

**El fomento de la cultura de paz en los entornos digitales.**

**The promotion of a culture of peace in digital environments.**

Saúl Adolfo Lamas Meza\*.

Recibido: 21/06/24 • Aceptado: 23/08/24

---

\*Doctor en Derecho por la Universidad Autónoma de Nayarit. Docente de tiempo completo adscrito a la Universidad de Guadalajara. Miembro del Sistema Nacional de Investigadores del CONAHCYT. SNII, nivel I. Identificador Orcid: <https://orcid.org/0000-0002-4680-9513>

**Resumen:** El presente artículo tiene como finalidad analizar a través de una metodología exegética y correlacional el fenómeno de la violencia sistémica que en la actualidad se suscita en los entornos virtuales. Se da cuenta de algunos de los instrumentos internacionales que intentan regular y atenuar estas conductas que cada vez encuentran nuevas formas de manifestación. En el cuerpo del documento se describen algunos programas de inteligencia artificial creados *ex profeso* y que se han venido empleando en los últimos años para favorecer procesos de avenencia y resolución de conflictos a través de esquemas automatizados. Al final del documento se presenta una propuesta de lo que podría ser un código de ética integral para incentivar la cultura de paz en la utilización de las disruptivas tecnologías de la información y la comunicación.

**Palabras clave:** Cultura de paz, tecnologías de la información, deontología jurídica, entornos digitales, justicia alternativa.

**Abstract:** The purpose of this article is to analyze, through an exegetical and correlational methodology, the phenomenon of systemic violence that currently arises in virtual environments. It is aware of some of the international instruments that attempt to regulate and mitigate these behaviors that increasingly find new forms of manifestation. The body of the document describes some artificial intelligence programs created "ex profess" that have been used in recent years to promote compromise processes and conflict resolution through algorithms or automated schemes. At the end of the document, a proposal is presented for what could be a comprehensive code of ethics to encourage a culture of peace in the use of disruptive information and communication technologies.

**Key-words:** Culture of peace, information technologies, legal ethics, digital environments, alternative justice.

**Índice:** I.- Preámbulo. II.- La regulación de la violencia digital en los instrumentos internacionales. III. El uso de las tecnologías como herramienta para la resolución de conflictos. IV. Proyectos de justicia alternativa *on-line* desarrollados por algunas Universidades y Centros de investigación. V. Programas exitosos de robótica burocrática y mediación extra-judicial. VI. La construcción de la cultura de paz en los entornos digitales.

Propuesta de un código deontológico en la utilización de las TIC(s). VII. Principios deontológicos en la utilización de tecnologías de innovación en la era digital.

## 1.- Preámbulo.

La violencia en cualquiera de sus manifestaciones es reprobable, y sin importar las razones que den origen a esta, es y será siempre una práctica socialmente inadmisibles. Fenómeno —que huelga decir— va *in crescendo*, por lo que es menester que las políticas públicas estatales se concentren en impedir que se normalice en el entramado social y se acentúe en la psique colectiva.

La palabra violencia proviene de la nomenclatura latina *violentia* que se integra de los vocablos *vis* fuerza y *olentus* exceso, es decir, actuar con exceso de fuerza o con fuerza desproporcionada.<sup>1</sup> La Organización Mundial de la Salud la ha definido como "el uso de la fuerza física o el poder, ya sea en grado de amenaza o efectiva, contra uno mismo, otra persona o un grupo o comunidad, que cause o tenga muchas posibilidades de causar lesiones, muerte, daños psicológicos, trastornos del desarrollo o privaciones"<sup>2</sup>. El vocablo "violencia" *lato sensu*, es descrito por Blair Trujillo como "el uso de una fuerza abierta o escondida, con el fin de obtener de un individuo o un grupo, eso que ellos no quieren consentir libremente"<sup>3</sup>.

Y aunque la violencia suele asociarse a menudo con actos de hostilidad física, este un fenómeno que puede adoptar matices de amplio espectro, así entonces podemos hablar de violencia verbal, emocional, moral, cultural, social o la que Galtung<sup>4</sup> ha denominado estructural, siendo aquella que es incentivada por el Estado y su aparato de

---

<sup>1</sup> Roberto Manero Brito, *Consideraciones teóricas sobre el estudio de la violencia*, (México: Enseñanza e Investigación en psicología, 2017), 389.

<sup>2</sup> Organización Mundial de la Salud, OMS, *Informe mundial sobre la violencia y la salud*, (Washington, E.U.A., 2003), 5.

<sup>3</sup> Elsa Trujillo, "Aproximación teórica al concepto de violencia: avatares de una definición", *Política y Cultura* 32, (2009): 20.

<sup>4</sup> Johan Galtung, *Tras la violencia, 3R: reconstrucción, reconciliación, resolución. Afrontando los efectos visibles de la guerra y la violencia*, (España: Bakeaz, 1988), 166.

gobierno quien a través de actos deliberados o subrepticios anula la posibilidad de que ciertas personas o grupos de personas puedan desplegar sus potenciales o desarrollar óptimamente sus posibilidades de expansión.

También existen otros tipo de violencias que son más sutiles, pero no por ello menos dañinas, como son la violencia simbólica, aquella que Bourdieu<sup>5</sup> ha abordado prolijamente en sus estudios sobre el patriarcado doméstico y que consiste precisamente en aquél tipo de violencia consuetudinaria en el cual el varón asume un rol de superioridad implícita y explícita sobre el género opuesto, sobre el cual ejerce una dominación tácita que deriva en vínculos asimétricos a través de un esquema de control-subordinación.

En el presente estudio, analizaremos una forma de violencia *sui generis* que a falta de una denominación homologada, a *grosso modo* se le ha denominado “virtual”, la cual apareció con la emersión y desarrollo acelerado de nuevas tecnologías, y que se han tornado para el perpetrador de estas conductas, en vehículos de materialización de toda suerte de prácticas hostiles y criminógenas.

En la última década, con la inmersión disruptiva de las tecnologías de la información y la comunicación en la vida de las personas, muchas conductas antisociales han sido trasladadas a los entornos digitales. La violencia, es un claro ejemplo de ello. La realidad *off-line* (incluyendo la criminal) se ha extrapolado a lo *on-line*, con facilidad. Empero, el problema no está en el instrumento tecnológico *per se*, sino en el sujeto mismo, pues una vez que el agente activo ya ha deliberado en su mente cometer un delito, buscará materializarlo, utilizando cualquier medio (físico o virtual) para su consumación.

Toda sociedad civilizada promueve la idea de que cualquier manifestación de violencia (moral, física, verbal, implícita o digital), es un fenómeno indeseable que debe ser proscrito de la realidad social. Ninguna persona debe ser víctima de actos de molestia o acoso, ni de manera física ni virtual. Sobre este particular, copiosos instrumentos

---

<sup>5</sup> Pierre Bourdieu, *La dominación masculina*, (Barcelona: Anagrama, 2003), 76.

internacionales se han pronunciado, reprobado la violencia en cualquiera de sus manifestaciones. A continuación, daremos cuenta de los más importantes.

## **2.- La regulación de la violencia digital en los instrumentos internacionales.**

La comunidad internacional, consciente de que los entornos digitales se han tornado en ecosistemas inculcadores de conductas violentas e incluso criminógenas, intentan regular esta realidad que cada vez es más compleja debido a que las tecnologías son cada vez más sofisticadas, lo que permite que los usuarios puedan hacer uso de ellas, incluso desde el anonimato para desplegar conductas inmorales y delictivas. Algunos tratados e instrumentos —de forma general algunos y particular otros—, condenan las prácticas de violencia expresa, implícita, exógena o virtual en cualquiera de su gama de manifestaciones de amplio espectro:

### 2.1.- “Protocolo de la ONU para combatir la violencia en línea contra las mujeres y las niñas” (Fragmento):

*“Tanto los gobiernos y los organismos reguladores, como las empresas y los ciudadanos comunes de Internet tienen que reconocer y actuar sobre la base del principio de que una Internet insegura significa que las mujeres utilizan Internet con menos libertad, y que ello conllevará costosas implicaciones sociales y económicas”.*

*“La práctica óptima debe basarse en las 3 ‘S’: Sensibilización, Salvaguardias y Sanciones.*

- *Medidas de prevención a través de la sensibilización del público. Cambiar las actitudes y normas sociales es el primer paso para cambiar la manera en que se percibe el abuso en línea y la seriedad con la que se trata. Se requiere educación pública y formación del personal de las fuerzas del orden, por ejemplo la policía.*

- *La promoción de salvaguardias para la seguridad e igualdad de las mujeres y las niñas en línea en Internet. Los marcos de seguridad para hacer frente a la violencia tradicional contra la mujer incluyen refugios para mujeres, centros de crisis, líneas de ayuda y educación: el mundo digital también requiere medidas de seguridad para adaptarse a una Internet que evoluciona con rapidez. Ello requerirá necesariamente recursos, y la atención y participación activa de los vigilantes digitales de la industria, la sociedad civil y los gobiernos.*

- *La creación de sanciones y su aplicación a través de los tribunales y los sistemas legales, a fin de definir y ejecutar las consecuencias punitivas para quienes incumplen la normativa.*
- *Cada uno de estos pilares de sensibilización, salvaguardias y sanciones sirve de apoyo a los demás, y requerirá una acción coherente y de colaboración en muchos niveles<sup>6</sup>’.*

## 2.2.- Convención Americana sobre Derechos Humanos:

*‘‘Artículo 11. Protección de la Honra y de la Dignidad.*

*I. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*

*II. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.*

*III. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques<sup>7</sup>’.*

## 2.3.- La Convención de los Derechos del Niño:

*‘‘Artículo 16.*

*I. Ningún niño/será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación.*

*II. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques<sup>8</sup>’.*

## 2.4.- Constitución Política de los Estados Unidos Mexicanos:

*‘‘Artículo 7o. Es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. No se puede restringir este derecho por vías o medios indirectos, tales como el abuso de controles oficiales o particulares, de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios y tecnologías de la información y comunicación encaminados a impedir la transmisión y circulación de ideas y opiniones<sup>9</sup>’.*

---

<sup>6</sup> Organización de las Naciones Unidas. ‘‘Protocolo de la ONU para combatir la violencia en línea contra las mujeres y las niñas’’, 2018, <https://en.unesco.org/sites/default/files/highlightdocumentspanish.pdf> (Consultado: 15/02/2024).

<sup>7</sup> Convención Americana sobre Derechos Humanos. (Costa Rica, OEA, 1978). Art. 11.

<sup>8</sup> Convención de los Derechos del Niño. (Suiza, UNICEF, 1989). Art. 16.

<sup>9</sup> *Ibidem*. Art. 7°. Artículo reformado DOF 11-06-2013.

*“Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento<sup>10</sup>”.*

## 2.5.- Ley General de Acceso de las Mujeres a una Vida Libre de Violencia:

*“Capítulo IV Ter. De la violencia digital y mediática.*

*Artículo 20 Quáter.- Violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia. Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación<sup>11</sup>”.*

En México, el fenómeno de la violencia digital se ha exponenciado dramáticamente en los últimos años. El INEGI en su informe anual, a través de su *Encuesta Nacional sobre disponibilidad y uso de Tecnologías de la Información en los Hogares* efectuada en el año 2022 documentó que de los 88.6 millones de usuarios de internet en México (mayores de 6 años), el 21%, dijo haber experimentado algún tipo de ciberacoso, es decir, más de 18 millones de mexicanos. En México existe una raigambre bélica histórica, siendo la violencia en este territorio, un fenómeno antiquísimo generalizado. Situación que se ha intensificado en las últimas décadas, tomando nuevos matices de manifestación, ya que este fenómeno de violencia se ha extrapolado a los entornos digitales.

Huelga referir que los tratados y convenciones internacionales adolecen de fuerza vinculante, lo que limita su aplicación jurídica e incluso fáctica, pues si bien es cierto que los países signatarios se comprometen a cumplir cabalmente sus disposiciones, la realidad es que no pueden ser coaccionados a que las apliquen taxativamente, pues la naturaleza de los instrumentos internacionales es tornarse en parámetros orientadores, más no en

---

<sup>10</sup> *Ibidem*. Art. 16°. Párrafo reformado DOF 15-09-2017.

<sup>11</sup> Ley General de Acceso de las Mujeres a una Vida Libre de Violencia. (México, Congreso de la Unión, 2021) Apartado IV.

imperativos categóricos, so pena de vulnerar la soberanía y libre autodeterminación de los estados miembros. Es por ello que este tipo de disposiciones normativas internacionales han sido denominadas por la doctrina como de *soft law* (de derecho blando), justamente porque no tienen la rigidez y coactividad que *a priori* sí tienen las leyes de cualquier Estado-nación en particular.

Empero, la preocupación que la comunidad internacional de forma genuina ha mostrado para combatir la violencia digital en cualquiera de sus multiformas de manifestación, es real, tan es así que en las últimas cumbres internacionales el abordaje de este tópico se ha debatido con denuedo, precisamente por el aumento alarmante del fenómeno de la ciberdelincuencia en el escenario internacional, el cual se ha exponenciado significativamente en las últimas dos décadas, lo que ha llevado a la promulgación de instrumentos diseñados *ex profeso* para hacer frente a esta problemática, entre los que destacan el "Convenio de Budapest", el "Tratado de la OMPI sobre el internet", la "Declaración del Milenio", el "Convenio del Consejo de Europa para la protección de las personas con respecto al Tratamiento Automatizado de Datos de carácter Personal" (Convención de Estrasburgo), la "Declaración de Principios derivados de la Cumbre Mundial sobre la Sociedad de la Información", entre otros más.

La comunidad internacional está haciendo este esfuerzo mancomunado para contrarrestar el fenómeno de la ciberdelincuencia, pero los Estados en su fuero interno son quienes deben de asumir la responsabilidad de implementar políticas públicas, principalmente profilácticas a efecto de atenuar esta problemática que se expande sin parangón.

El Estado como respuesta a ello, ha creado al Derecho en abstracto para regular los comportamientos humanos en aras de lograr la armonía social y al Derecho Penal en concreto, para hacer frente a las conductas antisociales; siendo entre ellas, "la violencia", la principal. Así entonces los gobiernos al firmar y ratificar los tratados internacionales que versan sobre ciberdelincuencia, deben extrapolar los principios de tales instrumentos internacionales y darles contención y aplicación pragmática, robusteciendo sus propios



cuerpos normativos internos y diseñando políticas públicas de corte preventivo, a través de la creación de fiscalías creadas *ex profeso* para investigar eventos delictivos relacionados al uso de las tecnologías, principalmente capacitando a sus agentes de policía de tal tenor que se erijan en una policía cibernética especializada en el manejo de los protocolos de actuación para la investigación y persecución de estos delitos complejos.

A la par se deben diseñar programas de detección, monitoreo y persecución de ciberconductas potencialmente criminógenas en los entornos virtuales, para ello es menester que cuenten con tecnología de alta gama que les permita orgánicamente cumplir con esta labor de suprema importancia. Para materializar esta laborar, el trabajo de supra-coordinación entre los tres órdenes de gobierno: federal, estatal y municipal es fundamental para optimizar los procesos de logística y actuación.

Sin embargo, la política pública profiláctica de mayor relevancia es la concientización ciudadana, a través de campañas de reeducación en el manejo de las herramientas digitales, en las que se sensibilice a los usuarios de los riesgos latentes que el manejo de estas tecnologías emergentes puede traer de suyo. Sabedores de que el ciberespacio es un universo tan vasto que es casi imposible de contener, la labor de concientización sobre el manejo responsable, ético y legal de estas herramientas, es una tarea que los gobiernos no deben obviar, sino antes bien, deben invertir los recursos necesarios para que la educación digital permee en la conciencia colectiva, a efecto de impulsar una prístina cultura de paz.

### **3. El uso de las tecnologías como herramienta para la resolución de conflictos.**

La transición en la metodología de impartición de justicia en las sedes judiciales se está dando de forma acelerada. Proceso que fue catalizado por la pandemia SARS-COV-19, la cual empujó a la sociedad (incluso contra su voluntad) hacia la inmersión de la realidad virtual. El confinamiento generalizado y obligado que se vivió por meses en el

contexto epidemiológico, trajo consigo un rezago significativo en el desahogo de las audiencias procesales. Lo que llevo a que los poderes judiciales (ante tal situación de apremio) tuvieran que diseñar estratagemas eficientes para hacer frente a esta problemática. El resultado de ello, fue la incorporación exponencial de las Tecnologías de la Información y la Comunicación (TIC) en los modelos de impartición de justicia, con la intención de optimizar sus esquemas judiciales, que les permitiera desarrollar innovación tecnológica que redundara en eficiencia, transparencia y confiabilidad.

Al día de hoy, puede constatarse que algunas instituciones judiciales han hecho ya una transición significativa de sus anteriores esquemas tradicionales (farragosos y presenciales), hacia modelos más modernos de naturaleza virtual. Empero, este proceso que se aceleró en los últimos tres años, no es reciente, ya desde los años 90's cuando el internet empezó su auge expansivo en Norteamérica, ya se comenzaba a hablar de esquemas de justicia —prioritariamente alternativa— a través de la implementación incipiente de metodologías *on line*, de las que daremos cuenta a continuación:

#### **4. Proyectos de justicia alternativa *on-line* desarrollados por algunas Universidades y Centros de Investigación.**

A continuación referiremos cuatro ejemplos de proyectos piloto de justicia digital que algunas universidades han desarrollado en materia de mediación virtual, en sus albores:

4.1.- ‘‘*Virtual Magistrate Project*’’. Programa que tuvo su inicio en el año 1995 en Washington, derivado de la reunión entre representantes del "Centro Nacional de Búsqueda de Información Automatizada" y el "Instituto Jurídico del Ciberespacio", del cual surgió un proyecto piloto de arbitraje virtual<sup>12</sup>, que consistió en diseñar un sistema que permitiera a los involucrados en un conflicto, presentar por escrito su controversia, con la intención de que el programa, de acuerdo a la base de datos que contenía su software, emitiera un diagnóstico neutral. El sistema concertaba encuentros telefónicos entre los intervinientes y mediaba el diálogo entre ellos, particularmente a través de *e-mail*. Este programa

---

<sup>12</sup> Robert Gellman, *The National Center for Automated Information Research*, (Washington: ILC, 1996), 78.

eventualmente sugería acuerdos potenciales, con cuotas justas para los intervinientes, proponía formatos para la elaboración de convenios, sistematizaba las ofertas y contraofertas de los intervinientes, recibía documentos para su validación y desde su motor de búsqueda evocaba leyes aplicadas al caso, citaba antecedentes de casos similares que se resolvieron en el pasado y concertaba citas progresivas hasta que las personas lograran alcanzar un acuerdo o dimitieran definitivamente del proceso.

4.2.- ‘‘*On line Ombuds Office*’’. Proyecto desarrollado en 1996 por el Departamento de Estudios Legales de la Universidad de Massachusetts, el cual tuvo como encomienda migrar los servicios del *ombudsman* presencial, hacia un esquema de naturaleza virtual, principalmente para resolver disputas relacionadas a violaciones de derechos humanos, derivadas de la utilización de la web<sup>13</sup>. Esta oficina virtual tenía como propósito, brindar información al usuario, para una vez analizada su causa, ofrecerle perspectivas de solución. La plataforma contaba con una gran base de datos, especialmente de precedentes judiciales, seleccionando aquéllos que más similitud tuvieran con las problemáticas de los usuarios, y que fueran orientadores para la celebración de sus propios acuerdos.

Cuando el justiciable introducía su queja al sistema, a los pocos días recibía vía electrónica, asesoría, delineación jurídica de su problemática, suministro de información y un elenco de perspectivas de solución focalizadas a su caso concreto.

4.3.- ‘‘*On line mediation project*’’. Proyecto digital de Justicia Alternativa, desarrollado por el Centro Jurídico de Práctica Tecnológica de la Universidad de Derecho de Maryland, que consistía en brindar a las partes en disputa, un espacio virtual seguro y expedito en el que pudieran resolver su desavenencia. Este servidor virtual se creó específicamente para mediar dos tipos de conflictos: disputas domésticas tales como custodias, regímenes de visitas, apoyo infantil (excepto problemáticas de violencia intrafamiliar), y disputas mercantiles suscitadas entre usuarios y empresas de seguros médicos. El sistema una vez recibida la solicitud, contactaba a la contraparte vía *e-mail*, a efecto de recibir su percepción y pliego argumentativo, para a los pocos días concertar un encuentro telefónico de

---

<sup>13</sup> Ethan Katsh, *The Online Ombuds Office: Adapting Dispute Resolution to Cyberspace*, (Massachusetts: University of, Department of Legal Studies, 1995), 97.

avenencia entre los intervinientes. Toda comunicación era vía remota y hasta que se llegaba a un pre-convenio se citaba a las partes para que firmaran y formalizaran el acuerdo de manera presencial.

El programa les facilitaba en todo momento material bibliográfico y asesoría telefónica especializada, a efecto de optimizar los ejercicios de pre-mediación.

4.4.- '*Cybertribunal project*'. Proyecto desarrollado por la Universidad de Montreal en 1996, que inició como programa virtual piloto de Mecanismos de Resolución de Controversias. Este sistema fue desarrollado para mediar disputas principalmente sobre quejas de consumidores. El software estaba diseñado para hacer análisis de mercado que facilitaran el arbitraje entre las partes en disputa. Este proyecto derivó en la creación del *Cyberjustice Laboratory*, considerada una de las plataformas judiciales virtuales más avanzadas de inteligencia artificial y pionera en la implementación de expedientes electrónicos, programas de asesoría telemática, audiencias virtuales y robots judiciales<sup>14</sup>.

## **5. Programas exitosos de robótica burocrática y mediación extra-judicial.**

En el mundo se han diseñado diferentes mecanismos de inteligencia artificial, con la finalidad de facilitar trámites y procesos de naturaleza administrativa, civil y de justicia alternativa con resultados halagüeños, lo que permite pronosticar, que en un futuro a mediano plazo, múltiples trámites burocráticos se desarrollarán de forma automatizada. He aquí algunos ejemplos de estos programas:

5.1.- '*Free resolver*'. Programa *on line* gratuito desarrollado en Inglaterra, el cual permite gestionar un mecanismo de avenencia entre clientes inconformes y las empresas de servicios demandadas, a efecto de resolver la disputa de forma extrajudicial y autocompositiva. Toda queja presentada en este servidor, es capturada en el sistema y es derivada a la empresa que está recibiendo la queja. El programa está diseñado para brindar

---

<sup>14</sup> Khaterine, Lynch, *The forces of economy Globaliation*, (London: Kluwer Law International, 2003), 374.

retroalimentación instantánea a los usuarios, a quienes se les garantiza que sus datos serán protegidos.

El sistema crea una carpeta digital personalizada para el usuario, a efecto de que pueda adjuntar evidencias, hacer propuestas y contrapropuestas a la contraparte; además de que puede descargar el expediente en su propio ordenador, con la intención de documentar el proceso y darle seguimiento. La plataforma para transparentar sus servicios, publica semestralmente información estadística: número de quejas, acuerdos alcanzados, convenios en trámite, etc.

5.2.- *“Do not pay”*. (*Robot Lawyer*). Aplicación creada en el año 2015 para brindar servicios digitales legales en Inglaterra y Estados Unidos, de forma remota y a costos simbólicos (3 dólares mensuales). La *app* permite a los usuarios, entre otros servicios, impugnar multas de tránsito, solicitar reembolsos por compras de boletos de avión, hacer reservaciones, tramitar visas, además de brindar asesoría a través de *bots* para llenar formularios, etc.

Este programa fue considerado como el primer abogado robot del mundo.

En el año 2020 fue galardonado por la ABA (*American Bar Association*) con el *"Premio Louis Brown de Acceso Legal 2020"*.

5.3.- *“Hello Divorce”*. Plataforma *on line* diseñada en California, Estados Unidos, para brindar a la comunidad de usuarios, la gestión digital de su trámite de divorcio, de forma expedita y sin necesidad de recurrir a una Corte. El trámite al ser virtual, naturalmente economiza significativamente los costos. El sistema está diseñado para ofrecer a los usuarios asistencia remota legal y seguimiento de su trámite. La aplicación garantiza la protección irrestricta de los datos personales de sus clientes. En la actualidad esta plataforma opera en los Estados de California, Colorado, Texas y Utah.

5.4.- *“Robot Lawyer Lisa”*. Plataforma digital diseñada para gestionar convenios entre partes en disputa, ayudando a ambas a celebrar acuerdos de forma rápida y a bajos costos. El programa brinda a los usuarios asesoría legal vía remota y eventualmente asistencia jurídica presencial, siendo entonces una plataforma de modalidad híbrida. Su servicio

virtual está disponible las 24 horas del día, los 365 días del año, convirtiéndose en una tecnología de inteligencia artificial disruptiva en el mundo del derecho digital.

5.5.- ‘AskKarla’. Programa digital diseñado en Estados Unidos por la ‘Asociación de Servicios Legales de Montana’, con la finalidad de asesorar vía remota a sus usuarios, en temas prioritariamente civiles. Esta plataforma asesora a los usuarios con preguntas jurídicas básicas, a efecto de ayudarles a entender sus problemáticas legales. El nombre de este sistema, se pensó como homenaje a la jurista Karla Marie Gray, quien fue la primera mujer jueza en ser electa como miembro de la Suprema Corte de Justicia de Montana. Ella colabora directamente en este proyecto de asistencia jurídica virtual.

5.6.- ‘Ross Intelligence’. Proyecto de inteligencia artificial desarrollado en Canadá en el año 2016, diseñado como un potente buscador de jurisprudencias y archivos legales, especialmente en temáticas de naturaleza mercantil, a través de procesos automatizados que se desarrollan de manera casi instantánea. Este programa es la versión superadora del proyecto Watson de IBM, como sistema de búsqueda de información legal digitalizada<sup>15</sup>.

Para concluir este apartado, solamente referiremos que naturalmente con el paso de los años, los avances de la ciencia, la innovación tecnológica y la evolución de la inteligencia artificial, han permitido que tanto en juzgados, en centros de justicia alternativa y en múltiples dependencias gubernamentales, se estén incorporando *softwares* y *hardwares* cada vez más sofisticados, para desahogar trámites legales y burocráticos con mejor eficiencia y mayor celeridad.

## **6. La construcción de la cultura de paz en los entornos digitales. Propuesta de un código deontológico en la utilización de las TIC(s).**

La expansión acelerada que ha tenido la Tecnología en las últimas dos décadas, ha generado nuevas formas de interacción entre los individuos. Concebir en la actualidad una

---

<sup>15</sup> Los fundadores de la empresa ‘Ross Intelligence’, inteligencia artificial de búsqueda e investigación legal, finalizó sus operaciones el 31 de enero del 2020, luego de perder una demanda millonaria en Estados Unidos, debido a que algunas compañías la demandaron por sustracción de información.

comunicación sin dispositivos tecnológicos, resulta casi imposible. La revolución digital de las sociedades ha transformado radicalmente la forma de entender y vivir la realidad.

Los avances tecnológicos han traído de suyo, grandes beneficios a toda la humanidad y consecuentemente las expectativas que se tiene de la evolución tecnócrata para los próximos años, son incommensurables. Se espera de ella una suerte de panacea que resuelva muchas problemáticas sociales, económicas, políticas, académicas, médicas, ambientales, etc. La esperanza de que las nuevas tecnologías resuelvan conflictos que hoy azotan a la humanidad, nos permiten ilusionarnos sobre un mejor futuro: más óptimo, próspero y en todos los sentidos, con mejor calidad de vida.

Sin embargo, para que ello tome un derrotero positivo, es menester que mancomunadamente todos los gobiernos impulsen denodadamente entre las sociedades, valores éticos, cuyos principios axiológicos hagan verdaderamente eco, tanto en las instituciones como en los individuos, quienes son los reales operadores y usuarios de las tecnologías de la innovación.

La ética entendida como "la teoría o ciencia del comportamiento moral de los hombres en su sociedad<sup>16</sup>", implica una categoría de regulación estatal, que *a priori* debe conducir a la sociedad a encontrar equilibrio y desarrollo armónico. Siendo entonces, la ética, el parámetro rector de todo fenómeno social.

Luego entonces, desarrollar un código de ética global, secundado por la asunción genuina de responsabilidad por parte de todos los Estados, adoptando, impulsando y promoviendo sus principios entre sus sociedades, es condición indispensable para que tal parámetro axiológico tenga real incidencia y permeabilidad en la consciencia colectiva; siendo una encomienda de suprema importancia, que no puede posponerse más en esta era digital. Los esfuerzos aislados son insuficientes; requiriéndose entonces un compromiso integral por parte de todos los países, para que tome carácter general.

Naturalmente organismos de escala mundial como la Organización de las Naciones Unidas, la Organización de Estados Americanos y la Unión Europea son los indicados para promover un protocolo con principios deontológicos universales *ad hoc* a esta Era Digital. Implementación de políticas públicas para atenuar el problema de la violencia digital.

---

<sup>16</sup> Adolfo, Sánchez V., *Ética*, (Barcelona: Grijalbo, 2000), 16.

## **7. Principios deontológicos en la utilización de tecnologías de innovación en la era digital.**

A continuación presentamos una serie de principios axiológicos (parámetro deontológico mínimo), que deseablemente toda persona (física o moral) debería tener como referente axiológico, cuando activa o pasivamente esté en contacto con alguna herramienta digital:

*Principio deontológico uno. Toda tecnología (independientemente) de su naturaleza, debe estar libre de cualquier práctica predatoria de manipulación, control o enajenación mental.*

De acuerdo al estudio realizado en el 2021 por “Hootsuite” a través de su informe "Digital 2021 Global Report", los mexicanos pasan un promedio de 9 horas 1 minuto al día en internet, lo cual es un dato alarmante, pues ello representa que cada mexicano, invierte más de un tercio del día, observando un dispositivo u ordenador (independientemente que esto sea para desarrollar una actividad académica, de teletrabajo, o recreativa).

Estar frente a una pantalla, se ha tornado en el *modus vivendi* de millones de personas, lo cual está derivando en una especie de enajenación digital perniciosa, trayendo para los cibernautas problemas de diversa índole:

1. *Físicos:* principalmente patologías oculares, desarrolladas por la exposición a los espectros electromagnéticos que emiten las computadoras y dispositivos móviles.
2. *Mentales:* fatiga excesiva por desarrollar actividades monotemáticas durante periodos prolongados.
3. *Emocionales:* codependencia digital, desplazamiento de la realidad, autosegregación, *stress*, indolencia social, etc.

El abuso en la utilización del internet (principalmente por practicar juegos de realidad virtual o interactuar en las redes sociales) puede inocular a largo plazo una suerte de enajenación mental entre los usuarios.

El escritor francés Henri Lefebvre, en el año 1947, en su libro visionario "Crítica a la Vida cotidiana", escribió estas líneas, que parecieran adelantadas a su época:



*"Tenemos un continuo estado de enajenación, tras enajenación. Apenas una enajenación se libera, aparece otra más enajenante. Una nueva tecnología genera una dependencia del individuo a ella y apenas surge una nueva, esta se torna más enajenante que su predecesora<sup>17</sup>".*

La enajenación entendida como un desplazamiento de la conciencia hacia algo externo, inducida por algo o alguien, con la intención de obtener un beneficio; es una práctica inmoral. Todo creador de contenido virtual (videojuegos, ambientes inmersivos en el *metaverso*, redes sociales, etc.) debe ser responsable, evitando diseñar plataformas de dependencia programática nociva. *V.gr.:* juegos que no permiten el reseteo o desconexión de sus usuarios sin penalizaciones, o generando cobros recurrentemente a los usuarios para brindarles beneficios de *pro gamers*; tales recomendaciones también aplican para las plataformas virtuales que exigen que un *streamer* genere contenido por determinada cantidad de horas semanales, so pena de inhabilitar su canal, si incumple con esta cláusula.

Si bien es cierto, que estas prácticas son casi imposible de evitar o controlar, ya que son los usuarios quienes *motu proprio* deciden usarlas, también lo es que las empresas que desarrollan estos productos, deberían asumir códigos de ética profilácticos, a efecto de que las experiencias digitales que ofrecen en el mercado digital, sean menos inducidas, codependientes y enajenantes, especialmente para los niños, quienes son los más atraídos por esta industria.

La tecnología virtual debe ser un instrumento controlada por el humano y que no sea aquella quien controle a éste. La industria tecnológica de programas de realidad virtual, debe actuar con ética y probidad, desarrollando herramientas útiles que ayuden al individuo a encontrar su libertad, sin convertirlo un cautivo de ellas.

*Principio deontológico dos. Los gobiernos capitalistas deben evitar las brechas digitales, la segregación y la desigualdad en el acceso a los avances científicos y tecnológicos.*

Las tecnologías deben impulsar el progreso humano en todos los sentidos y su difusión debe ser universal e incluyente y ningún país del orbe debe quedar excluido de sus beneficios. La era digital debe traer consigo una promesa de progreso acelerado, para todos los pueblos. Para ello las grandes potencias deben asumir un talante de solidaridad internacional, coadyuvado con los países más menesterosos, a través de financiamientos

---

<sup>17</sup> Henri, Lefebvre, *Crítica a la vida cotidiana*, (París: Stock, 1979), 463.

asequibles o a través de liberación de patentes, a efecto de que estos últimos puedan hacerse de infraestructura e impulsar su crecimiento industrial.

La Organización de las Naciones Unidas (ONU), impulsando precisamente esta tarea de desarrollo global, en el año 2015 diseñó un proyecto al que denominó: "Agenda 2030, sobre el Desarrollo Sostenible", con la finalidad de que todos los países del mundo puedan emprender una ruta de crecimiento y expansión económica y social. En el documento se plasmaron 17 objetivos de transformación mundial. El objetivo 9° fue intitulado "Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación", en el cuál se planteó la encomienda de difundir los avances científicos y facilitar el acceso a las nuevas tecnologías en todas las naciones del mundo, a través de intercambio de información y el impulso de los sectores manufactureros tecnológicos, fomentando mercados justos.

La principal meta trazada en este instrumento fue prospectar que en el año 2030, exista cobertura de red móvil y acceso a la banda ancha en todos los rincones del mundo. En un mundo globalizado como el actual, la cooperación internacional, la fraternidad, la solidaridad y el servicio, deben ser los valores universales, que deben asumir todas las naciones, si pretenden alcanzar objetivos a escala global.

*Principio deontológico tres. Los experimentos con nanotecnología, robótica cuántica e inteligencia artificial, deben efectuarse con un enfoque antropocéntrico.*

Innovadoras tecnologías han emergido en las últimas décadas, sorprendiendo al mundo, debido a sus capacidades extraordinarias: sistemas informáticos que resuelven problemas matemáticos en segundos, programas que analizan y sistematizan grandes paquetes de información (*big data*) instantáneamente, etc. Los avances tecnológicos parecieran tener solo como límite la creatividad humana, y prueba de ello es la inteligencia artificial, que en la última década ha hecho progresos incólumes. Múltiples ciencias se han beneficiado de tales avances, particularmente la ciencia médica, que en la actualidad, valiéndose de dispositivos inteligentes, ahora puede practicar microcirugías no invasivas, hacer trasplantes con desfibriladores y órganos artificiales, construir prótesis mecánicas y una lista enorme de prácticas automatizadas que ya se desarrollan con naturalidad en miles de laboratorios y nosocomios equipados con tecnología de punta.

La era tecnocrática del siglo XXI en el tema de la biotecnología, ha hecho progresos espectaculares, empero, tales prácticas deben siempre ceñirse a sólidos códigos de ética, especialmente en temas hipersensibles, como son la clonación de animales, experimentación con energías nucleares radioactivas, temas de impacto medioambiental, etc.

Todas las ramas del conocimiento científico deben guiarse por principios axiológicos, pero muy particularmente las que desarrollen tecnologías potencialmente riesgosas. Y justo ante esta preocupación, la UNESCO en Noviembre del 2021 convocó a sus países signatarios, con la finalidad de debatir esta temáticas; de cuya convención surgió el documento intitulado "Recomendación sobre la ética de la inteligencia artificial", en el que se instó a todos los países industrializados que investigan, desarrollan, distribuyen o comercializan tecnologías de inteligencia artificial, a que practiquen los siguientes parámetros axiológicos:

- \*Proporcionalidad e inocuidad.
- \*Seguridad y protección.
- \*Equidad y no discriminación.
- \*Sustentabilidad.
- \*Protección de información sensible.
- \*Supervisión Humana.
- \*Transparencia.
- \*Responsabilidad y rendición de cuentas.
- \*Sensibilización y educación digital.
- \*Gobernanza y colaboración adaptativa.

*Principio deontológico cuatro. Los entornos digitales deben estar diseñados para fomentar aptitudes humanas y procesos formativos cívicos, educativos y culturales, buscando siempre la dignificación del ser humano.*

Todas las tecnologías deben tener como teleología, dotar al ser humano de mejores herramientas para mejorar su calidad de vida. Y a *contrario sensu* toda tecnología (independientemente de cual sea su naturaleza) que sea nociva, física, mental, emocional o moralmente para el individuo debe ser prohibida sin más.

La era digital debe regirse por los más elevados principios deontológicos, que respeten irrestrictamente la dignidad humana y garanticen el bienestar de las sociedades presentes y las sociedades del futuro. Apenas se advierta que alguna tecnología representa un riesgo potencial (real, inminente o futuro) para la salud o integridad del individuo o un peligro para el medio ambiente, deberá prohibirse categóricamente su uso, al menos que ulteriormente se presente un nuevo diseño que garantice la confiabilidad y seguridad en su utilización.

Las Cumbres Internacionales deberán erigir orgánicamente un Comité Técnico Multidisciplinario de Supervisión, Valoración, Aprobación y Validación de toda tecnología emergente, conformado por expertos de la comunidad científica y personas reconocidas internacionalmente por su probidad, reputación intachable y servicio a la humanidad, que estén legitimados para emitir un diagnóstico en el que valoren la viabilidad o no del uso de determinada tecnología. Siendo solo por consenso y unanimidad de tal Comité, que podrá aprobarse y autorizarse la socialización, distribución y comercialización de tecnología sensible.

Asimismo dicho Consejo Técnico internacional, podrá, cuando advierta que alguna tecnología sea denunciada como potencialmente peligrosa, hacer comparecer a sus dueños y diseñadores, a efecto de que rindan su informe y justifiquen su proyecto, el cual será sometido a dictamen para obtener o no su autorización.

*Principio deontológico cinco. Respeto a la intimidad de los usuarios. (Prohibición en la utilización ilícita de geolocalizadores, malwares de espionaje, interceptación de comunicaciones para obtener datos personales o información industrial protegida).*

Toda práctica invasiva a la privacidad de las personas (físicas o morales), independientemente de su medio de comisión, es socialmente reprochable. Pero cuando esta se da a través de un dispositivo electrónico para alcanzar este fin, la situación se agrava, en tanto el agente activo se vale de una herramienta que *a priori* debería ser positiva, pero que en este caso es utilizada de manera ilícita e inmoral, para facilitar su conducta.

Toda intervención de comunicaciones, instalación de programas de seguimiento, *ransomware* (secuestro de información), etc., son prácticas que por su gravedad, han sido

tipificadas como conductas delictivas tanto en instrumentos internacionales, como en múltiples códigos penales en legislaciones locales.

En México en el *Código Penal Federal*<sup>18</sup>, contempla diversos supuestos penales que tipifican estas prácticas ilícitas de amplio espectro. Asimismo desde el año 2010, México cuenta con una *Ley Federal de Protección de Datos Personales en Posesión de Particulares*, la cual conmina a toda entidad que tenga (por motivo de sus giros comerciales o actividades administrativas o comerciales) base de datos de sus usuarios, a que se conduzca siempre respetando los principios de licitud, consentimiento, información, secrecía, lealtad, proporcionalidad y responsabilidad institucional. La seguridad digital y el derecho a la privacidad, son prerrogativas que deben ser reguladas por el binomio axiológico-legal.

*Principio deontológico seis. Responsabilidad en la difusión de información en las redes sociales.*

El derecho a la expresión de la ideas es una prerrogativa constitucional y convencional indiscutible, sin embargo, esta garantía no es absoluta, puesto que tiene ciertos diques, estando condicionada a no dañar a terceros (difamación, daño moral, apología del delito, incitación a la cultura de odio, etc.), de ahí el aforismo célebre que reza "la libertad termina, donde inicia la libertad de los demás".

Uno de los grandes desafíos que ha traído la Era Digital, es la de regular y contener la difusión de noticias falsas (*fake news*) que circulan incontrolablemente en las redes sociales, con la finalidad de timar a las personas, inducir información para manipular a las masas, dañar la imagen de personas o instituciones, o al contrario, adularlas para sesgar la percepción que los cibernautas tienen sobre ellas.

El fenómeno de la desinformación malintencionada no es nuevo, históricamente se ha dado esta práctica inmoral, propiciada por medios de información (o mejor dicho de desinformación) conocidos como "tabloides amarillistas". Sin embargo, esta práctica se potenció radicalmente con la llegada del internet y la aparición de las redes sociales, las cuales facilitan que cada publicación pueda ser difundida por todo el mundo, en solo segundos.

---

<sup>18</sup> Código Penal Federal. (México: Congreso de la Unión, 2008), Tomo II.

Este fenómeno creciente ha representado un gran reto para las grandes plataformas virtuales, las cuales se han mostrado incapaces de regular tales prácticas, y aunque han implementado algoritmos para detectar contenidos inapropiados y censurarlos, la realidad es que es casi imposible que tales programas puedan validar la falsedad o veracidad de una publicación. Afortunadamente tales plataformas han ido incorporando progresivamente funciones que permiten que los usuarios puedan denunciar ciertos contenidos, de tal tenor que un algoritmo pueda analizarlos y decidir si deben ser suprimidos o no de su servidor, teniendo inclusive la opción de *banear* las cuentas que recurran en estas prácticas.

La OEA preocupada por este fenómeno creciente, en el año 2017, publicó la “Declaración conjunta sobre libertad de expresión y noticias falsas (*fake news*), desinformación y propaganda”, a efecto de contrarrestar los negativos impactos sociales, políticos, psicológicos, económicos, culturales, educativos, etc., que estas prácticas desleales pueden provocar en las sociedades digitales.

Actuar con probidad y responsabilidad en la difusión de información digital, es la categoría ética deseable, que debe asumir todo cibernauta que use una red virtual social.

Principio deontológico siete. *Respeto a la decisión autónoma de todo usuario de tener o no una identidad digital en los entornos virtuales.*

La web fue creada —entre otras cosas—, para servir como un entramado de conexión entre todos los países del mundo, facilitando la comunicación entre todas las personas del orbe, interconectados a través del ciberespacio.

Fue a partir de la última década cuando la proliferación de las redes sociales, tuvo su gran auge, ofreciendo a cualquier persona con acceso a internet, la posibilidad de abrir una cuenta personal, que le permitiera tener una personalidad virtual, con la que pudiera identificarse e interactuar. En la actualidad, millones de personas son usuarios de estas plataformas, asumiendo un avatar personal que les dota de realidad ontológica.

Sin embargo, las persona que *motu proprio* hayan decidido no utilizar estas plataformas, deben tener salvo su derecho tanto a la desconectividad, como su derecho ‘*a no existir virtualmente*’; prerrogativas que también deben ser reconocidas y tuteladas. Tales decisiones que vengan de la autonomía de la voluntad de un individuo, jamás podrán ser vulneradas. Cualquier persona física o jurídica (independientemente de su naturaleza) que coaccione a un individuo a "existir virtualmente", comete no solo un acto inmoral, sino

antijurídico, al transgredir los denominados Derechos ARCO (derechos a acceder, rectificar, cancelar u oponerse al tratamiento de datos personales).

*Principio deontológico ocho: Respeto irrestricto al reconocimiento de derechos de autoría de todo contenido que se suba y difunda en la web.*

Los derechos de autor son el conglomerado de prerrogativas jurídicas que poseen los titulares de alguna obra (independientemente de su naturaleza), al ser sus legítimos propietarios. Esta autoría de contenidos desde luego también se extrapola a los entornos virtuales, los cuales deben ser respetados *erga omnes*.

Todo autor de contenido, por más nimio que este sea, tiene la prerrogativa legal —o al menos moral— a su reconocimiento, incluso del contenido publicado en las redes sociales, (aunque es sabido que por derechos de adhesión, las plataformas absorben los derechos de todo lo que se publica en sus *muros digitales*).

El plagio simbólico se ha tornado en un fenómeno recurrente en las redes sociales, debido a que múltiples usuarios postean fotos e ideas de otros, sin darles crédito a sus autores; y aunque jurídicamente esta práctica no puede perseguirse (por la subsunción referida que hace la plataforma de todo contenido), al menos los usuarios que las ejecutan, debería evitar por un principio de ética digital. La consciencia de respeto, hacia la propiedad intelectual de otro, es un principio de consciencia digital que debe permear en todos los entornos virtuales.

## **8. Conclusiones finales.**

Socializar la cultura de paz es una encomienda que han emprendido los estados democráticos, especialmente en estos últimos años en los que se han vivido tiempos azarosos y revolucionarios. Los gobiernos tomando consciencia de la problemática que representa la violencia estructural que permea de manera inverosímil en la dinámica social, están poniendo sus mejores afanes en diseñar políticas públicas frontales que hagan frente a este fenómeno creciente.

El vocativo "violencia" se populariza aludiendo a connotaciones de amplio espectro, que incluso derivan en acciones criminosas. Las manifestaciones de esta son cada vez más disímiles y han trastocado a todos los sectores; los entornos virtuales no han quedado ajenos a su influencia. Al ser la realidad virtual una proyección ideológica de la realidad material, esta ha trasladado a sus planos digitales.

Experiencias deleznable de violencia que se presumían meramente empíricas, ahora sabemos tienen manifestaciones virtuales en el ciberespacio. En la actualidad, múltiples legislaciones han erigido fiscalías especializadas en cibercriminalidad que procuran combatir eventos delictivos tales como el *grooming*, el *ransomware*, el *phishing*, la suplantación de identidad, la difusión de pornografía infantil, etc.

Este fenómeno creciente ha emergido con denuedo a raíz de la proliferación de las nuevas tecnologías de la información y la comunicación, las cuales están siendo utilizadas negativamente para efectos no solo inmorales, sino incluso delictivos. Luego entonces los retos que está enfrentando por esta razón el derecho penal son ingentes y muy difíciles de contrarrestar debido a la celeridad con la que emergen nuevas tecnologías que se están empleando con propósitos ilícitos.

La justicia resarcitoria y la difusión de la cultura de paz deben tornarse en la respuesta para atenuar esta problemática que ya parece desbordada. Las acciones de profilaxis, concientización y re-educación digital son valores de suprema importancia que deben ser socializados desde las edades tempranas a través de programas educativos que promuevan el manejo ético y consciente de las tecnologías de la información y la comunicación en todas sus gamas. Esta tarea educativa debe incentivarse desde la educación básica que es en donde los menores tienen su primer contacto con estos dispositivos virtuales.

La cultura de paz, el respeto, el decoro, la dignidad, la tolerancia y la autonomía deben ser valores que deben prevalecer siempre en el mundo virtual, y su afianzamiento solo puede lograrse desde la concientización y la educación cívica digital. Alcanzar este objetivo no debe percibirse como una tarea utópica e inaccesible, sino como una realidad asequible que puede lograrse con la suma de voluntades de todos los actores sociales, a través del diseño de programas y políticas públicas implementadas de forma asertiva, inteligente, consciente y transversal.

Y si bien es cierto que hay conductas criminales en los entornos virtuales que ameritan un tratamiento más frontal y enérgico, al menos en las conductas baladís los Estados deben garantizar la instauración de programas eficaces que intenten proscribir las prácticas de violencia moral (denostaciones, *bullying*, segregación, etc.), siendo estas últimas, prácticas hostiles e inmorales que se han acentuado especialmente en las redes



sociales, que por lo general son consideradas conductas menores, pero que a menudo (más común de lo que se cree) son acciones que inoculan eventos delictivos ulteriores.

Las legislaciones creadas *ex profeso* para regular este fenómeno deben endurecer sus postulados, a efecto de poner diques y filtros que reduzcan al máximo estas formas de violencia implícita y explícita que tanto pululan en la actualidad.

Las redes sociales que en su origen fueron pensadas para unir a las personas y dinamizar las comunicaciones entre ellos, se han tornado en ecosistemas potencialmente criminógenos en dónde los grupos delictivos se han infiltrado para reclutar personas e inmiscuirlos en células delictivas; así mismo las redes sociales también se han visto contaminadas por el mercado negro a través del tráfico de drogas y trata de blancas. Es por ello que la regulación del uso del internet es una tarea incommensurable que debe ser colmada sin demora, con la finalidad de combatir el fenómeno de la ciberdelincuencia.

El impulso de principios deontológicos, la creación de políticas públicas focales y el fortalecimiento normativo del ciberespacio son encomiendas que los Estados deben asumir con renovado esfuerzo de forma estratégica, frontal y holística, teniendo a los derechos humanos como los ejes rectores que permitan ir afianzando progresivamente la tan anhelada cultura paz en los ecosistemas virtuales.

## 9. Fuentes de consulta.

Bourdieu, Pierre. *La dominación masculina*. Barcelona: Anagrama, 2003.

Código Penal Federal. 2008, México, Congreso de la Unión. Diario Oficial de la Federación.

Convención Americana sobre Derechos Humanos. 1978, Costa Rica, OEA. Convención de los Derechos del Niño. 1989, Suiza, UNICEF.

Galtung, Johan. *Tras la violencia, 3R: reconstrucción, reconciliación, resolución. Afrontando los efectos visibles de la guerra y la violencia*. España: Bakeaz, 1988.

Gellman, Robert. *The National Center for Automated Information Research*. Washington: ILC, 1996.

Katsh, Ethan. *The Online Ombuds Office: Adapting Dispute Resolution to Cyberspace*. Massachusetts: University of, Department of Legal Studies, 1995.

Lefebvre, Henri. *Crítica a la vida cotidiana*. París: Stock, 1979.

Ley General de Acceso de las Mujeres a una Vida Libre de Violencia. 2021, México, Congreso de la Unión. Diario Oficial de la Federación.

Lynch, Khaterine. *The forces of economy Globaliation*. London: Kluwer Law International, 2003.

Manero Brito Roberto. *Consideraciones teóricas sobre el estudio de la violencia*. México: Enseñanza e Investigación en psicología, 2017.

Organización de las Naciones Unidas. “Protocolo de la ONU para combatir la violencia en línea contra las mujeres y las niñas”, 2018, <https://en.unesco.org/sites/default/files/highlightdocumentspanish.pdf> (Consultado: 15/02/2024).

Organización Mundial de la Salud, OMS. *Informe mundial sobre la violencia y la salud*, E.U.A., Washington, 2009.

Sánchez Adolfo, V. *Ética*. Barcelona: Grijalbo, 2000.

Trujillo Elsa. “Aproximación teórica al concepto de violencia: avatares de una definición”, *Política y Cultura* 32, (2009): 20.