial de Salta, Ministerio de Educación entre otros), no fue posible recabar información concreta y comprobable que permitiera definir un diagnóstico certero desde el cual partir para generar acciones tendientes a luchar contra este delito. Así, se entendió que antes de formular acciones de contención que atiendan esta problemática, la UCASAL debía trabajar primeramente en un diagnóstico que mostrara la realidad de las escuelas de Salta.

## III. ESTADO DEL ARTE

De una primera revisión bibliográfica, se encontraron investigaciones similares al proyecto ProDigNNA, entre las que se pueden mencionar las siguientes.

“Grooming y quemar: Agresiones sexuales en el estudiantado mexiquense durante el confinamiento 2020-2021” [1] describe un conjunto de situaciones de violencia virtual producidas durante la pandemia de COVID 19. En este caso, el relevamiento de datos se realizó mediante un formulario virtual y sin plantear instancias de concientización sobre la problemática identificada.

El trabajo de Febriyana et al [2] aborda el análisis de ciberacoso de los NNyA a través de las redes sociales. Es interesante analizar el crecimiento de los cibercrímenes contra los niños que muestran una tendencia creciente para el período 2016-2020 para Indonesia. También se destaca en este estudio el análisis de las técnicas de aproximación que utilizan los perpetradores a través de las redes sociales.

La investigación de Mallqui Ramos [3] tiene como objetivo conocer el estado actual sobre el grooming y analizar la información teórica y empírica sobre los indicadores de salud mental en las víctimas tras experiencias de grooming NNyA entre los años 2013-2023, a través de una revisión documental en plataformas de investigación dentro de América Latina y España. Como resultado de su investigación, la autora destaca cuatro puntos de relevancia: a) conceptualización del grooming en sí, b) variables personales que predisponen a los

NNyA a ser víctimas de grooming, c) factores de riesgo externos que influyen en la victimización; y d) indicadores de salud mental tras experiencias de grooming en los NNyA.

Por su parte, Jaramillo Díaz [4] realizó una investigación acerca de la Explotación Sexual Comercial de NNyA en Colombia, bajo el foco de la legislación penal las malas prácticas en línea asociadas a este delito. Se basa en la metodología INSPIRE [5] propuesta por la Organización Mundial de la Salud, que señala siete estrategias para atacar la problemática de la violencia contra la niñez.

En particular, se analizaron también trabajos basados en encuestas o relevamientos de campo orientados específicamente a la averiguación de datos sobre la problemática del Grooming, entre los que se pueden citar el trabajo de Báez Lacasta [6] que se basó en una encuesta realizada en una escuela de Ituzaingó (Buenos Aires); la investigación de Moreira Zambrano et al. [7] basado en una encuesta realizada a estudiantes de primero, segundo y tercero de bachillerato de la Unidad Educativa 13 de octubre de la ciudad de Calceta durante el año lectivo 2020 – 2021; Comenares-Guillén et al. [8] que trabajó con encuestas realizadas a 30 NNyA que utilizan juegos en línea, identificando que el 73% de ellos admitió haber conversado con personas desconocidas en los juegos en línea; y la investigación de Reneses Botija et al. [9] que muestra los resultados de encuestas realizadas en ocho países europeos y el caso particular de 682 encuestas realizadas en Madrid (España), en el marco del proyecto H2020 Rayuela sobre cibercrimen y menores<sup>2</sup>, analizados desde una perspectiva de género.

Si bien los trabajos analizados muestran resultados de interés, se observó también que las realidades que se estudian son muy diferentes entre sí, como para proponer una generalización de la problemática del Grooming, más allá que se coincide en que es un flagelo a nivel mundial que debe atacarse de inmediato.

Se rescata del proyecto ProDigNNA, frente a las investigaciones analizadas, que se recurrió a un **contacto directo y personal** con los alumnos y docentes de las escuelas visitadas, la cual es una de las características distintivas de este proyecto.

#### IV. PROYECTO PRODIGNAA

En este apartado se describen los objetivos, el plan de acción y el equipo de trabajo del proyecto ProDigNNA.

##### A. Objetivos

Se plantea como objetivo principal concientizar a la población escolar de Salta Capital sobre los peligros online y el uso seguro de internet, mediante la implementación de una encuesta dirigida a identificar situaciones de cibercrimen en la población escolar, mediante la obtención de datos certeros y de fuentes primarias. Los objetivos específicos que se formulan son los siguientes:

- Realizar una efectiva prevención primaria del problema en las escuelas.
- Realizar un diagnóstico del impacto de los cibercrimen en la población escolar seleccionada mediante la toma de encuestas.
- Generar un informe condensando los datos obtenidos y que el mismo, sirva a la comunidad en el afán de prevenir estos peligros.
- Realizar un diagnóstico del impacto de los cibercrimen en la población escolar encuestada.
- Desarrollar un sistema de toma de encuestas y probarlo en una experiencia piloto, considerando un número limitado de escuelas como público objetivo.
- Generar informes que servirán de insumo para otros proyectos vinculados a la Forensia Digital y a la protección de la infancia.

##### B. Plan de Acción

En esencia, el proyecto previó dos acciones conjuntas: CHARLAS DE CONCIENTIZACIÓN y TOMA DE ENCUESTAS, las que se realizaron mediante un plan de visitas a escuelas seleccionadas de Salta Capital. Con un modelo de encuesta definido por la ACGA, se inició la identificación de la situación real sobre los cibercrimen que impactan en los NNyA en Salta, aprovechando el espacio brindado por las escuelas primarias y secundarias que se sumaron al proyecto.

Estas actividades se desglosaron en un conjunto de tareas que se desarrollaron durante 6(seis) meses de trabajo:

- **Capacitación del equipo de trabajo:** se realizaron acciones de capacitación de los equipos de trabajo, referidas al conocimiento de la problemática del Grooming, actividades a cargo de cada uno e indicaciones sobre como debían actuar ante los alumnos y docentes.
- **Organización de las Visitas a las escuelas:** se realizó una identificación de instituciones escolares interesadas en participar del proyecto y se coordinó con ellas los aspectos logísticos para la realización de la visita.
- **Organización de los equipos de visita para cada escuela:** en función de los tiempos asignados, se organizó un cronograma de visitas y la asignación de escuelas a los 4(cuatro) equipos de trabajo que se conformaron.
- **Tareas de Campo:** referidas específicamente a las Charlas de Concientización y Toma de Encuestas, se contó para esta actividad con material de apoyo visual y digital previamente seleccionado y elaborado. Se debe aclarar que la primera acción de la visita fue la toma de encuestas y luego se impartió la charla de concientización, esto con el fin de no condicionar la respuesta de los alumnos a las consignas de la encuesta.
- **Procesamiento Informático y Estadístico de las encuestas por escuela:** como las encuestas se tomaron “en papel” fue necesario realizar la carga y validación de los documentos entregados por cada escuela.
- **Análisis de la visita y datos de la encuesta por escuela:** procesadas las encuestas, se realizó el informe individual para cada institución.

---

<sup>2</sup> <https://www.horizonteueuropa.es/antiores-programas/h2020>

- **Informes de devolución a cada institución escolar:** se remitió el informe a cada institución visitada, en modo reservado por la información sensible que pudiera contener.
- **Análisis integral de las visitas e Inferencia Estadística integral:** se trabajó en la elaboración de un Informe a partir de los datos anonimizados, con el objetivo de encontrar datos que luego permitieran deducir un diagnóstico de la situación relevada.
- **Publicación de Resultados:** se remitió el Informe Final del Proyecto al Vice-Rectorado de Extensión e Integración Universitaria de la UCASAL.

Se visitaron 26 (veintiséis) instituciones educativas de Salta Capital y se obtuvieron 2186 (dos mil ciento ochenta y seis) encuestas. Aunque inicialmente se propuso una zonificación para que las escuelas seleccionadas representaran los barrios y zonas más populosas de Salta Capital, al momento de seleccionar las escuelas que podrían servir como experiencia piloto para el presente estudio, se consideraron 26 (veintiséis) instituciones, las que fueron seleccionadas en función de condiciones de factibilidad operativa que hicieran posible obtener una primera mirada de la situación. Los criterios para selección de las escuelas fueron:

- Instituciones ubicada en Salta Capital y alrededores
- Instituciones con las que hubiera un contacto o comunicación previa por otras acciones realizadas desde el OPPI
- Instituciones cercanas al equipo de trabajo interviniente

Un factor importante al momento de trabajar con las instituciones seleccionadas fue la identificación de los grados o cursos a quienes se convocaría para estudiar la problemática del Grooming, así, surgió la premisa de trabajar con alumnas y alumnos pre-adolescentes de nivel primario (estudiantes de sexto y séptimo grado), aun cuando al momento de la visita, el equipo de trabajo se vio sorprendido porque la escuela pidió que se ampliara la charla a otros cursos, lo cual por supuesto se atendió debidamente.

### C. Equipo de Trabajo

La X Convocatoria de Proyectos de Extensión de la UCASAL, exigió que el equipo de trabajo esté conformado por docentes, alumnos y graduados de la casa. En respuesta a este requerimiento, ProDigNAA contó con la intervención de:

- 7(siete) alumnos de las carreras de Ingeniería en Informática, Ingeniería en Telecomunicaciones, Ingeniería Industrial y Servicio Social de la UCASAL; y
- 4(cuatro) graduados de las carreras de Derecho, Criminalística y Tecnicatura en Seguridad Informática de la UCASAL.

A este equipo se sumaron las autoridades del OPPI y del Grupo de I+D+i de Forensia Digital en tareas de organización y supervisión del proyecto, como extensión de las actividades docentes que las mismas realizan.

Cada escuela invitada recibió la visita de un equipo de trabajo a cargo de la Charla de Concientización y la Toma de Encuestas, conformado por un graduado (que se encargó de la

charla de concientización) y de dos alumnos (responsables de la distribución de las encuestas entre el alumnado presente).

## V. RESULTADOS OBTENIDOS

A manera de resumen, esta sección muestra los resultados más destacados del Informe Final del proyecto<sup>3</sup>.

### A. Caracterización de la Muestra

Las 26 (veintiséis) escuelas que participaron del proyecto ProDigNNA responden a esta distribución muestral (Fig. 1).

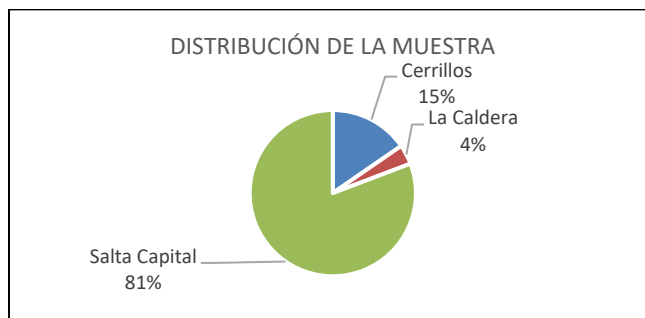


Figura 1: Distribución Muestral de las Instituciones Educativas Participantes

Si se consideran el Padrón de Escuelas del año 2020<sup>4</sup>, Salta Capital cuenta con 363 escuelas de nivel primario y secundario, por lo que la muestra relevada (21 escuelas) no se considera representativo del universo en estudio.

Por esta razón, los datos del presente informe no pueden utilizarse para inferir o proyectar los valores estadísticos encontrados, no obstante, sirven de ejercicio para tomar conciencia de que la problemática existe y que debería ser urgentemente atendida por la salud de nuestros niños, niñas y adolescentes.

Tomando esa distribución de la muestra, la cantidad de encuestas recabadas se distribuyen porcentualmente se indica en la Tabla 1:

Tabla 1: Distribución Porcentual de las Encuestas

| LUGAR         | Cantidad de Encuestas | Distribución Porcentual |
|---------------|-----------------------|-------------------------|
| Cerrillos     | 257                   | 12%                     |
| La Caldera    | 58                    | 3%                      |
| Salta Capital | 1871                  | 86%                     |
| Total general | 2186                  | 100%                    |

### B. Estadísticas Demográficas

Los datos recabados de los niños, niñas y adolescentes encuestados presentan la siguiente **Distribución por Sexo** (Fig. 2), lo que manifiesta un número parejo entre varones y mujeres entre los encuestados.

<sup>3</sup> El cual puede consultarse libremente en el siguiente link: [https://drive.google.com/file/d/1oo44TYd5E4O3xeEO7\\_aGyGMPdRdNLRKR/view?usp=sharing](https://drive.google.com/file/d/1oo44TYd5E4O3xeEO7_aGyGMPdRdNLRKR/view?usp=sharing)

<sup>4</sup><http://www.edusalta.gov.ar/index.php/docman/dpto-estadistica/establecimientos/5624-padron-general-establecimientos-educativos-2020>

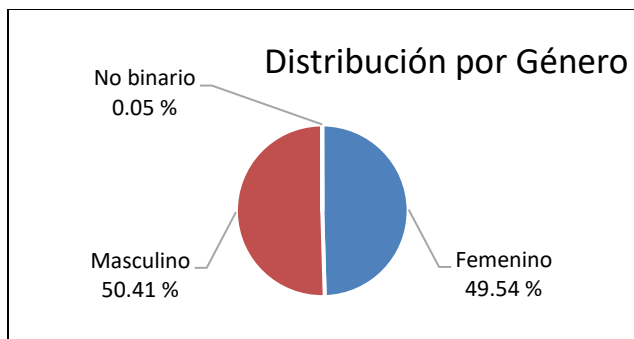


Figura 2: Distribución por Sexo

La **Distribución por Edad** (Fig. 3), considerando el total de encuestas muestra una tendencia central de niños y niñas entre las edades de 11 a 13 años (92.5 %).

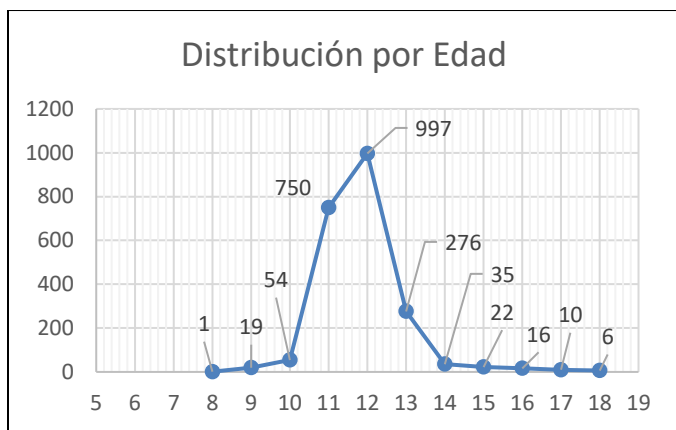


Figura 3: Distribución por Edad

### C. Resultados destacados de las encuestas

Considerando las 11(once) consignas de la encuesta, se presentan los mayores valores de respuesta para cada uno.

Cabe mencionar que en el INFORME FINAL DEL PROYECTO se puede observar el análisis detallado para cada consigna.

#### 1) ¿A qué edad tuviste tu primer celular?

Se observa que los encuestados inician su contacto con el celular mayormente a los 9 años o más (el 48%), pero también es importante destacar que un porcentaje similar (42%) recibe un celular antes de los 9 años.

Esto señala que a muy temprana edad los NNYA se encontrarían activos en internet a disposición de los ciberdelincuentes.

#### 2) ¿Cuántas horas al día estás conectado/a frente a un dispositivo electrónico?

De las respuestas a estas preguntas se puede deducir que los niños y niñas encuestados, en un porcentaje importante (el 48%) acceden a internet entre 5 o más horas diarias.

#### 3) ¿Qué aplicaciones usas?

Para esta consigna se le presentó al encuestado una serie de aplicaciones informáticas, de las cuales podría seleccionar una o varias. Del total de opciones seleccionadas, se estableció que las aplicaciones **WhatsApp, YouTube, Tik Tok e Instagram** son las de mayor interés y representan el 73% de las respuestas.

#### 4) ¿Qué juegos on line utilizas?

Los juegos preferidos por los niños, niñas y adolescentes que respondieron son **Free Fire, Roblox y Minecraft**. Todos estos juegos **no tienen restricción de edad** de los jugadores, por lo que los hace muy peligrosos para los niños, niñas y adolescentes, ya que se exponen a contacto con pedófilos o delincuentes de trata sexual de menores.

Las características de interés de estos juegos se indican a continuación:

- **Free Fire:** es un juego de disparos, en tercera persona (es decir el niño observa su avatar en la pantalla). Tiene 2 modos de juego: cooperativo o multijugador e individual. El juego se presenta solo en plataforma de celulares o Tablet. Se lo considera un juego Free to Play (gratis para jugar) con la opción de invertir plata en el juego a fin de conseguir mejoras estéticas o visuales que no modifican en nada la jugabilidad.
- **Roblox** es un juego en el que se puede crear y compartir mundos virtuales con otros usuarios, la plataforma de este juego es multidispositivo, se categoriza como “del mundo libre”, con pocas restricciones para armar el mundo virtual principalmente acerca de cuestiones éticas (no hay consecuencias por hacer el mal).
- **Minecraft:** es el antecesor de Roblox y es exclusivamente un juego de roles multijugador, clasifica exclusivamente como mundo abierto, la finalidad del juego es la construcción de un mundo abierto. Es un juego multiplataforma bajo la modalidad “pay to win”, es decir, se aporta dinero para conseguir mejoras en el juego para dar más oportunidades para ganar.

#### 5) ¿Realizaste alguna vez un reto viral? Si la respuesta es sí, ¿recuerdas como se llama?

Solo el 18% respondió esta consigna. De los 393 encuestados que respondieron afirmativamente a esta consigna, el 61% indicó algunos de estos retos virales: Arcano, Bailar, Ballena Azul, Batalla campal, Challegger de la Vaca Negra, Charlie Charlie, Copa desafio FreeFire, Desafio de la Botella, Ping Pong, Simon dice, Sprite challenge, Tik Tok, Water dash.

#### 6) ¿Hablas o alguna vez hablaste en internet con personas que no conoces personalmente? Si la respuesta es sí, ¿por cuál aplicación o juego se conocieron?

El 49% de los encuestados respondió esta pregunta. Los juegos más utilizados en la comunicación con desconocidos son **Free Fire y Roblox**, mientras que las redes sociales **Tik Tok e Instagram** también se destacan como contacto con desconocidos. El mayor valor lo tiene el juego **Free Fire** lo que indica la preferencia de los NNYA con esta aplicación lúdica.

#### 7) ¿Estás de acuerdo que un adulto de confianza (papá, mamá, docente, etc.) comparta tus fotos en redes sociales sin preguntarte?

Para esta consigna, relacionada más con la privacidad de los datos personales, los encuestados respondieron según la siguiente distribución: 62% respondió que no está de acuerdo, 35% que sí está de acuerdo y el 3% no contestó.



8) *¿Sabes qué es el sexting? Si la respuesta es SI ¿alguna vez realizaste esta práctica?*

Del 13% que respondió positivamente a esta consigna, 54 personas indican que sí lo practicaron. Y teniendo presente la edad mayoritaria de los encuestados (11 a 13 años), es preocupante que se conozca esta práctica y además se practique.

9) *¿Sabes qué es el Grooming?*

Solo el 30% de los encuestados reconocer saber qué es esta práctica. Esto refuerza el objetivo de **concientizar acerca de Grooming** entre el alumnado y los docentes de las instituciones escolares.

10) *¿Alguna vez te solicitaron imágenes de desnudez en internet? Si la respuesta es SI ¿conocías personalmente a quien te lo pidió? ¿Cómo reaccionaste en ese caso?*

El 87% de los que respondieron indicaron que no le solicitaron imágenes de desnudez. De los 244 que respondieron positivamente, el 52% indicó que le contó a un amigo de su edad, el 13% le contó a una persona adulta de confianza y el 35% no le contó a nadie. Se observa que en el 65% de los casos, los encuestados manifiestan haberse comunicado con alguien para darle a conocer la situación que se les había presentado, lo que nos indica que, independientemente que en su mayoría no reconocen el grooming como un delito por faltas de conocimientos, pudieron haber intuido que la propuesta presentada por medios de las plataformas empleadas atentaban contra su seguridad personal y vulneraban su integridad sexual, causándole una situación de incomodidad no deseada.

11) *¿Crees que sabes más de tecnología que tus padres?*

Esta pregunta se puede interpretar como una situación de alarma ante la vulnerabilidad de los NNyA frente al entorno virtual, ya que el 68% de ellos cree que sus padres podrían no estar capacitados para ayudarlos con la tecnología.

Entre otros aspectos de interés que resultaron del proyecto se pueden indicar:

- Si bien en las intervenciones de los establecimientos se seguía el mismo procedimiento, es decir en primer lugar se llevaban adelante las encuestas y con posterioridad la charla de concientización, en cada institución educativa independientemente de que sean públicas o privadas se llevaron adelante vivencias diferentes. Cuando se presentaban las encuestas se notaba un completo desacuerdo sobre los temas planteados, situación que les generaba diferentes sentimientos, pero sobre todo destacamos mucho interés y deseos de comunicar y consultar sobre sus vivencias personales.
- Al iniciar la charla de concientización, se notaba en sus expresiones que empatizaban con los disertantes y seguían por completo el hilo discursivo, al finalizar el taller reflexivo, siempre notamos que los participantes en su mayoría tenían la necesidad de dar a conocer hechos que habían vivido durante estos años. Situaciones que desencadenaron la activación de diferentes Protocolos de Intervención de forma inmediata, entre los que destacamos: Maltrato Infantil, Acoso escolar, Abuso sexual infantil, Autolesión, Intento de suicidio, Cyberbullying y Grooming. Todos ellos fueron

abordados teniendo presente los pasos establecidos por la Resolución 546D/10 del Ministerio de Educación<sup>5</sup>, Ciencias y Tecnologías de la Provincia de Salta. Según la índole de la situación problemática presentada, se comunicaba al docente, a los directivos y con posterioridad al Ministerio Público Pupilar, que intervenían mediante los Asesores de Incapaces para proteger los derechos de los niños, niñas y adolescentes afectados por cualquier tipo de delito que atentaba contra su seguridad física y psicológica.

- Por otra parte, se armó un **RESERVORIO DE RECURSOS ON-LINE** de acceso gratuito para que los docentes y directivos de las instituciones puedan trabajar en el aula las problemáticas que surgen del uso inadecuado de internet. También se desarrolló una **INFOGRAFÍA** con notas y datos de interés sobre el tema, destinado a que las instituciones lo utilicen como material de difusión en la escuela.
- Si bien el modelo de encuesta se elaboró a partir la propuesta de ACGA, la experiencia lograda en este proyecto ha permitido observar varias cuestiones que sería importante mejorar para la continuación de este proyecto. Tales como:
  - Identificar la opción de “otros dispositivos electrónicos” en la pregunta de “A que edad tuviste tu primer celular”. Esa consigna debería reformularse para que el encuestado tenga a la vista más opciones de respuesta, por ejemplo: “A que edad tuviste tu primer dispositivo electrónico (celular, computadora, Tablet, notebook)”
  - Incorporar **Telegram** como opción de aplicación a disposición de los NNyA, ya que es una red en donde se realiza la venta sexual explícita.
  - Revisar las preguntas abiertas a fin de incorporar valores de respuesta como opciones, esto ayudará a realizar una tabulación más ajustada
  - Mejorar detalles de forma del instrumento (agregar fecha e institución)

## VI. CONCLUSIONES

A todas vistas consideramos que este proyecto ha sido exitoso, iniciando un camino para la estructuración y organización de un relevamiento con mayor alcance, si se tienen en cuenta, por ejemplo, los siguientes criterios:

- Se deberá identificar el universo en estudio, definiendo lugares o áreas que -en sucesivas etapas- permita abarcar todas las instituciones educativas de la provincia.
- Identificado el universo, el espacio muestral debe ser de un tamaño “N” adecuado a fin de poder inferir con cierto grado de confianza los datos que se encuentren.
- Se requiere de la participación de otros actores internos (de la propia UCASAL) y externos (de los organismos del estado) a fin de conformar un equipo de trabajo sólido y con más experticia en este tipo de actividades.

---

<sup>5</sup><http://www.edusalta.gov.ar/index.php/docentes/normativa-educativa/resoluciones/5161-res-min-n-546d-19>



- Los datos del presente informe no pueden utilizarse para inferir o proyectar los valores estadísticos encontrados hacia el universo de estudio (considerando a éste como el conjunto de instituciones educativas de la provincia de Salta), no obstante, sirven de ejercicio para tomar conciencia de que la problemática existe y que debería ser urgentemente atendida por la integridad personal de nuestros NNyA.
- Se observa que los encuestados inician su contacto con el celular mayormente a los 9 años o más (el 48%), pero también es importante destacar que un porcentaje similar (42%) recibe un celular antes de los 9 años. Esto señala que a muy temprana edad los niños y niñas se encontrarían activos en internet a disposición de los ciberdelincuentes.
- Se sobreentiende la necesidad actual de interconexión, no solo por qué es indispensable para afrontar las diversas realidades de la familia salteña, sino también debido a que los procesos de socialización han evolucionado, tomado este carácter dual: on y off line. Dentro de estos mundos (on y off line) que los adultos delimitamos tan fácilmente, los NNyA habitan sin distinguir los límites y alcances de cada uno, no solo a nivel comportamental sino también a nivel psico-emocional.
- Considerando las preguntas que abordaban la identificación de las redes sociales o juegos en línea, se registraron como las aplicaciones **de mayor interés para los NNyA**:

- Redes Sociales: **Tik Tok e Instagram**
- Aplicaciones Informáticas: **WhatsApp, YouTube**
- Juegos en Línea: **Free Fire, Roblox y Minecraft**

Estos datos son preocupantes, ya que, estas aplicaciones y juegos son ampliamente utilizadas por los agresores donde tienen a su favor dos situaciones claramente evidenciadas: el uso indiscriminado sin supervisión de adultos responsables de los NNyA, y la falta de las correctas herramientas de seguridad.

Estos dos factores en conjunción con la abundancia de agresores, dejan a los NNyA completamente vulnerables frente a los flagelos del ciberespacio.

Por último, es de destacar la instancia de “presencialidad” utilizada para este proyecto, yendo directamente a la fuente misma de los datos (la escuela), aprovechando el espacio de relevamiento de los datos para realizar acciones de concientización; características éstas que distingue a ProDigNAA de otros proyectos similares.

## VII. AGRADECIMIENTOS

Agradecemos a los estamentos institucionales de la UCASAL que colaboraron en la concreción de este proyecto: Vice-Rectorado de Extensión e Integración Universitaria, Observatorio para la Protección de la Infancia y Facultad de Ingeniería. También se debe destacar el trabajo de los graduados y alumnos que participaron de las tareas de campo.

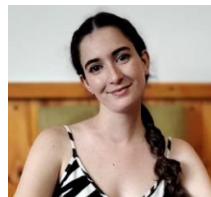
## VIII. REFERENCIAS BIBLIOGRÁFICAS

- [1] Reyes, L. M. V. (2023). Grooming y "quemar": agresiones sexuales en el estudiantado mexiquense durante confinamiento 2020-2021. *GénEroos. Revista de investigación y divulgación sobre los estudios de género*, 1(2), 4-31.
- [2] Febriyana, A., & Gusnita, C. Child Grooming Approach Model of Offenders toward Children on Social Media. *Martabat: Jurnal Perempuan dan Anak* ISSN (p): 2581-2076; ISSN (e): 2581-0472 Vol. 7, No. 1, Juni Tahun 2023, pp. 67-82.
- [3] Mallqui Ramos, W. J. (2023). Estado de arte sobre indicadores de salud mental tras experiencias de grooming online en niños, niñas y adolescentes entre el 2013-2023. Trabajo de Tesis para optar al título de Licenciada en Psicología, de la Universidad Peruana Cayetano Heredia.
- [4] Jaramillo Diaz, K. (2023). Explotación sexual comercial de niñas, niños y adolescentes en Colombia: análisis de estrategias para la protección y prevención del delito. Escuela de Gobierno, UNIANDES (Ecuador).
- [5] INSPIRE Seven Strategies for Ending Violence Against Children. Executive Summary © World Health Organization 2016 WHO/NMH/NVI/16.7.
- [6] Báez Lacasta, E. Y. (2021). El aula como ámbito de prevención del grooming en los adolescentes. Universidad Abierta Interamericana (UAI).
- [7] Moreira, J., Zambrano, A., Vera, I., & Vera, O. (2021). Impacto del Child Grooming en los estudiantes de bachillerato de la Unidad Educativa 13 de Octubre de la ciudad de Calcuta. *Revista Científica de Informática ENCRIPART- ISSN: 2737-6389*, 4(7), 25-37.
- [8] Colmenares-Guillén, L. E., & Nava, N. J. T. (2023). Online Grooming: de los juegos en línea a la obtención de material de abuso sexual. *Revista Científica Multidisciplinaria SAPIENTIAE*. ISSN: 2600-6030, 6(12), 60-77.
- [9] Reneses Botija, M., Riberas Gutiérrez, M., & Bueno Guerra, N. (2022). Base de datos para el manuscrito: Violencia en línea y roles de género en menores. Discurso de odio, ciberacoso y online grooming.

## IX. BIOGRAFÍAS



**María Inés María Ines Gonzalez Farias.** Lic en Criminalística. Perito en inspecciones oculares y Dactiloscopia. Perito accidentólogo. Especialista en Investigación de Homicidios. Magistrado en Criminalística. Diplomada en Ciberdelitos y ciberseguridad. Diplomada en Educación Universitaria. Docente de la Universidad Católica de Salta en las carreras de Lic. en Criminalística, Lic. En Criminología y Lic. En Seguridad. Actualmente coordinadora en el Departamento de Criminalística del Departamento judicial Orán y Tartagal de la UEI (Unidad Especial de Investigación) del Cuerpo de Investigaciones Fiscales del Ministerio Público Fiscal de Salta.



**Micaela Soto Llatser.** Licenciada en criminalística por Ucasal, Diplomada en Ciberdelitos contra la niñez por UNSTA, Maestrando en Psicología Criminal por la Universidad Europea del Atlántico, miembro colaborador del Observatorio de Protección para la Infancia de UCASAL, Perito de parte y técnica en investigación para DigiLab y Universidad FASTA



**Fernanda Jael Bischoff Herrera.** Lic. En Criminalística UCASAL, Maestrando en Criminalística e investigación criminal en la UNEATLANTICO - UNINI-MX mediante FUNIBER. Dip. En Ciberdelitos contra la niñez. Miembro adherente del Observatorio para Protección de la Infancia de UCASAL.



**Ezequiel Rubén Lamas.** Técnico Superior en Mecatrónica con orientación en autotrónica. Licenciado en Criminalística. Profesor Universitario. Especialista en Informática Forense. Coordinador Técnico del DigiLab-Laboratorio de Forensia Digital de la Facultad de Ingeniería de UCASAL. Docente de las Facultades de Ingeniería, Ciencias Jurídicas, Economía y Ciencias de la Salud de la UCASAL.



**Herminia Beatriz Parra de Gallo,** Especialista en Informática Forense, Dra. en Ingeniería Mención Sistemas de Información, Master en Administración de Negocios, Ingeniería en Computación. Con una extensa carrera académica como docente e investigadora en la UCASAL reviste la categoría de INVESTIGADOR INDEPENDIENTE “B” (CI-UCASAL), y es Directora del Grupo de I+D+i de Forensia Digital

de esa institución, grupo abocado al desarrollo de proyectos de i+d interinstitucionales con universidades nacionales y latinoamericanas. Es además, Directora del Instituto de Estudios Interdisciplinarios de Ingeniería de la Facultad de Ingeniería de la UCASAL y Directora de la carrera de Especialización en Administración de Bases de Datos. Participa en la formación de recursos humanos impartiendo cursos de posgrado y como docente de carreras de grado y posgrado en UFASTA (Argentina), UTN-FRSF (Argentina), UTN-FRC (Argentina), UNIVA (México), UNISANGIL (Colombia), Universidad Católica de Colombia (Colombia), UniTECH (España). Perito Informático de Parte. Consultora en Proyectos Tecnológicos Críticos. Sus temáticas de interés son: Forensia Digital, Educación en Ingeniería y Ética en la Ingeniería.

# Readecuación del Perfil Docente/Investigador en la Facultad Regional Delta

Carla Carrillo, Germán Carrillo, Valeria Traverso, Pablo Visintin, Nancy Carrizo, Florencia Leiva  
Universidad Tecnológica Nacional – Facultad Regional Delta- Buenos Aires- Argentina.  
ccarrillo@frd.utn.edu.ar

**Abstract--** Este trabajo propone examinar la necesidad y la viabilidad de la readecuación del perfil docente/investigador en el ámbito actual de la Universidad Tecnológica Nacional (UTN) Facultad Regional Delta. Se analizan los cambios en las demandas educativas y las expectativas de investigación, proponiendo estrategias para la adaptación de los profesionales de la educación superior. La investigación combina revisión bibliográfica, análisis de casos y propuestas concretas para abordar estos desafíos.

**Palabras claves—**Perfil docente – Perfil investigador – Desafíos – Demandas educativas.

## I. INTRODUCCIÓN

Este trabajo pretende proporcionar un contexto detallado sobre la dinámica cambiante del perfil docente/investigador en el actual escenario académico de la UTN Facultad Regional Delta, delineando la evolución de las expectativas que recaen sobre estos profesionales. En un entorno académico caracterizado por rápidos avances tecnológicos, transformaciones pedagógicas y una creciente interconexión global, la figura del docente/investigador se ve sometida a una constante redefinición.

Este proceso evolutivo, marcado por una demanda cada vez mayor de habilidades multifacéticas, abarca la excelencia en la transmisión del conocimiento, la capacidad de generar investigaciones innovadoras y relevantes para el contexto actual. La intersección entre la docencia y la investigación se vuelve fundamental, conformando un binomio que influye en la calidad de la educación superior, y también impacta directamente en la contribución de la institución al desarrollo de la sociedad y la generación de conocimiento.

En este escenario dinámico, la adaptación continua del perfil docente/investigador se erige como un requisito esencial para el éxito profesional y la pertinencia académica. Los docentes/investigadores enfrentan una serie de desafíos, desde la integración efectiva de las nuevas tecnologías hasta la respuesta a las cambiantes expectativas de los estudiantes y las demandas emergentes de la sociedad. La capacidad de adecuarse a estos desafíos no solo determina la efectividad de la labor académica individual, sino que también influye en la posición competitiva de la institución educativa en el panorama global.

En este contexto, la presente investigación se propone explorar las razones subyacentes a la necesidad de readecuar el

perfil docente/investigador, identificando las áreas clave que requieren atención y ofreciendo perspectivas fundamentadas sobre estrategias para lograr una adaptación exitosa. A través de la delimitación de objetivos específicos, se busca proporcionar un análisis exhaustivo de los factores que inciden en esta readecuación y proponer soluciones concretas para maximizar el impacto positivo en el ámbito académico.

La relevancia de esta investigación radica en su potencial para informar a la comunidad académica sobre las mejores prácticas, permitiendo una comprensión más profunda de las tendencias emergentes y las demandas cambiantes. Al abordar estos temas críticos, se beneficia la labor diaria del docente/investigador y también se contribuye al enriquecimiento del entorno educativo en su conjunto, promoviendo una formación superior que responda de manera eficaz a los retos actuales y futuros, promoviendo, fundamentalmente, el trabajo mancomunado con los departamentos académicos.

## II. MARCO TEÓRICO

Esta investigación se basa en una exploración detallada de los cambios fundamentales que han dado forma al entorno académico de la Facultad Regional Delta. En primer lugar, se examinan los avances tecnológicos, los cuales han revolucionado la manera en que se accede, se comparte y se utiliza la información en el ámbito educativo. La creciente integración de herramientas digitales y plataformas en línea ha transformado los métodos de enseñanza, incrementando las expectativas en cuanto a la accesibilidad y la interactividad en el proceso de aprendizaje.

Paralelamente, se consideran los cambios en la pedagogía, destacando las tendencias emergentes en enfoques educativos. Se profundiza en modelos pedagógicos innovadores que van más allá de la tradicional transmisión de conocimiento, explorando estrategias activas de aprendizaje, el fomento de habilidades críticas y el énfasis en el desarrollo de competencias prácticas para preparar a los estudiantes para un mundo en constante cambio.

Adicionalmente, se aborda la evolución de las expectativas en investigación, contextualizando cómo las demandas de la sociedad y la comunidad académica han influido en la dirección y el propósito de la investigación universitaria. Se examinan los cambios en la valoración de la interdisciplinariedad, la relevancia social de la investigación y la creciente importancia

de la transferencia de conocimiento hacia la práctica.

En este contexto dinámico, se lleva a cabo una revisión exhaustiva de las teorías y enfoques actuales que delinean el rol del docente/investigador. Se exploran modelos pedagógicos como el aprendizaje activo y colaborativo, así como teorías que enfatizan la importancia de la conexión entre la enseñanza y la investigación, como la teoría del docente-investigador reflexivo. Se busca comprender cómo estas teorías se aplican en la práctica y cómo pueden orientar la readecuación del perfil docente/investigador en el contexto actual de la educación superior. Este análisis enriquece la comprensión del entramado conceptual que sustenta el papel crucial de estos profesionales y sienta las bases para las recomendaciones prácticas propuestas en esta investigación. McLaughlin, P. (2020).

#### *A. Perfil docente*

La transformación constante del entorno educativo ha colocado al perfil docente en el epicentro de cambios significativos. En este contexto, se aborda la evolución del perfil docente desde una perspectiva integral, reconociendo la diversidad de estilos y ritmos de aprendizaje presentes en el estudiantado contemporáneo. La comprensión profunda de las variadas necesidades y habilidades de los estudiantes se convierte en un pilar esencial para la excelencia docente. Fernández Mc Cann, D. (2012).

La incorporación de la tecnología educativa se erige como un elemento clave en la evolución del perfil docente. Más allá de ser un mero complemento, la tecnología se visualiza como una herramienta poderosa para potenciar el proceso de enseñanza y aprendizaje. La habilidad del docente para integrar efectivamente estas herramientas digitales en su práctica diaria se convierte en un factor determinante para la optimización de la experiencia educativa y la preparación de los estudiantes para un mundo cada vez más digitalizado.

En consonancia con estos avances, se subraya la importancia de cultivar habilidades pedagógicas avanzadas. La mera transmisión de conocimientos cede espacio a la necesidad de desarrollar estrategias pedagógicas que fomenten la participación de los estudiantes, el pensamiento crítico y la aplicación práctica de los conceptos aprendidos. Habilidades como la empatía, la adaptabilidad y la capacidad de motivar y guiar a los estudiantes se elevan a un nivel de importancia crucial en el perfil docente contemporáneo. Kentucky Department of Education (2020)

En este escenario, se proponen estrategias específicas para mejorar la enseñanza y la interacción con los estudiantes. Estas estrategias incluyen el diseño de materiales educativos adaptados a diferentes estilos de aprendizaje, la implementación de herramientas tecnológicas innovadoras para fomentar la contribución dinámica y la creación de ambientes de aprendizaje inclusivos que promuevan la diversidad.

La habilidad del docente para adaptarse a estos cambios y abrazar una perspectiva continua de mejora se convierte en un factor diferenciador en la configuración del perfil docente moderno. La capacidad de ser un facilitador del aprendizaje, un guía en la exploración de nuevos conocimientos y un motivador intrínseco se presenta como esencial para el éxito en la

formación de los estudiantes en la era contemporánea. Florencia Santi, M., (2015).

#### *B. Perfil investigador*

En el contexto específico de la Facultad Regional Delta, el perfil investigador adquiere matices particulares que reflejan no solo las tendencias globales, sino también las necesidades y características propias de una institución orientada a la formación técnica y tecnológica. En este entorno, la interdisciplinariedad cobra un papel aún más crucial, dado que la resolución de problemas tecnológicos y científicos a menudo requiere la convergencia de conocimientos provenientes de diversas disciplinas. Hernández Arteaga, I., (2009). El investigador de la Regional se distingue por su capacidad para integrar y aplicar conocimientos multidisciplinarios, fomentando la sinergia entre ingeniería, tecnología y otras áreas de estudio.

La colaboración internacional se convierte en una estrategia clave para el investigador de la Regional. Dada la naturaleza globalizada de la investigación y el desarrollo tecnológico, establecer alianzas con instituciones extranjeras no solo amplía las oportunidades de investigación, sino que también enriquece la perspectiva y la calidad de los proyectos. Hernández Arteaga, I., (2009). La colaboración dinámica en redes internacionales permite, al investigador de la Regional, acceder a recursos, metodologías y enfoques innovadores, contribuyendo así a la excelencia en la generación de conocimiento.

La vinculación con el sector productivo cobra una relevancia aún mayor en el contexto de la Regional. La orientación práctica y aplicada de esta universidad demanda una colaboración estrecha entre los investigadores y las empresas o instituciones del entorno tecnológico. El investigador de la Regional, al estar consciente de las demandas y retos del sector productivo, se convierte en un agente activo en la transferencia de conocimiento y tecnología, contribuyendo al desarrollo económico y social de la región.

Para fortalecer la productividad y relevancia de la investigación en la Facultad Regional Delta, se proponen enfoques específicos. La implementación de proyectos de investigación aplicada en colaboración con la industria, el establecimiento de centros de innovación y la promoción de la formación continua para mantenerse actualizado en las últimas tecnologías y tendencias, son estrategias clave. Además, la difusión efectiva de los resultados de la investigación, tanto a nivel académico como empresarial, es esencial para maximizar el impacto y la utilidad de los hallazgos.

#### *C. Desafíos y oportunidades*

Para los docentes investigadores de la Facultad Regional Delta la readecuación de su perfil implica desafíos y oportunidades particulares, dados los contextos específicos de esta institución centrada en la formación tecnológica.

##### *Desafíos:*

Resistencia al Cambio Tecnológico: Dada la rápida evolución de las tecnologías, los docentes investigadores de la UTN pueden enfrentar resistencia al cambio, especialmente en la integración de nuevas herramientas tecnológicas en sus métodos de enseñanza e investigación.

Falta de Recursos Tecnológicos: La infraestructura tecnológica puede ser un desafío, ya que no todos los docentes pueden tener acceso a recursos avanzados, equipos especializados o plataformas digitales necesarias para llevar a cabo investigaciones de vanguardia.

Necesidad de Desarrollo Profesional Continuo en Tecnología: La demanda de habilidades tecnológicas en constante cambio puede generar la necesidad de un desarrollo profesional continuo. Los docentes investigadores deben mantenerse actualizados con las últimas tendencias tecnológicas para maximizar su efectividad en la docencia y la investigación.

Vinculación Efectiva con el Sector Productivo: La colaboración con la industria puede ser un desafío, ya que se requiere establecer y mantener relaciones sólidas con empresas para la transferencia efectiva de conocimientos, y esto puede enfrentar obstáculos logísticos y de coordinación.

#### *Oportunidades:*

Enriquecimiento Académico a Través de la Interdisciplinariedad: La adaptación a nuevos enfoques interdisciplinarios enriquece la investigación tanto como la enseñanza, permitiendo a los docentes investigadores de la Facultad Regional Delta explorar la convergencia de la tecnología con otras disciplinas.

Participación en Proyectos de Innovación Educativa: La adaptación exitosa a nuevas metodologías y tecnologías brinda oportunidades para participar en proyectos de innovación educativa, contribuyendo al desarrollo de nuevas estrategias pedagógicas y materiales didácticos innovadores.

Colaboración Internacional: La globalización de la investigación ofrece oportunidades para establecer colaboraciones internacionales, permitiendo a los docentes investigadores de la Regional contribuir a proyectos de alcance global y beneficiarse de la diversidad de enfoques y experiencias.

Impacto en la Industria y Desarrollo Regional: La vinculación efectiva con el sector productivo no solo fortalece la aplicabilidad de la investigación, sino que también contribuye al desarrollo regional al facilitar la transferencia de tecnología y conocimientos a la industria local. Aznar et al (2014).

### III. ESTRATEGIAS PARA LA READECUACIÓN DEL DOCENTE INVESTIGADOR EN LA FACULTAD REGIONAL DELTA

Programas de Desarrollo Profesional Continuo: Implementar programas específicos de desarrollo profesional que aborden las habilidades tecnológicas emergentes y las metodologías de enseñanza innovadoras. Estos programas podrían incluir talleres, cursos en línea y certificaciones que permitan a los docentes investigadores mantenerse actualizados con las últimas tendencias y herramientas.

Fomento de la Investigación Aplicada: Establecer incentivos y reconocimientos para la investigación aplicada, destacando la importancia de los proyectos que tienen un impacto directo en la solución de problemas prácticos de la industria y contribuyen al desarrollo económico y tecnológico.

Creación de Centros de Innovación: Establecer centros de innovación dentro de la Facultad Regional Delta que sirvan como espacios de colaboración interdisciplinaria. Estos centros pueden facilitar la interacción entre docentes de diferentes disciplinas, fomentando la convergencia de conocimientos para abordar desafíos tecnológicos complejos.

Promoción de la Colaboración Internacional: Facilitar y promover oportunidades para la colaboración internacional, como intercambios académicos, participación en proyectos de investigación conjuntos con instituciones extranjeras y la organización de conferencias internacionales. Esto permitirá a los docentes investigadores de la Regional enriquecer sus perspectivas y contribuir a la investigación global.

Vinculación Efectiva con la Industria: Establecer mecanismos formales para la vinculación efectiva con el sector productivo. Esto podría incluir la creación de convenios y alianzas estratégicas, facilitando la transferencia de tecnología y conocimientos entre la academia y la industria.

Diseño de Cursos y Materiales Interactivos: Fomentar la creación de cursos y materiales didácticos interactivos que incorporen tecnologías educativas innovadoras. Estos recursos deben adaptarse a diversos estilos de aprendizaje y enfocarse en el desarrollo de habilidades prácticas, preparando a los estudiantes para los desafíos tecnológicos del mundo real.

Incentivos para la Participación en Proyectos de Innovación Educativa: Reconocer y recompensar el compromiso e involucramiento de los docentes investigadores en proyectos de innovación educativa. Estos proyectos pueden incluir el diseño de nuevas metodologías de enseñanza, la implementación de herramientas educativas tecnológicas y la evaluación continua de su efectividad.

Formación en Habilidades de Colaboración y Comunicación: Ofrecer programas de formación específicos en habilidades de colaboración y comunicación interdisciplinaria. Estas habilidades son esenciales para facilitar la colaboración efectiva entre docentes de diferentes áreas y para establecer conexiones sólidas con la industria.

La implementación de estas estrategias contribuirá significativamente a la readecuación del perfil docente/investigador en la Regional, fortaleciendo su capacidad para enfrentar los desafíos actuales y capitalizar las oportunidades emergentes en el ámbito tecnológico y educativo. CEPAL (2020)

### IV. EXPERIENCIAS EXITOSAS

La Facultad Regional Delta ha sido testigo de experiencias transformadoras protagonizadas por docentes/investigadores que han liderado con éxito la readecuación de sus perfiles, adaptándose a los desafíos contemporáneos. Este estudio de caso se centra en analizar prácticas exitosas y extraer lecciones aplicables para inspirar a otros profesionales de la UTN.

Se seleccionaron casos destacados de la Regional mediante entrevistas y revisión de sus perfiles académicos. Se analizaron sus experiencias, éxitos y estrategias adoptadas durante el proceso de readecuación.

*Desarrollo de Competencias Tecnológicas en la Facultad Regional Delta*

#### Caso de Éxito:

El Departamento de Ingeniería en Sistemas de Información (ISI), consciente de la importancia de mantener la actualización de la comunidad académica en un entorno tecnológico en constante evolución, lideró con éxito la implementación de un programa integral de capacitación en competencias tecnológicas. La participación entusiasta de docentes, no docentes, alumnos y graduados en cursos especializados abordó tanto el dominio de nuevas herramientas como la adopción de metodologías pedagógicas innovadoras.

El departamento ISI promovió la colaboración entre docentes, facilitando el intercambio de conocimientos y experiencias. Este enfoque enriqueció la comunidad académica, y también sentó las bases para la implementación exitosa de tecnologías innovadoras en el aula. Esta iniciativa inspiró a otros departamentos a seguir su ejemplo, creando un ambiente de aprendizaje continuo y adaptativo en la Facultad Regional Delta.

#### Lecciones Aplicables:

La experiencia del departamento ISI destaca la importancia de establecer programas de formación continua en competencias tecnológicas. Estos programas deben ser diseñados para adaptarse a las necesidades específicas de la comunidad académica, fomentando la interacción proactiva y brindando oportunidades para la aplicación práctica de lo aprendido en el contexto educativo.

#### *Investigación Aplicada y Vinculación con la Industria en la UTN:*

##### Ampliación del Caso de Éxito:

Docentes del departamento de Ingeniería Química lideraron un equipo de investigación que se destacó por la calidad de sus contribuciones académicas y también estableció una colaboración fructífera con empresas del sector tecnológico. Su enfoque en la investigación aplicada permitió la creación de soluciones prácticas que fueron adoptadas por la industria, demostrando el impacto directo de la investigación en el desarrollo tecnológico y económico.

Los docentes no solo llevaron a cabo investigaciones de relevancia, sino que también estableció mecanismos formales para vincular los resultados de la investigación con las necesidades específicas de la industria. Esto fortaleció la posición de la Facultad Regional Delta como líder en investigación aplicada y proporcionó a los estudiantes la oportunidad de participar en proyectos con un impacto tangible en el mundo real.

#### Lecciones Aplicables:

El caso de los docentes de Ingeniería Química resalta la importancia de incentivar la investigación aplicada y establecer vínculos formales con la industria. En la Facultad Regional Delta, esto implica fomentar la colaboración entre investigadores y empresas, facilitando la transferencia de conocimientos y tecnología para abordar desafíos específicos de la industria.

#### *Proyectos Interdisciplinarios e Innovación Educativa en la UTN:*

##### Ampliación del Caso de Éxito:

El Departamento de Ingeniería Mecánica lideró la creación

de un programa innovador de proyectos interdisciplinarios en la Facultad Regional Delta. Este programa abordó desafíos tecnológicos complejos y promovió la colaboración entre diferentes disciplinas. La intersección de la investigación y la enseñanza en proyectos prácticos permitió a los estudiantes experimentar de primera mano la aplicación de conocimientos teóricos en contextos reales.

El departamento de Ingeniería Mecánica implementó estrategias que fomentaron que los docentes y alumnos de diversas áreas se involucren, creando un ambiente propicio para el intercambio de ideas y enfoques. Este enfoque elevó la calidad de la enseñanza, además de generar proyectos innovadores que destacaron la relevancia de la Facultad regional Delta en el ámbito tecnológico.

#### Lecciones Aplicables:

El caso del departamento de Ingeniería Mecánica destaca la necesidad de impulsar la creación de programas interdisciplinarios que integren la investigación con la enseñanza. En la Facultad Regional Delta, esto implica la promoción de proyectos colaborativos que involucren a docentes y alumnos de diferentes disciplinas, brindando a los estudiantes experiencias educativas enriquecedoras y aplicadas.

## V. COMO IMPACTARIA EL DERECHO EN LA READECUACION

La interrelación entre la Informática y el Derecho en el tema de la Readecuación del Perfil Docente/Investigador en la Facultad Regional Delta se plantea desde una perspectiva multidisciplinaria que reconoce la importancia de ambas áreas en el contexto actual de la educación superior.

**Legislación sobre Tecnología Educativa:** La Informática y el Derecho se entrelazan en el marco regulatorio que regula el uso de tecnologías educativas en la enseñanza superior. El Derecho se encarga de establecer normativas relacionadas con la privacidad de los datos de los estudiantes, la accesibilidad digital, la propiedad intelectual de los materiales educativos en línea y otros aspectos legales relevantes. Los docentes/investigadores deben estar al tanto de estas regulaciones para garantizar el cumplimiento ético y legal en el uso de la tecnología en el ámbito académico.

**Protección de Datos y Seguridad Informática:** La Informática y el Derecho convergen en la protección de datos personales y la seguridad informática en el contexto educativo. Los docentes/investigadores deben considerar aspectos legales relacionados con la recopilación, almacenamiento y uso de datos de los estudiantes en plataformas educativas en línea, así como implementar medidas de seguridad cibernética para proteger la integridad de la información.

**Propiedad Intelectual y Derechos de Autor:** La Informática y el Derecho se entrecruzan en la gestión de la propiedad intelectual y los derechos de autor en el ámbito académico. Los docentes/investigadores deben estar familiarizados con las leyes de propiedad intelectual que regulan la creación y distribución de materiales educativos digitales, así como con las licencias de uso de software y contenido en línea. Esto implica asegurar que se respeten los derechos de autor y promover el

acceso abierto al conocimiento cuando sea posible.

Ética y Responsabilidad Digital: La Informática y el Derecho convergen en el ámbito de la ética y la responsabilidad digital en la educación superior. Los docentes/investigadores deben promover prácticas éticas en el uso de la tecnología, incluida la prevención del plagio digital, el respeto a la propiedad intelectual y la promoción de un entorno en línea inclusivo y respetuoso. Además, deben estar al tanto de las implicaciones legales de su conducta en línea y actuar con responsabilidad en el entorno digital..

## VI. CONCLUSIONES Y TRABAJO A FUTURO

La investigación sobre la readecuación del perfil docente/investigador en la Facultad Regional Delta de la UTN revela la complejidad y la vital importancia de adaptarse a un entorno académico en constante evolución. En un escenario marcado por rápidos avances tecnológicos, transformaciones pedagógicas y una creciente interconexión global, la figura del docente/investigador se encuentra en el epicentro de cambios significativos. La intersección entre la docencia y la investigación se presenta como esencial para la calidad de la educación superior, para la contribución de la institución al desarrollo de la sociedad y la generación de conocimiento.

La adaptación continua se destaca como un requisito esencial para el éxito profesional y la pertinencia académica. Docentes e investigadores enfrentan desafíos que van desde la integración efectiva de nuevas tecnologías hasta la respuesta a las cambiantes expectativas de los estudiantes y las demandas emergentes de la sociedad. Sin embargo, también se presentan oportunidades para enriquecer la labor académica a través de la interdisciplinariedad, la colaboración internacional y la vinculación efectiva con el sector productivo.

### *Líneas de acción a futuro:*

**Desarrollo Profesional Continuo:** Implementar programas específicos de desarrollo profesional que aborden las habilidades tecnológicas emergentes y las metodologías de enseñanza innovadoras. Talleres, cursos en línea y certificaciones pueden mantener actualizados a los docentes/investigadores.

**Fomento de la Investigación Aplicada:** Establecer incentivos para la investigación aplicada, reconociendo proyectos con impacto directo en la solución de problemas prácticos de la industria. Esto fortalecerá la conexión entre la academia y el sector productivo.

**Creación de Centros de Innovación:** Establecer centros de innovación que promuevan la colaboración interdisciplinaria. Estos espacios pueden facilitar la convergencia de conocimientos para abordar desafíos tecnológicos complejos.

**Promoción de la Colaboración Internacional:** Facilitar oportunidades para la colaboración internacional, como intercambios académicos y participación en proyectos conjuntos, enriqueciendo perspectivas y contribuyendo a la investigación global.

**Vinculación Efectiva con la Industria:** Establecer mecanismos formales para la vinculación efectiva con el sector productivo, mediante convenios y alianzas estratégicas,

facilitando la transferencia de tecnología y conocimientos.

**Diseño de Cursos Interactivos:** Fomentar la creación de cursos y materiales didácticos interactivos que incorporen tecnologías educativas innovadoras. Estos recursos deben adaptarse a diversos estilos de aprendizaje y enfocarse en el desarrollo de habilidades prácticas.

**Incentivos para Proyectos de Innovación Educativa:** Reconocer y recompensar la participación comprometida en proyectos de innovación educativa, incluyendo el diseño de nuevas metodologías de enseñanza y la implementación de herramientas educativas tecnológicas.

**Formación en Habilidades de Colaboración:** Ofrecer programas de formación en habilidades de colaboración y comunicación interdisciplinaria, esenciales para facilitar la colaboración efectiva entre docentes de diferentes áreas y establecer conexiones sólidas con la industria.

Estas líneas de acción, basadas en lecciones extraídas de experiencias exitosas en la Facultad Regional Delta, apuntan a fortalecer la capacidad del docente/investigador para afrontar los desafíos contemporáneos y capitalizar las oportunidades emergentes en el ámbito tecnológico y educativo.

## VII. BIBLIOGRAFÍA

Aznar Minguet, P., Ull, M. A., Piñero, A., & Martínez-Agut, M. P. (2014). La Sostenibilidad En La Formación Universitaria: Desafíos Y Oportunidades. Educación XX1, 17(1), 133-158.

CEPAL (2020) Educación, juventud y trabajo: Habilidades y competencias necesarias en un contexto cambiante.

Fernández Mc Cann, D. (2012). Impacto de las tecnologías de la información y comunicación en la educación superior. Ingeniería Y Sociedad, (4), 21–28. Recuperado a partir de <https://revistas.udea.edu.co/index.php/ingeso/article/view/11671>

Florencia Santi, M., (2015). VULNERABILIDAD Y ÉTICA DE LA INVESTIGACIÓN SOCIAL: PERSPECTIVAS ACTUALES. Revista Latinoamericana de Bioética, 15(2), 52-73.

Hernández Arteaga, I., (2009). El docente investigador en la formación de profesionales. Revista Virtual Universidad Católica del Norte, (27), 1-21.

Kentucky Department of Education (2020) Characteristics of Highly Effective Teaching and Learning (CHETL). Recuperado de: [https://education.ky.gov/curriculum/standards/teachtools/Pages/Characteristic-s-of-Highly-Effective-Teaching-and-Learning-\(CHETL\)](https://education.ky.gov/curriculum/standards/teachtools/Pages/Characteristic-s-of-Highly-Effective-Teaching-and-Learning-(CHETL))

McLaughlin, P. (2020). From Small Things: Building Cross-Disciplinary, Transformative Learning Experiences Through a Global Mobility Experience for Higher Education Students In: Tertiary Education in a Time of Change, Springer, Singapore.



# Recomendaciones para una infraestructura legal y normativa adecuada en organizaciones de I+D y Gestión de la Propiedad Intelectual en disciplinas STEM

D'Onofrio, Antonela, Giaccaglia, María Fernanda, Otero, María Cecilia, Ruiz De Angeli, Gonzalo Matias

**Abstract**—Las instituciones universitarias, grandes generadoras de conocimiento, necesitan contar con una infraestructura legal y normativa adecuada que facilite la producción de bienes intangibles y brinde los mecanismos necesarios para garantizar su protección y adecuada gestión. La Universidad Fasta (UFASTA) es consciente de esta necesidad y, por este motivo, hace algunos años trabaja para procurar una infraestructura de este tipo que esté a la altura de las circunstancias. De esta manera, ha desarrollado una *Guía de Recomendaciones para contar con una Infraestructura Legal y Normativa* que permita alcanzar esos objetivos, planteando la necesidad de desarrollar diferentes áreas clave (AC). Siguiendo estas recomendaciones, se decidió profundizar en un AC, orientada a la protección de bienes intangibles: *Gestión de la Propiedad Intelectual*. Para recorrer este camino, se relevaron instituciones referentes, normativa existente y se diagnosticó la realidad intra institucional, lo que permitió entender y priorizar los pasos a seguir.

**Index Terms**—propiedad intelectual, políticas, régimen, capital intelectual.

## I. INTRODUCCIÓN

En el presente trabajo haremos mención a un conjunto de recomendaciones de diseño institucional que constituyó el punto de partida para la redacción de una Guía orientadora en la conformación de la Infraestructura Legal y Normativa para organizaciones I+D en disciplinas STEM<sup>1</sup>.

La Guía constituye el producto de un trabajo de varios años llevado a cabo entre las Facultades de Ingeniería y de Ciencias Jurídicas y Sociales de la Universidad Fasta, como resultado del proyecto de investigación en conjunto, titulado: *Desarrollo de un*

*Modelo de Infraestructura Legal y Normativa para organizaciones de I+D de disciplinas STEM.*

No puede perderse de vista que contar con el adecuado marco legal y normativo facilita el crecimiento y la interacción de las organizaciones, a la vez que les permite perseguir los objetivos buscados y proteger los derechos personales e institucionales.

En disciplinas STEM, donde se presenta una fuerte vocación interinstitucional, resulta de vital importancia proponer un modelo legal y normativo que facilite el crecimiento de las organizaciones, de la mano de una adecuada protección de sus bienes intangibles. La ausencia de un marco adecuado de este tipo puede generar algunas problemáticas para el desarrollo de distintas actividades de la organización, por la insuficiente orientación para la toma de decisiones, la eventual generación de inconsistencias convencionales y/o contractuales, entre otras, lo que fundamenta fuertemente contar con los instrumentos necesarios en este sentido.

Es partiendo de las premisas anteriores que nos propusimos el diseño de un *Modelo* con fuerte vocación de trabajo interinstitucional, que tuvo como finalidad principal aportar una guía rápida para su implementación.

La estructura del modelo partió de la definición de distintas áreas estratégicas o claves, las que iremos mencionando en el desarrollo del presente, y enfocándonos luego en el estudio de la *gestión de la propiedad intelectual*, por los motivos que analizaremos consecuentemente.

---

<sup>1</sup> STEM se refiere a Science, Technology, Engineering and Mathematics en su sigla en inglés (Ciencia, Tecnología, Ingeniería y Matemáticas).

En este sentido, a los efectos de procurar la consecución del objetivo, se abordó la problemática desde dos aspectos centrales: el *status quo* y el abordaje intrainstitucional de la cuestión.

En el primer aspecto, se realizó un relevamiento de instituciones referentes, sus modelos organizacionales y normativos, como así también de la normativa vigente tanto a nivel nacional, regional, como internacional.

En el segundo aspecto, se realizó un estudio de la misión y visión de la institución sobre la que se asentó el proyecto, las normativas vigentes, reglas básicas que regulan su desempeño y su plan estratégico. Este último aspecto nos permitió generar propuestas dentro de la estructura organizacional que respondan a las necesidades planteadas en el proyecto.

## II. LA GUÍA DE RECOMENDACIONES

La redacción de la Guía “*Recomendaciones para el desarrollo de herramientas que permitan contar con una infraestructura legal y normativa para organizaciones de I+D en disciplinas STEM*”, como mencionamos anteriormente, es el resultado de un proyecto de investigación interdisciplinario, llevado a cabo por investigadores de las Facultades de Ingeniería y de Ciencias Jurídicas y Sociales de la UFASTA.

El proyecto al que hacemos referencia tuvo como objetivo principal desarrollar un modelo de infraestructura legal y normativa para organizaciones de I+D en disciplinas STEM, con fuerte vocación de vinculación interinstitucional.

La finalidad principal de la guía consistió en la redacción de algunas recomendaciones de implementación de dicho modelo.

Es así como esta Guía propone:

- Exponer la importancia de contar con esta herramienta.
- Identificar claramente las áreas clave.
- Brindar diferentes enfoques organizacionales con respecto a su estructura para facilitar los procesos clave.
- Proponer algunos diagnósticos organizacionales para entender el punto de partida.

- Brindar una guía rápida para poder implementar estas herramientas en organizaciones reales en un contexto real.

Tal como dijimos anteriormente, el marco normativo y organizacional debe ser una herramienta que facilite que las organizaciones, como pueden ser las universidades, aprovechen las oportunidades de creación, transmisión y aplicación de conocimientos. En pocas palabras, debe ser un facilitador que guíe el desarrollo de la universidad hacia sus metas mientras promueve la libertad de acción y la búsqueda de oportunidades.

## III. EL CAMINO RECORRIDO

Teniendo en cuenta los objetivos trazados, estimamos adecuado relevar y analizar cuál era el abordaje existente en instituciones referentes, respecto de la existencia o no de una infraestructura legal que permitiera dar respuesta a la generación de conocimiento en un contexto de continuo desarrollo y avance tecnológico, así como su alcance en caso de existir.

Desde otra perspectiva, analizamos la normativa vigente a nivel nacional, regional e internacional en la búsqueda de una marco común que resultara orientador a la hora de diseñar el modelo.

En consecuencia, nuestro análisis partió de relevar más de 60 fuentes de información, sobre la base de dos ejes: el normativo y bibliográfico por un lado, y el institucional por otro.

En relación a las fuentes normativas y bibliográficas, los instrumentos relevados más destacados a mencionar consisten en:

- los reglamentos, ordenanzas y resoluciones de otras instituciones universitarias, tales como la Universidad Nacional de Cuyo, la Universidad Austral, la Universidad Nacional de San Juan, la Universidad Nacional de La Plata, la Universidad Nacional del Litoral, la Universidad de Buenos Aires, la Universidad Católica del Norte, para mencionar algunas, evidenciaron que la normativa institucional se encuentra

principalmente orientada a la protección de bienes intangibles a través de regímenes de propiedad intelectual, así como la regulación de los compromisos de confidencialidad que deben asumir los intervinientes. Otro gran aspecto regulado consiste en la transferencia de tecnología y la innovación, como es el caso de la Universidad Nacional de Quilmes a través del Centro Interdisciplinario de Estudios en Ciencia, Tecnología e Innovación (CIECTI) y la Universidad Tecnológica Nacional a través de su reglamento para la creación y funcionamiento de Centros de I+D;

- la norma modelo *Sumar Valor* [1][2] sobre Protección y Comercialización de los resultados de las actividades de enseñanza, investigación y/o extensión para instituciones de educación superior y organismos que conforman el Sistema Nacional de Ciencias Tecnología e Innovación, desarrollada en 2016 en el marco del Programa Nacional de Gestión de la Propiedad Intelectual y de la Transferencia Tecnológica, resultado de la labor conjunta de universidades nacionales, el CONICET, el ITBA, el INTA y el INTI;
- los convenios del CONICET que abordan diversos aspectos de la vinculación tecnológica, aportando modelos para formalizar los vínculos interinstitucionales en la materia;
- la normativa internacional resultante de diversas instituciones, arroja la misma tendencia en cuanto a promover la regulación en materia de propiedad intelectual, si bien con algunos aportes en materia de indicadores de vinculación y estructura organizacional, tal como, las reglamentaciones de la Unión Europea, de la Universidad Autónoma de Barcelona, el MIT o el Observatorio Iberoamericano de la Ciencia, Tecnología y la Sociedad (OCTS-OEI) que en conjunto con la Red Iberoamericano de Indicadores de Ciencia y Tecnología (RICYT), desarrollaron el Manual de Valencia.

Por otro lado, se realizó un relevamiento de instituciones referentes en la temática, y sus modelos

legales y normativos, en función de los siguientes criterios:

- Vocación interinstitucional.
- Propiedad intelectual y patentes.
- Régimen de cesiones y donaciones.
- Régimen de confidencialidad.
- Reglamento operacional.

Para ello, consultamos por un lado bibliografía específica que nos permitiera identificar de modo adecuado cuáles eran las características y funciones esperadas de las oficinas de transferencia tecnológica o espacios de investigación, desarrollo y transferencia de tecnología independientemente de la institución u organismo en los cuales estuvieran inmersos; y, por otro, indagamos sobre los modelos adoptados por instituciones líderes tales como UNL-CETRI (Centro para la Transferencia para los resultados de la Investigación de la Universidad Nacional del Litoral), la UNQ (Universidad Nacional de Quilmes), UNT (Universidad Tecnológica Nacional), el CONICET (Consejo Nacional de Investigaciones Científicas y Técnicas de Argentina), UNSJ (Universidad Nacional de San Juan), entre más de 10 instituciones/organizaciones relevadas.

Los ejes claves relevados fueron los siguientes:

- visión y misión de la organización como base fundante de la misma, capacidad jurídica de la organización;
- autonomía/autarquía económica;
- instrumentos facilitadores que promuevan la vinculación interinstitucional;
- régimen de propiedad de los bienes producidos;
- registración;
- régimen de confidencialidad de los miembros integrantes;
- desvinculación;
- responsabilidad;
- modelos de contratos tales como donaciones;
- cesiones;
- licencias de uso;
- licenciamiento de productos;
- reglamento de operaciones.

Por otra parte, las instituciones relevadas fueron categorizadas según los siguientes criterios:

- Acceso a la información: ya que no todas las organizaciones proveen información sobre sus políticas, procesos, estructura interna, objetivos, entre otros, lo que nos llevó a seleccionar aquellas con información disponible en volumen, calidad y profundidad.
- Trayectoria/Madurez: también se evaluó la trayectoria de la organización a lo largo de los años con relación a la actividad académica y/o de I+D, además de la madurez que demostraron en sus procesos clave asociados a la explotación de resultados de investigación.
- Afinidad con la actividad académica y de I+D: se priorizaron organizaciones gubernamentales, no gubernamentales sin fines de lucro y educativas ; dejando de lado instituciones exclusivamente con finalidad comercial.
- Estructura organizacional: poseen estructuras especializadas para la gestión de I+D. Algunas de las organizaciones proveen un detalle de su estructura organizacional que sirvió como referencia para esta etapa.

Es importante destacar que no existe un único modelo de gestión de la transferencia y de la propiedad intelectual. Muy por el contrario, a nivel nacional e internacional, los organismos líderes en las temáticas aplican una diversidad de enfoques y métodos para la generación y explotación de la propiedad intelectual y las actividades de transferencia de tecnología, todo ello en base a factores tales como su tamaño, el presupuesto y los recursos humanos disponibles, así como también las características propias del entorno, entre otros aspectos.

Algunas de las organizaciones relevadas fueron: Universidad Nacional de Cuyo, CONICET, Universidad Nacional de San Juan, Universidad Austral, Instituto Nacional de Propiedad Intelectual, Oficina Española de Patentes y Marcas, OTRI - Universidad Hernández España, Universidad Tecnológica Nacional, Universidad Nacional del

Litoral, CETRI-UNL Centro para la Transferencia de los Resultados de Investigación, Universidad Nacional de Quilmes, MIT Instituto de Tecnología Massachusetts, Laboratorio de Investigación y Formación en Informática Avanzada, Universidad Nacional de La Plata, CIECTI - Centro Interdisciplinario de Estudios de Ciencia, Tecnología e Innovación dependiente de la Universidad Nacional de Quilmes, COTEC, Universidad Católica del Norte de Chile, EEAD - Instituto de investigación perteneciente al Ministerio de Economía y Competitividad de España, UE - Unión Europea, CCS - Conferencia de Consejos Sociales de las Universidades de España.-

También, en la etapa de investigación se detectó la existencia de otras fuentes bibliográficas que permiten la generación de conocimiento en la materia: uno de ellos es el Manual de Valencia, comentado anteriormente en este documento; otro fue la Norma Modelo sobre Protección y Comercialización de los resultados de las actividades de enseñanza, investigación y/o extensión para instituciones de educación superior y organismos que conforman el Sistema Nacional de Ciencia Tecnología e Innovación; por último, tuvimos en cuenta la Guía de Buenas prácticas en gestión de la transferencia de tecnología y de la propiedad intelectual en instituciones y organismos del sistema nacional de ciencia, tecnología e innovación, guía que fue elaborada en el año 2013 por el Ministerio de Ciencia, Tecnología e Innovación Productiva, y su objetivo principal es constituirse en una herramienta de consulta para poder identificar lineamientos y directrices fundamentales referidas a qué actividades se deberían planificar e implementar con el objetivo de realizar una gestión efectiva de la transferencia de tecnología y la propiedad intelectual.

Expresado en números, el relevamiento organizacional involucró a 18 instituciones en total, de las cuales poco más del 50% son de carácter nacional y cerca del 80% de gestión pública frente a un 20% de gestión privada. A su vez el 47% de las organizaciones relevadas fueron Universidades, un 33% Instituciones de I+D de otra naturaleza.

Todo ello nos permitió abordar el diseño del *Modelo* teniendo en consideración las diferentes alternativas que en mayor o menor profundidad fueron objeto de regulación y formalización en diversas instituciones.

#### IV. MODELO ILyN-STEM

Para que las organizaciones de I+D en disciplinas STEM puedan realizar con éxito sus actividades sustantivas (docencia, investigación y extensión), necesitan contar con una adecuada infraestructura legal y normativa que facilite esto.

De esta manera, para partir de un punto de referencia que abarque todos los ejes y aspectos que debe contener dicha infraestructura, se desarrolló un Modelo denominado ILyN-STEM. Dicho modelo brinda recomendaciones, buenas prácticas y herramientas, planteando Puntos de Abordaje Clave (PAC) que se entendieron como fundamentales para desarrollar y contar en instituciones con las características mencionadas:

- 1) Buenas prácticas asociadas a la definición de la Misión y Visión de la organización.
- 2) Identificación de Áreas estratégicas y definición de procesos clave.
- 3) Propuesta de Estructura organizacional.
- 4) Normativa y cláusulas para la promoción de la generación de resultados de investigación y la protección de la propiedad intelectual.
  - a. Beneficios económicos de la organización.
  - b. Beneficios económicos de los docentes e investigadores.
  - c. Acuerdos de confidencialidad.
  - d. Contratos de cooperación.
  - e. Contratos de desarrollo concertado.
  - f. Declaración de Resultados de Investigación (obligación de comunicar resultados y evaluación de los mismos).
  - g. Financiamientos.
  - h. Licencias de Derechos de Propiedad Intelectual.
  - i. Licencias de Software.
  - j. Licencias: exclusivas y no exclusivas, territoriales o universales, indefinidas o temporales.
  - k. Patentes.
  - l. Registro de software.
  - m. Titularidad (cesión, exclusiva de la entidad o del investigador, conjunta, de terceros).

- n. Canales de transferencia.
- o. Uso de Marcas.

Con relación a los PAC mencionados, sobre identificación de Áreas Estratégicas y definición de procesos clave, el modelo propone desarrollar 5 (cinco) áreas clave, entendiendo que, necesariamente, deben formar parte de la estructura organizacional de la institución:

1. Vinculación Tecnológica (VT) [3]: tiene como propósito vincular los conocimientos y resultados de I+D con la sociedad, para hacer una contribución a su desarrollo. Además, permite mejorar la posición competitiva de la institución.
2. Vigilancia Tecnológica e Inteligencia Estratégica (VTelE): para monitorear y conocer las tecnologías disponibles y emergentes, para que permita orientar los objetivos y los esfuerzos para alcanzarlos. Es fundamental para mejorar la toma de decisiones en la institución, por ejemplo, en materia de protección de los bienes intangibles
3. Asesoramiento Legal Intrainstitucional (ALI): para contratos, acuerdos de confidencialidad [4], licencias de uso y goce, cesiones de derechos, registración de derechos o marcas.
4. Financiamiento, Gestión Económica y Vigilancia Financiera (VF): para una adecuada gestión económica y para el conocimiento y dominio de las diferentes estrategias de financiamiento (convocatorias, redes de financiamiento, fondos externos) y la identificación de oportunidades para acceder a estos tipos de ingresos.
5. Gestión de la Propiedad Intelectual (GPI): para garantizar el mayor beneficio público que sea posible del bien intangible producido, al mismo tiempo de asegurar su protección y su adecuada explotación, sobre la base de políticas definidas por cada organización involucrada en lo producido [5].

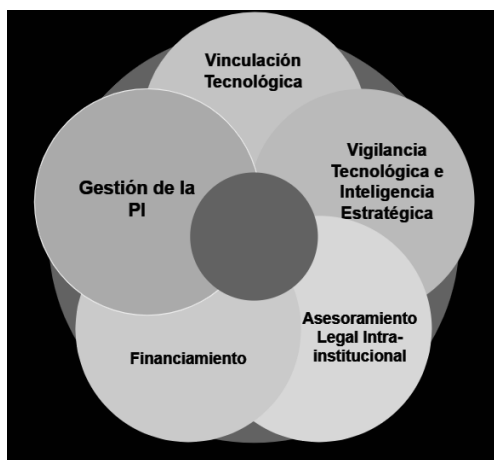


Fig. 1. Áreas clave que propone abordar el modelo ILyN-STEM en organizaciones de I+D en disciplinas STEM.

Cada una de estas áreas, debe brindar diferentes servicios a la institución a través de la implementación de distintos procesos con objetivos concretos, lo que le da un significado funcional a cada una de dichas áreas y dan vida a las actividades claves de la institución.

Además de estos procesos, se necesita de un adecuado marco legal y normativo. Las organizaciones en general, y las instituciones de I+D en disciplinas STEM en particular, necesitan contar con herramientas adecuadas para facilitar el desarrollo de sus actividades, promover la generación de bienes intangibles y garantizar su adecuada protección, además de impulsar su explotación.

Existen diferentes tipos de estructuras organizacionales que reflejan el enfoque que éstas pretenden darle a la generación de bienes intangibles, a la identificación de bienes para su protección y potencial explotación y a la transferencia tecnológica. Estos enfoques, muy probablemente dependen de la madurez organizacional, de su tamaño, de sus objetivos estratégicos e, inevitablemente, del entorno o contexto que toca atravesar. El Modelo ILyN-STEM identifica 3 (tres) modelos de organización legal y normativa y de vinculación y transferencia (OLNVT): modelo *in-house*; modelo de nodos territoriales; modelo de tercerización. El primer modelo propone una estructura adecuada para cuando el objetivo es

generar una cultura de I+D+i y transferencia hacia dentro de la organización. En el caso del segundo modelo, el objetivo es la generación de dicha cultura, pero en una determinada región, por ejemplo, a través de una OLNVT que gestione a varias universidades de una determinada región. Por último, en el tercer caso, es el indicado cuando el principal objetivo es maximizar el aprovechamiento de oportunidades de explotación y comercialización de los productos generados por la institución, minimizando la inversión.

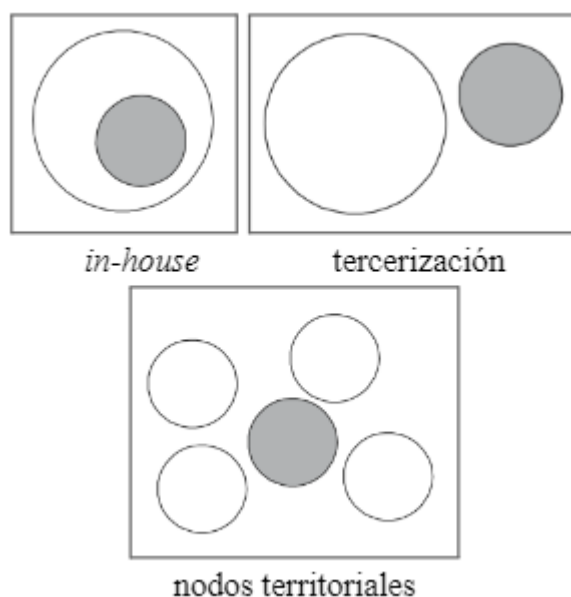


Fig. 2. Modelo de estructura organizacional legal y normativa.

## V. APLICACIÓN DEL MODELO - OBJETIVO PRINCIPAL DE LA GUIA

Por último, para poder aplicar el modelo en instituciones reales, es necesario un plan de implantación o implementación del mismo. Dicho proceso debe contar con tres actividades principales a llevar a cabo:

- 1) Análisis del entorno: análisis del contexto Político, Económico, Social, Tecnológico y Legal; análisis de la competencia. Su objetivo es identificar oportunidades y amenazas.
- 2) Diagnóstico organizacional: para identificar fortalezas y debilidades, comprender cuál es la cultura organizacional, sus valores, qué

conocimiento posee y potencialmente puede generar y conocer su Plan Estratégico, dado que la aplicación del modelo, tiene que facilitar alcanzar los objetivos que en éste se hayan definido.

- 3) Plan: donde se definan los objetivos que se pretenden alcanzar (los cuales tienen que estar alineados con el Plan Estratégico de la organización), las acciones a ejecutar para alcanzarlos y los resultados esperados.



Fig 3. Proceso para la aplicación del Modelo ILYN-STEM.

## VI. IMPORTANCIA DE ABORDAR CON PRIORIDAD LA GESTIÓN DE LA PROPIEDAD INTELECTUAL

Tal como indicamos previamente, nuestro modelo identificó 5 AC a desarrollar a fin de contar con una adecuada estructura legal y normativa para organizaciones I+D en disciplinas STEM.

Todas ellas merecen atención particularizada, y una exploración profunda de alternativas, herramientas, modelos que fortalezcan su desarrollo, por lo tanto, cuando llegó el momento de definir cuál de ellas abordaríamos, el contexto tecnológico, económico y de desarrollo acelerado de la economía del conocimiento junto a algunas particularidades institucionales vinculadas a la protección de los intangibles generados en la Universidades, nos facilitó la decisión.

No resulta ajeno de modo alguno que en la era del conocimiento, las instituciones I+D+i deben contar con políticas bien definidas en lo que hace a la protección de sus intangibles, de modo de contar con reglas institucionales claras para sí, sus equipos y terceros.

Las organizaciones de I+D, y en particular las universidades, al generar un gran caudal de bienes

intangibles, necesitan contar con herramientas que garanticen un abordaje integral de la Propiedad Intelectual.

Dicho abordaje debe comprender desde la definición de políticas y valores institucionales en torno a la Propiedad Intelectual, la identificación, definición, encuadre y tipificación de los bienes intangibles generados, su adecuado tratamiento, la eventual protección, y la administración y explotación de los recursos generados a partir de los mismos.

En este sentido, es que, desde organizaciones nacionales e internacionales referentes en la temática, se resalta la relevancia de una adecuada gestión integral de la Propiedad Intelectual, la cual a grandes rasgos permite: proteger la innovación incentivar la inversión en investigación y desarrollo de tecnología, facilitar la transferencia de tecnología, promover la innovación mediante la colaboración y la interdisciplina.

Particularmente, la Organización Mundial de la Propiedad Intelectual (OMPI) [6] trata esta cuestión diciendo:

“La propiedad intelectual es un instrumento importante en el ámbito de la investigación y el desarrollo. Ayuda a garantizar la titularidad sobre los resultados de la actividad intelectual y la capacidad de controlar el uso de la Propiedad Intelectual en armonía con la misión y los valores fundamentales de una institución.

La Propiedad Intelectual también es una poderosa herramienta de negocios que permite establecer una posición en el mercado y reivindicar derechos exclusivos con respecto a un nuevo producto o proceso. Esto la transforma en un instrumento importante para atraer asociados y posiblemente obtener un rendimiento sobre la inversión en investigación y desarrollo.”

<https://www.wipo.int/technology-transfer/es/>

Así es que, analizando la normativa vigente tanto a nivel nacional como internacional, el estado de la cuestión en otras instituciones educativas de la Argentina, la realidad actual de la Universidad FASTA y la interpelación realizada por organismos internacionales como la OMPI o el Ministerio de Ciencia y Tecnología en esta materia, asumimos la responsabilidad de trabajar en herramientas



adecuadas para la gestión integral de la Propiedad Intelectual en nuestra institución, la cual puede ser escalada a cualquier otra institución que tenga similares características e idénticas necesidades.

La Guía Orientadora en la conformación de la Infraestructura Legal y Normativa para organizaciones I+D en disciplinas STEM, busca, ni más ni menos, que desarrollar un modelo de infraestructura legal y normativa que tenga como finalidad principal servir como instrumento para que el desarrollo de las actividades de la organización pueda orientarse con facilidad al aprovechamiento de las oportunidades de generación, transmisión y aplicación de conocimiento, entre ellas la generaciones y producción de bienes intangibles sujetos a ser regulados mediante los institutos de la Propiedad Intelectual.

El modelo propuesto por la Guía antes citada, identifica la necesidad de establecer un área de gestión de la propiedad intelectual orientado a dotar de protección a los bienes y servicios resultantes de la actividad universitaria en particular y de las organizaciones de I+D en general en sus diversos aspectos, para lo cual es necesario contar con un marco regulatorio de la Propiedad Intelectual.

### *Marco Regulatorio de la Propiedad Intelectual*

En razón de todo lo expuesto anteriormente y con la intención de profundizar en el abordaje integral de la Propiedad Intelectual, identificada como área clave y estratégica de nuestra Institución, hoy en día nos encontramos en proceso de redacción de la normativa o marco regulatorio de la Propiedad Intelectual en la Universidad FASTA.

El documento SUMAR VALOR [1],[2], norma modelo sobre Protección y Comercialización de los Resultados de las actividades de enseñanza, investigación y/o extensión para instituciones de educación superior y organismos que conforman el Sistema Nacional de Ciencia, Tecnología e Innovación, recurso inspiracional del proyecto menciona:

“El diseño de marcos normativos específicos y adecuados es uno de los factores clave para una eficaz y eficiente protección, valoración y comercialización de los resultados de las actividades

de enseñanza, investigación y extensión de los diferentes actores que componen el Sistema Nacional de Ciencia, Tecnología e Innovación.”.

En este sentido, el desafío asumido de redactar una normativa que trate de manera integral la Propiedad Intelectual implica reconocer el valor de todo el trabajo que nuestra institución y sus miembros vienen desarrollando desde hace ya más de 30 años. En consecuencia, destacar y fidelizar la labor de docentes, investigadores, extensionistas, estudiantes y equipo de gestión, favorecer el crecimiento y fortalecimiento organizacional, propiciar el trabajo colaborativo e interdisciplinario, fomentar la inversión en investigación, posicionar a la universidad en materia de investigación y desarrollo, como así también, crear espacios de innovación y mejora continua.

## VII. RELEVAMIENTO INTERNO Y DE OTRAS INSTITUCIONES PARA EL ABORDAJE DE LA GESTIÓN DE LA PROPIEDAD INTELECTUAL

Siguiendo las propias recomendaciones, se llevó adelante un relevamiento sobre la Gestión de la Propiedad Intelectual en UFASTA y de otras organizaciones, para poder comenzar con el desarrollo de una de las áreas clave que el modelo ILyN-STEM y la Guía recomiendan abordar: la Gestión de la Propiedad Intelectual.

El relevamiento se realizó en 4 grandes ejes:

1. De las necesidades de la UFASTA, con una visión holística, en relación a la Gestión de la Propiedad Intelectual.

Se realizó una encuesta destinada a actores clave de la universidad para poder complementar el relevamiento. Preparamos un formulario de Google que fue enviado a los responsables de las siguientes áreas:

- Unidades Académicas.
- Colaboratorio de Innovación.
- Biblioteca.
- Revista In Itinere.
- InFo-Lab (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense).

- Área de investigación.
  - Área de Extensión.
  - Subsecretaría Legal y Técnica.
2. De la normativa existente con relación a la Protección de la Propiedad Intelectual. Este relevamiento fue realizado en dos niveles:
    - 1er Etapa: a nivel nacional.
    - 2da Etapa: a nivel regional e internacional.
  3. De los regímenes de protección de la propiedad intelectual en otras instituciones. Normativa vigente nacional e internacional en materia de propiedad intelectual.
  4. De los regímenes o soluciones en la UFASTA.

Finalmente, en la actualidad, estamos desarrollando en este momento una propuesta de régimen para atender a las necesidades internas concretas de nuestra institución.

## VIII. CONCLUSIONES

Tanto el desarrollo del proyecto de investigación, como el diseño de la Guía nos ha permitido arribar a algunas conclusiones que compartimos a continuación.

En primer lugar, definir un modelo de infraestructura legal y normativa orientado a que las organizaciones de I+D en disciplinas STEM puedan realizar con éxito sus actividades sustantivas de modo articulado no ha sido una tarea sencilla dada la diversidad de instituciones que convergen en tales actividades y que resultan heterogéneas desde su conformación, estructura legal, nivel de crecimiento, sostenibilidad económica, para mencionar algunos aspectos.

Por otro lado, no existe un régimen normativo común, que defina una orientación clara, dependiendo de las particularidades institucionales y el contexto en el cual se encuentra inserto.

Ante ello, el modelo partió de la definición de áreas clave que entendemos necesarias y lo

suficientemente abarcativas teniendo en cuenta los fines propuestos.

La Guía “*Recomendaciones para el desarrollo de herramientas que permitan contar con una infraestructura legal y normativa para organizaciones de I+D en disciplinas STEM*”, que aquí presentamos propone un método y un recorrido a fin de poder implementar el modelo teniendo en miras las particularidades institucionales.

A partir de allí, tal como mencionamos anteriormente, definimos la necesidad de profundizar El abordaje de la propiedad intelectual a través de políticas organizacionales, toda vez que fortalece y propicia la generación de producciones científicas y tecnológicas, generando un impacto trascendental en las funciones esenciales de la universidad: docencia, investigación y extensión. Todo ello promueve una virtuosa retroalimentación entre la generación de conocimiento, la transferencia de los mismos y, como resultado, la obtención de beneficios económicos para la institución.

En razón de ello, es vocación de este grupo de investigación profundizar y desarrollar con compromiso las áreas claves y estratégicas de nuestra institución como las mencionadas.

En efecto, generar un círculo virtuoso entre las organizaciones de I+D, sus miembros y la sociedad en las que se encuentran inmersas.

## IX. REFERENCIAS

1. SUMAR VALOR (2016) . Norma modelo sobre protección y comercialización de los resultados de las actividades de enseñanza, investigación y/o extensión para instituciones de educación superior y organismos que conforman el Sistema Nacional de Ciencia, Tecnología e Innovación.
2. SUMAR VALOR (2013). Guía de Buenas Prácticas en Gestión de la Transferencia de Tecnología y de la Propiedad Intelectual en Instituciones y Organismos del Sistema Nacional de Ciencia, Tecnología e Innovación. Programa Nacional de Gestión de la Propiedad Intelectual y de la Transferencia Tecnológica.
3. ALBORNOZ, M., BARRERE, R., CASTRO, M. E., & CARULLO, J. C. (2017). Manual Iberoamericano de

Indicadores de Vinculación de la Universidad con el Entorno Socioeconómico. Manual de Valencia. Observatorio Iberoamericano de la Ciencia, la Tecnología y la Sociedad (OCTS-OEI) Red Iberoamericana de Indicadores de Ciencia y Tecnología (RICYT)(Ed.).

4. InFo-Lab (2019). Compromiso de confidencialidad. Laboratorio de Investigación y Desarrollo de Tecnología en

Informática Forense. Universidad FASTA, Ministerio Público

Fiscal Pcia de Buenos Aires y Municipalidad de General Pueyrredón.

5. DI IORIO, A. H. (2018). Gestión de la Propiedad Intelectual de un Laboratorio de Investigación y Desarrollo de Tecnología Interinstitucional. Apuntes sobre el Caso InFo-Lab. Trabajo Final Integrador Curso de Postgrado “Gestión de la Propiedad Intelectual”. Universidad Nacional de Mar del Plata, Argentina.

6. OMPI. ¿Qué es la propiedad intelectual?. Recuperado de <https://www.wipo.int/about-ip/es/>.

# Tecnología H5P y aprendizaje autodirigido

Ballesteros Carlos<sup>1</sup>, Filippi Jose Luis<sup>2</sup>

Facultad de Ingeniería – UNLPam. Calle 110 N° 390. General Pico  
La Pampa – Argentina – Tel. 54-02302-422780

{balleste, filippij}@ing.unlpam.edu.ar

**Resumen:** Un alto porcentaje de estudiantes de primer año universitario evidencia dificultades con la complejidad y el volumen del contenido abordado. Además de atribuir una parte de estas dificultades a la falta de articulación entre los niveles medios y superiores de educación, consideramos que es fundamental buscar soluciones que contribuyan en la progresión y la mejora del rendimiento académico de los ingresantes. En este trabajo, utilizamos la tecnología H5P (h5p.org) para implementar animaciones que simulen el comportamiento de la arquitectura básica de un procesador, y así poder ofrecer a los estudiantes los beneficios de aprender a través de una simulación y la posibilidad de un aprendizaje autodirigido. El tema elegido como primera experiencia para generar animaciones interactivas fue la arquitectura de von Neumann, un tópico en el que muchos estudiantes evidencian dificultades. En nuestra experiencia percibimos que estas dificultades se deben a la forma en que la arquitectura de un procesador es generalmente presentada en la bibliografía, es decir, a través de texto plano con algunas imágenes estáticas representativas y a la utilización de prácticas de aula tradicionales más centradas en un aprendizaje pasivo. Fundamentado en principios y heurísticas para la aplicación exitosa de gráficos animados y principalmente en el aporte del aprendizaje autodirigido para una comprensión más profunda de los objetivos de aprendizaje, desarrollamos contenido interactivo utilizando H5P, el cual tuvo un alto nivel de satisfacción. Entre otros resultados, fue calificado entre 8 y 10 (escala 0-10) por el 80% de los estudiantes que lo utilizaron y el 100% recomendaría este contenido a un colega que quisiera aprender sobre el tema. Consideramos que los resultados de la experiencia ameritan su divulgación y postulamos que la creación de este tipo de contenido innovador facilita la comprensión de cualquier tema y contribuye al aprendizaje autodirigido.

**Palabras clave:** Animación, Aprendizaje autodirigido, Contenido interactivo, H5P, Herramienta didáctica, Rendimiento Académico, Simulación, Tics en Educación.

## 1 Introducción

Muchas universidades, principalmente luego de la pandemia, se han desplazado hacia entornos de aprendizaje combinados, con nuevas tecnologías que brindan la oportunidad de impulsar el aprendizaje centrado en el estudiante combinando métodos tradicionales de enseñanza en el aula con herramientas en línea. En las asignaturas introductorias a la informática y en asignaturas relacionadas con arquitectura de computadoras, generalmente se introduce la organización de computadoras a través de la arquitectura de von Neumann, ya que es crucial para un entendimiento inicial de cómo un procesador es capaz de ejecutar instrucciones. Existe variada bibliografía que describe las fases de búsqueda y ejecución dentro de este contexto, sin embargo, la mayoría evidencia limitaciones cuando deben presentar la funcionalidad de cada componente del procesador, su interacción con el resto, las distintas señales enviadas en la línea de tiempo y el propósito general perseguido detrás de un grupo de señales.

El entendimiento de las componentes conceptuales de un procesador, y de sus funciones e interacción para la búsqueda y ejecución de instrucciones, muestra una complejidad que generalmente dificulta su entendimiento a través de un texto plano con algunas imágenes descriptivas, tal es el modo en que es presentado en la bibliografía. Tampoco el pizarrón ni las presentaciones de las clases magistrales tradicionales han mostrado ser un medio suficiente para explicar y visualizar apropiadamente la función e interacción de las componentes.

Por tal motivo, en este trabajo se utilizó la técnica de simulación como enfoque alternativo para modelizar la

arquitectura básica de un procesador, de modo de facilitar la comprensión sobre su funcionamiento, y se la implementó a través de contenido interactivo en línea, lo que además de los beneficios de la simulación, contribuyó hacia un aprendizaje autodirigido. Se define a la simulación como el proceso de construir un modelo matemático o lógico de un sistema, y experimentar con el modelo para obtener conocimiento del mismo [1]. Las computadoras brindan la posibilidad de crear estrategias de aprendizaje innovadoras, con frecuencia se utilizan sistemas educativos multimedia y gráficos animados para enseñar sistemas complejos y conceptos abstractos. Se define como software educativo a aquellas herramientas de computación desarrolladas con el objetivo de ser utilizadas como facilitadoras del proceso de enseñanza [2].

El software educativo comparte ciertas características esenciales: tiene una finalidad didáctica, utiliza la computadora como soporte, es interactivo, permite el diálogo e intercambio de información, posibilita la personalización de la velocidad de los aprendizajes y es relativamente fácil de utilizar [3]. Entre las funciones que puede realizar el software educativo se incluyen: informativa, instructiva, evaluadora e indagadora.

Las computadoras poseen también la capacidad de integrar elementos de animación como herramientas de enseñanza-aprendizaje. Se define a la animación como una visualización gráfica que cambia su estructura u otra propiedad a lo largo del tiempo, y que dispara la percepción de un cambio continuo [4]. La técnica de animación tiene gran potencial para cumplir una función pedagógica en la enseñanza de conceptos complejos, particularmente aquellos que no son simples de describir verbalmente. Además, ayuda a crear imágenes mentales de sistemas que poseen elementos que cambian en el tiempo. Sirve también para mostrar cómo la manipulación de una variable afecta a otras o la existencia de influencias simultáneas en sistemas [5].

La tecnología H5P brinda la posibilidad de generar contenido interactivo, lo que le agrega a la animación, la posibilidad de que el aprendiz interactúe, la visualice paso a paso, avance o retroceda, realice autoevaluaciones no amenazantes (“si me equivoco no desapruebo”), maneje su ritmo de aprendizaje y tenga independencia para poder utilizarla en cualquier momento y ubicación geográfica.

Es factible y relevante la utilización de animaciones interactivas como herramientas para el abordaje de la enseñanza de la arquitectura de von Neumann, considerando también que la interactividad transforma a un receptor pasivo que sólo puede recibir información, en un receptor activo [6]. Nuestro propósito fue desarrollar una herramienta en línea que estuviera más enfocada en un aprendizaje activo, autodirigido, y que complementara las prácticas docentes tradicionales de aula.

Si bien hay varios trabajos que utilizan la simulación a través de animaciones como herramientas para desarrollos de software educativo en la enseñanza de la arquitectura de von Neumann, por variados motivos no elegimos utilizar su implementación en nuestro curso, entre otros: no son interactivas, están en inglés (aún la mayoría de nuestros estudiantes evidencia dificultades para entender cuestiones de cierta complejidad en otro idioma), requieren de conocimientos de lenguaje ensamblador, no pueden insertarse dentro el LMS Moodle de la universidad, o no abordan el tema con el enfoque o profundidad pretendida.

Algunas de las herramientas indagadas que concluimos que no eran adecuadas para utilizarlas en nuestro curso fueron:

- Von Neumann Machine (<http://vnsimulator.altervista.org/>)
- Johnny Simulator ([www.onworks.net/software/app-johnny-simulator](http://www.onworks.net/software/app-johnny-simulator))
- IASSim (<https://cs.colby.edu/djskrien/IASSim/>)
- Simple-As-Possible Computer (<http://aserrano.es/portafolio/informatica-con-processing/sap1/>)
- Little Man Computer (<https://peterhigginson.co.uk/lmc/>)

Con el propósito de contar con una herramienta en castellano, que no requiriera de conocimientos previos de lenguaje ensamblador, que fuera interactiva, que abordada el tema con la profundidad que pretendíamos, que pudiera utilizarse en línea dentro del Moodle de la universidad, nos enfocamos en diseñar animaciones interactivas para simular la arquitectura básica de un procesador, utilizando la tecnología H5P, a fin de mejorar el rendimiento académico de los estudiantes y contribuir al desarrollo de un aprendizaje autodirigido. En el entorno actual de la educación superior, los educadores no pueden permanecer estancados en la forma en que enseñan, y deben buscar y desarrollar estrategias innovadoras [7].

## 2 Animaciones interactivas para la enseñanza de von Neumann

Luego de obtener ideas de las distintas propuestas de simulación de arquitectura de procesadores indagadas, y fundamentando en teoría cognitiva del aprendizaje multimedia [8], teoría de la fidelidad epistémica [9], en principios para la aplicación exitosa de gráficos animados, principio de congruencia, principio de aprehensión [10], en heurísticas prácticas [11], y en la contribución en el proceso de enseñanza del aprendizaje autodirigido, se diseñaron animaciones interactivas en línea para simular las distintas componentes de la arquitectura básica de un procesador, y sus funciones e interacción durante las fases de búsqueda y ejecución de instrucciones, apoyándonos además en el hecho de que la presentación y organización de los

contenidos en la mayor cantidad de modos posibles facilita nuevos y genuinos significados [12][13].

### ¿Por qué H5P?

Muchas herramientas para la generación de contenido interactivo en línea tienden a ser técnicamente complejas, costosas y a menudo, no consideran un LMS, lo que significa que no se puede adquirir análisis sobre el progreso de los estudiantes. H5P brinda una solución innovadora en este espacio tecnológico y educativo, que puede utilizarse dentro de un LMS, y por ser gratuita y de código abierto, permite crear, compartir y reutilizar HTML5.

El creador de contenido no necesita experiencia técnica especial para crear contenido con H5P, a diferencia de aplicaciones alternativas como Articulate Storyline y Adobe Captivate, los tipos de contenido que se pueden implementar son fáciles de aprender y adoptar. El educador puede adquirir competencia en la creación de un tipo de contenido como "Arrastrar y soltar" o "Rellenar espacios en blanco", y luego pasar a otro tipo de contenido, pudiendo crear actividades fragmentadas o combinar fragmentos para desarrollar actividades de aprendizaje más complejas.

Los usuarios de H5P pueden crear más de 40 tipos diferentes de contenido interactivo. Utilizando combinaciones de estos tipos de contenido, se pueden mejorar diversos tipos de enseñanza, aprendizaje y evaluación, desarrollar la capacidad del docente y, en última instancia, conducir a un aprendizaje dentro y fuera del aula. Aprendimos fácilmente la creación, uso y desarrollo de objetos de aprendizaje H5P dentro del LMS de la universidad. Construir dentro del LMS nos alentó además a complementar el material didáctico compartiendo lecturas a través de PDFs.

El estudiante puede ver la actividad fragmentada (animación en nuestro caso) de H5P con un texto instructivo. Además, se puede agregar un vínculo "Pista", el cual puede actuar como un enlace a un libro de texto o a cualquier material de aprendizaje relevante para la actividad. La retroalimentación es el principal mecanismo que tiene el estudiante para determinar su progreso dentro de una tarea de aprendizaje [14]. El interactivo de aprendizaje H5P proporciona retroalimentación inmediata con las opciones "verificar" o "mostrar solución", que es muy importante para reforzar y guiar el aprendizaje. También hay investigaciones que sugieren que la retroalimentación clara y consistente puede aumentar la motivación de un estudiante hacia un tema determinado [15].

La introducción de las actividades H5P complementando las técnicas tradicionales, contribuye a un aprendizaje didáctico centrado en la experiencia interactiva y brinda un contenido que invita a la reflexión. El alumno interactúa con el contenido que tiene como objetivo guiarlo e involucrarlo

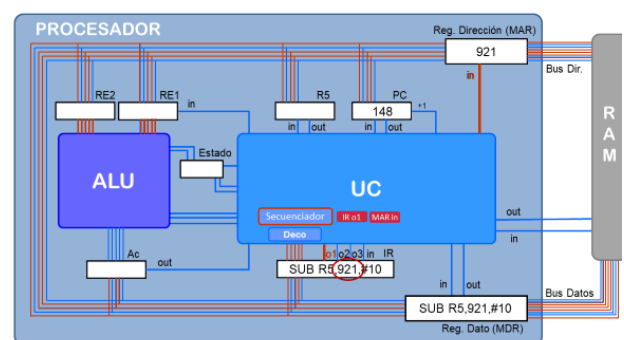
en la adquisición de conocimientos de una manera activa en lugar de pasiva [16], promoviendo habilidades de pensamiento de orden superior [17].

Además, los contenidos H5P se pueden etiquetar con metadatos como: Universidad de origen, disciplina, una descripción y palabras clave para permitir que otros docentes los localicen y los utilicen, o adopten el concepto y los manipulen para adaptarse a otro contexto. Consideramos que la posibilidad de compartir contenido H5P con colegas puede fomentar la formación de comunidades de práctica para la enseñanza y el aprendizaje mejorados con tecnología.

### 3 Diseño del contenido

Una vez elegida la tecnología para la implementación de las animaciones que simularan von Neumann, se seleccionó el conjunto de registros, circuitos, buses y señales que se representarían (Fig. 1). Se seleccionaron además las señales, operaciones, e instrucciones que se iban a simular, como así también la interacción autoevaluativa con el estudiante. La interacción diseñada contempla la posibilidad de predecir el contenido de los distintos componentes del procesador luego de ejecutarse una instrucción, una fase, o un conjunto de señales. De este modo las animaciones se podrían ejecutar paso a paso y en distintas instancias se podrían detener a fin de realizar evaluaciones no amenazantes.

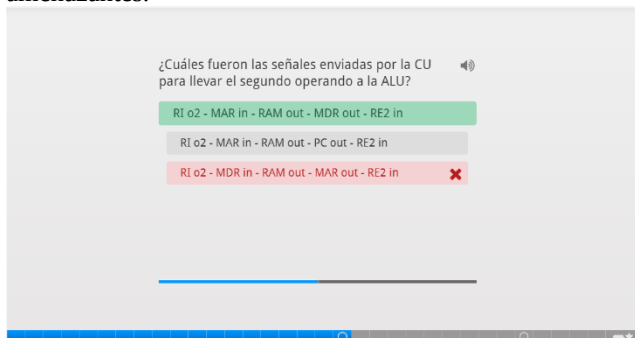
Se aprovechó también la posibilidad que brindaban los cambios de colores para generar impacto visual, fue así que se seleccionaron los colores y cambios para los distintos canales de comunicación, los componentes y las señales, de modo de resaltar cuando un bus, registro o señal eran activados. En una primera instancia se implementó la fase de búsqueda en su totalidad, y luego de observar la buena respuesta y retroalimentación por parte de los estudiantes, se diseñaron otras animaciones para representar las fases de ejecución de instrucciones clásicas.



**Fig. 1 Instantánea de la animación durante la ejecución de una instrucción**

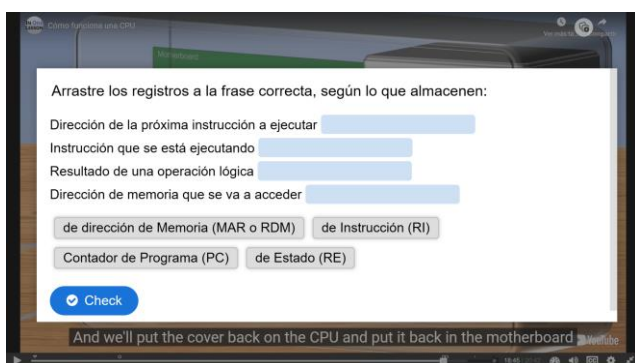
El contenido interactivo fue diseñado e implementado para estar disponible en línea, como así también para asistir en el aula. Cuando es presentado en el aula, el docente tiene la posibilidad de interactuar con los estudiantes pausando la

animación y realizando preguntas que ayuden a interpretar lo simulado, por ejemplo, prediciendo el contenido de registros, buses y RAM. Se diseñaron además un conjunto de interacciones y autoevaluaciones para cuando la herramienta es accedida en forma autónoma por el estudiante a través de la Web (Fig. 2 y 3). La interacción brinda la posibilidad de que los estudiantes manejen su ritmo de aprendizaje y puedan realizar evaluaciones no amenazantes.



**Fig. 2 Evaluación durante la reproducción de una presentación interactiva**

Las actividades de aprendizaje diseñadas, desafiaron a los estudiantes, los involucraron activamente y aumentaron la probabilidad de un aprendizaje autodirigido a través de una retroalimentación formativa e inmediata [18] (la opción "verificar" de H5P permite esto). La autoevaluación, vista como una evaluación no amenazante o de "poco en juego", en lugar de una tarea de evaluación sumativa de "mucho en juego" con criterios de desaprobación/aprobación [19], es crucial. Las formas de evaluación de bajo impacto, particularmente para los estudiantes de primer año, son fundamentales para obtener resultados exitosos [20], por lo tanto, fueron fundamentales para el diseño de las actividades.



**Fig. 3 Evaluación durante la reproducción de un video interactivo (arrastrar y soltar)**

## 4 Resultados y discusión

En la encuesta anónima realizada al finalizar el ciclo sobre un total de 30 estudiantes, reveló que el 100 % recomendaría la utilización de estas animaciones interactivas para el aprendizaje de la arquitectura de von Neumann. El 83% de

los encuestados utilizó las palabras entendible y útil para definir el contenido interactivo, y el 70% utilizó además la palabra "claro". Cabe señalar también que el 80% lo calificó entre 8 y 10 puntos sobre 10 y que, si bien sólo al 36 % le resultó fácil aprender el tema utilizando este contenido, la mayoría de los que no la consideraron ni fácil ni difícil, comentaron que no habían podido cumplir con la lectura previa propuesta para la utilización de las animaciones.

Además de los resultados ampliamente favorables de las encuestas realizadas, se apreció una mejora significativa en los resultados de las evaluaciones formales sobre la arquitectura de von Neumann. Se evidenció también un aumento en la media de aprobación sobre el tema de un 18% respecto a los últimos cinco años previos a su utilización. Hay que considerar también otros resultados favorables difíciles de medir como la interacción cotidiana con los estudiantes y el intercambio de preguntas y respuestas, en los que se evidenció una mejor comprensión y se percibieron estudiantes más activos y autodirigidos.

## 5 Conclusiones y trabajo futuro

En las asignaturas introductorias a la informática y en asignaturas relacionadas con organización de computadoras, generalmente se introduce el funcionamiento básico de un procesador a través de la arquitectura de von Neumann, ya que es crucial para un entendimiento inicial de cómo un procesador es capaz de ejecutar instrucciones. Hay variada bibliografía que describe las fases de búsqueda y ejecución, sin embargo, la mayoría evidencia limitaciones cuando deben explicar la funcionalidad de cada componente del procesador, su interacción con el resto, las distintas señales enviadas en una línea de tiempo y el propósito general que persiguen.

En nuestra experiencia docente percibimos que los estudiantes ingresantes evidenciaban mayoritariamente dificultades en el aprendizaje de este tema, y luego de indagar consideramos que probablemente, buena parte de las dificultades evidenciadas se debían a que no poseían una base de conocimiento como para abordar la lectura y el entendimiento en la forma en que generalmente es presentada en la bibliografía, es decir, a través de texto plano con algunas imágenes simbólicas representativas. Tampoco notábamos que el uso del pizarrón ni las presentaciones, a través de prácticas de aula tradicionales, fueran un medio suficiente para explicar y visualizar apropiadamente la función e interacción de los componentes, ni como para desarrollar y analizar la complejidad del conjunto de señales que son enviadas durante la ejecución de instrucciones.

Fue así que decidimos abordar una propuesta didáctica que, a través de un conjunto de animaciones, simulara la arquitectura de von Neumann durante las fases de búsqueda y ejecución de instrucciones, con el propósito de mejorar el rendimiento académico y contribuir en modo general a un



aprendizaje autodirigido. Las animaciones fueron implementadas a través de dos tipos de contenidos H5P: presentaciones y videos interactivos. Las presentaciones incluyen una interacción paso a paso con el usuario, con posibilidad de avanzar y retroceder, y con interrupciones en las que se realizan evaluaciones no amenazantes, entre las cuales se destaca la posibilidad de que el estudiante pueda predecir los valores de los registros del procesador luego de una o varias señales o luego de ciertas operaciones típicas. Los videos proveen interacción en puntos clave para que el usuario realice autoevaluaciones.

El contenido interactivo desarrollado tuvo un alto nivel de satisfacción, entre otros resultados fue calificado entre 8 y 10 (escala 0-10) por el 80% de los estudiantes que la utilizaron, y el 100% recomendaría la herramienta a un colega que desee aprender sobre el tema. Cabe acotar que se evidenció un mejor rendimiento académico en las evaluaciones formales realizadas a posteriori sobre el tema.

Si bien no pueden hacerse conclusiones definitivas, ya que cada ciclo involucra a distintos grupos de estudiantes, el contenido interactivo presentado ha logrado facilitar la comprensión de los conceptos y las relaciones envueltas en el funcionamiento básico de un procesador, lo que se ha evidenciado en las calificaciones obtenidas, la satisfacción de los estudiantes, y en modo más general, percibimos que ha contribuido hacia un aprendizaje autodirigido.

En cuanto a cuestiones pendientes y trabajo futuro, además de atender los resultados de nuestra autoevaluación, serán consideradas las mejoras propuestas por los estudiantes en la encuesta realizada, entre las que se destacan: definir al principio las siglas utilizadas, mejorar el diseño gráfico y agregar más interacción. También se prevé permitir que el usuario pueda seleccionar una instrucción, a partir de un conjunto propuesto, para simular su ejecución. Finalmente, dadas las evidencias de haber fortalecido el aprendizaje autodirigido y la producción de aprendices independientes, se prevé la utilización de H5P para diseñar contenido interactivo sobre otros temas de la asignatura.

## Referencias

- [1] Evans, J.R.; Olson, D.L.: Introduction to simulation and risk analysis. New Jersey: P. Hall. (1998).
- [2] Cataldi, Z.: Metodología de diseño, desarrollo y evaluación de software educativo. Tesis de Magister en Informática, Facultad de Informática, UNLP. (2000). <http://laboratorios.fi.uba.ar/lsi/>
- [3] Marqués, P.: El software educativo. (1996). <http://www.lmi.ub.es/te/any96/>.
- [4] Schnotz, W.; Lowe, R.K.: A unified view of learning from animated and static graphics. New York: Cambridge University Press, 304 a356. (2008).
- [5] Rieber, L.P.; Kini, A.: Theoretical foundations of instructional applications of computer-generated animated visuals. Journal of Computer Based Instruction, 18(3), 83 a 88. (1991).
- [6] Scolari, C.: Hipermediaciones. Elementos para una teoría de la comunicación digital interactiva. Barcelona. Gedisa. (2008).
- [7] Petty, J.: Interactive, technology-enhanced self-regulated learning tools in healthcare education: A literature review. Nurse Education Today, 33, 53–59. (2013).
- [8] Zoabi, W.; Sabag, N; Gero.: A. Using Animation to Improve the Student's Academic Achievement on Bipolar Junction Transistor. American Journal of Engineering Education – Fall 2012, 3, 2. (2012).
- [9] O'Donnell, F.: Simulation frameworks for the teaching and learning of distributed algorithms. Ph.D. Thesis, University of Dublin College. (2006). <http://www.tara.tcd.ie/bitstream/handle/2262/1277/TCD-CS-2006>
- [10] Tversky, B.; Morrison, J.B.; Betrancourt, M.: Animation: can it facilitate?. Int. J. Human Computer Studies, 57, 247 a 262. (2002).
- [11] Weiss, R.E.; Knowlton, D.S.; Morrison, G.R.: Principles for using animation in computer-based instruction: theoretical heuristics for effective design. Computers in Human Behavior, 18, 465 a 477. (2002).
- [12] Schneider, Débora; Imperatore, Adriana; Gergich, Marina: Hipermodalidad y estrategias didácticas virtuales: reflexiones conceptuales en torno al hipermedia como material didáctico. Apertura. (2011). <http://www.redalyc.org/html/688/68822701009/>
- [13] Lemke, Jay: Travels in hypermodality, SAGE Publications, vol1, núm.3. (2002)
- [14] Lucas, B.; Spencer, E.; Claxton, G.: Learning and teaching methods that work. How to teach vocational education: a theory of vocational pedagogy. London: City and Guilds Centre for Skill Development in conjunction with the Centre for Real-World learning at the University of Winchester. (2012).
- [15] Hoskins, S. L.: The development of undergraduate's approaches to studying and essay writing in higher education, PhD Thesis, University of Plymouth. (1999)
- [16] Anderson, T.; Elloumi, M.: Theory and Practice of Online Learning. Canada: Athabasca University. (2004).
- [17] Bloom, B. S.: Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain. New York: David McKay Co Inc. (1956).
- [18] Nicol, D.J.; Macfarlane D.: Formative assessment and self-regulated learning: a model and seven principles of good feedback practice. Studies in Higher Education, 31 (2). (2006).
- [19] JISC: Effective practice with e-assessment – An overview of technologies, policies and Practice in Further and Higher Education. HEFCE. (2007).

<http://www.jisc.ac.uk/media/documents/themes/elearning/effpraceassess.pdf>.

[20] Nelson, K.; Creagh, T.; Kift, S.; Clarke, J.: Transition Pedagogy Handbook. A Good Practice Guide for Policy and Practice in the First Year Experience at QUT. 2nd Edition. (2014).

