

INTERACCIÓN DEL DERECHO Y LAS TECNOLOGÍAS: RETO PARA UNA NUEVA SOCIEDAD CON CONCIENTIZACIÓN DIGITAL¹⁵⁶

Edda Karen Céspedes Babilón^{157*}

RESUMEN

La carrera de Derecho en la Universidad Nacional de Río Negro incorporó en su Plan de Estudios Obligatorio la asignatura Derecho Informático, ubicándola así como una de las primeras carreras de universidades públicas del país en tener esta política de formación. Ello entendiendo que resulta necesario que los futuros profesionales del Derecho en todas sus funciones conozcan la relación entre su actividad y las nuevas tecnologías. Por lo que se busca estimular la lectura, el estudio y el análisis crítico en los temas que hacen a la relación entre el derecho y las tecnologías de la información y las comunicaciones.

El Derecho Informático representa un área de vacancia en la formación jurídica con impacto en el ejercicio profesional del Derecho, el acceso a la justicia y el estado de derecho en la sociedad de la información.

Ello ha impulsado a desarrollar actividades de investigación y extensión en múltiples temas vinculados con el derecho aplicado al ciberespacio.

156 Enlace al video <https://youtu.be/M1Q0He3VHMY>

157* Abogada Investigadora y Fedataria Juramentada especialista en Derecho Informático y TIC. Directora y Fundadora de Interactuemos Derecho Tecnología y Ciencia – IDTC. Miembro del Consejo Consultivo Nacional de Informática de la Presidencia del Consejo de Ministros PCM-SEGDI – mail: kcespedes@infonegocio.net.pe - <https://www.facebook.com/EddaKarenCespedesBabilon/> - www.linkedin.com/in/eddakarencespedesbabilon

PALABRAS CLAVE: Derecho Informático, enseñanza, innovación, formación profesional - ciberderechos

INTRODUCCIÓN

Vivimos un vertiginoso crecimiento en la Tecnología, cuya necesidad de uso ha sido extremadamente impulsada por los tiempos actuales de crisis, causando significativos cambios en nuestra vida familiar, laboral y profesional; y en consecuencia, se fue manifestando en la ciudadanía, cierta confusión por el obligatorio aislamiento social, que conllevó a la sociedad en general, a desenvolverse rápidamente en un ambiente digital dentro de una mezcla de desconcierto y temor, principalmente por el desconocimiento a lo que nos enfrentábamos, y la extrema necesidad de conocer y manejar las herramientas digitales, sin darnos tiempo de tomar conciencia adecuada del impacto de la Transformación Digital, impulsada apresuradamente por ésta crisis.

En ese sentido, fue menester desenvolvernos desde nuestros hogares, en actividades necesarias como Educación y Trabajo, originando, en muchos casos, un desorden y stress social que, en la actualidad, aún necesita de muchos esfuerzos para restablecer el

orden y la tranquilidad que permitan dar paso al conocimiento y uso adecuado de las Tecnologías.

Dentro de éstos avatares, el Derecho como ciencia y disciplina de regulación y normatividad, juega un rol importante en nuestra sociedad, que responsabiliza a todos los profesionales a trabajar arduamente; no sólo para evitar que el Derecho quede rezagado en el tiempo soslayando la modernidad de la Tecnología y la Ciencia, sino, además, nos convoca a realizar un trabajo investigativo que permita resaltar al Derecho como baluarte de valores, justicia y respeto por los Derechos fundamentales de la Persona inserto en los Derechos Humanos, que deben prevalecer en temas tan importantes como la evolución de los algoritmos, la neurociencia, la robótica, el Internet de las Cosas y en general todo lo referente a la Inteligencia Artificial que se torna en un ente principal de controversia y estudio, ahondándose la prioridad y respeto del marco constitucional y la Protección de los Datos Personales; asimismo, resguardar y actualizar el marco legal de

los Delitos Informáticos, como el Cibercrimen, la Ciberseguridad, la Seguridad de la Información, además de la evolución del Teletrabajo, Telemedicina, Telesalud, Teleeducación y otros rubros de avances tecnológicos y nuevos descubrimientos científicos cuya necesidad de investigación y aplicación de un marco regulatorio se tornan prioritarios.

Ésta situación de necesidad normativa y regulatoria, obliga a los Gobiernos y Estados a tomar cartas en el asunto, siendo menester priorizar la convocatoria a profesionales calificados y multidisciplinarios, con el fin de interactuar en un equipo de trabajo exclusivo para la “Concientización Digital” de toda la ciudadanía, donde emerja la adecuación a una verdadera Transformación Digital basada y enraizada en una labor sostenible de Alfabetización y Educación que llegue a todas las zonas del país, con el fin de generar una “Cultura Digital”, que nos permita como Estado y Sociedad afrontar los nuevos retos del impacto tecnológico y científico.

PROBLEMA

El desconocimiento de la ciudadanía, en general, sobre el impacto del avance de las tecnologías, y la falta de interacción de disciplinas tan importantes como el Derecho, han originado un atraso socio-tecnológico que se ve afectado actualmente en la economía de muchos países.

OBJETIVO

Conocer la importancia de la interacción del Derecho con el avance de las Nuevas Tecnologías y la Ciencia, creando un marco legal que permita su progreso basado en los valores humanos, los derechos fundamentales de la persona y en el acceso a la Educación y Concientización Digital desde la ciudad hasta las zonas más alejadas del país.

MARCO TEÓRICO

Durante algún tiempo atrás, en Latinoamérica, el tema de la Transformación Digital venía dando sus pasos en diversos países, quizás en algunos más que en otros, pero lo certero y sin duda alguna, es que la crisis

pandémica no sólo aceleró su proceso, sino que, además, nos obligó intempestivamente a afrontar una nueva realidad sin estar completamente preparados.

Éste nuevo mundo transformado por las tecnologías y la ciencia debe iniciarse con la base de ciertos conceptos indispensables e imprescindibles para el manejo adecuado de las herramientas digitales y asimismo prepararnos en un marco de concientización digital, que nos permita evitar los peligros y riesgos por el mal uso que, los ciberdelincuentes y las personas sin escrúpulos, les dan a las nuevas tecnologías.

INTERNET

El mundo se revolucionó, desde que nació Internet, (*International Network of Computers*), allá por los años 60, llamada también la “Red de Redes”, o descrita en sus orígenes como la “Red Galáctica”¹ (*Galactic Network*) por J.C.R. Licklider² del MIT³, cuyo concepto es muy similar al Internet de hoy. Una versión muy conocida es que Internet nació como ARPANET, en respuesta al Departamento de Defensa de los Estados Unidos de Norteamérica, en la Guerra Fría; sin embargo, fue Licklider como director del Programa de Investigación informática de

DARPA, (1962) quien, seguido por Ivan Sutherland, Robert Taylor y Lawrence G. Roberts, desarrollan el proyecto, que continua en investigación y avance por Leonard Kleinrock, Paul Baran y otros más.

Lo cierto es que Internet revolucionó la Informática y las comunicaciones interconectando a las personas con diferentes computadoras a nivel mundial y actualmente el número de usuarios de Internet se viene incrementando exponencialmente debido al uso de los dispositivos móviles.

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES - TIC

Internet es una fuente de información y conocimiento y sus servicios múltiples van en crecimiento, como el uso de la Web⁴, correos electrónicos, telefonía, transmisión de datos multimedia, mensajería instantánea, redes sociales, videojuegos, plataformas de intercambio de archivos, plataformas multimedia (audio y video), comercio electrónico y muchos otros desarrollos de las Tecnologías de la Información y las Comunicaciones (TIC), a las cuales podemos acceder mediante Internet, que en sí misma es parte de las TIC.

Por lo expuesto las TIC son el conjunto de tecnologías que permiten el acceso, producción, transmisión, procesamiento, almacenamiento, recuperación y tratamiento de la información y que se desarrollan a partir de los avances científicos producidos en los ámbitos e interacción de la informática y las telecomunicaciones.

CIBERDELITOS

Los Ciberdelitos son aquellas actividades ilícitas o antijurídicas cuyo fin malsano es causar daño, provocar pérdidas o impedir el uso de los sistemas y redes informáticas

Los ciberdelitos afectan a un conjunto de bienes, que pueden ser dirigidos hacia las personas, a las empresas o a los intereses colectivos, y tienen diferentes modalidades como:

- **Ciberacoso:** Violan los derechos fundamentales de la persona, como el derecho a la privacidad e intimidad, derecho al honor y la dignidad de la persona, estos delitos generalmente se suscitan a través de las Redes Sociales con calumnias y amenazas y/o el chantaje sexual llamado Sextorsión⁵.
- **Grooming:** Una indignante figura delictiva, que tiene diferentes

modalidades, como aquellos realizados por ciberdelincuentes pedófilos quienes atentan sexualmente contra los menores de edad.

- **Phishing:** Otra modalidad de ciberdelito que hace uso de la ingeniería social o técnicas de engaños utilizada por ciberdelincuentes, valiéndose de la buena fe del usuario final, para lograr obtener y robar información sensible bajo la fachada de un sitio confiable (https)⁶, mediante este método logran obtener claves de acceso, números de tarjetas bancarias y toda información sensible⁷ de la víctima, producto de este engaño; logrando la suplantación de identidad o la clonación de tarjetas.

- **Ciberdelitos de alta tecnología:** Es necesario resaltar los delitos de alta tecnología, originados por Malwares⁸ y Ransomware⁹ que afectan principalmente al sector financiero mundial, en esa categoría podemos mencionar serios delitos de extorsión, operaciones fraudulentas por Internet, sabotaje informático, tráfico ilegal de datos personales, y en general toda operación financiera y comercial engañosa, causada por el acceso no autorizado a los sistemas informáticos, conocido como piratería informática (cracking)

Para evitar los ciberdelitos es necesario tener una política de Ciberseguridad.

CIBERSEGURIDAD

La ciberseguridad es el marco global del cuidado monitoreo y protección tanto de datos como de plataformas informáticas en el cual se aplican políticas de seguridad informática para evitar acciones delictivas sobre estos activos. (Leonett, J. R.)

INTELIGENCIA ARTIFICIAL

Fue en el año de 1956 que John McCarthy¹⁰ lanza el concepto de Inteligencia Artificial definiéndola como la ciencia e ingeniería de hacer máquinas inteligentes.

La comunicación de la Comisión Europea¹¹ en el Plan coordinado sobre Inteligencia Artificial, indica: "...se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos..."

Con éstos y otros antecedentes teóricos y prácticos se puede definir que la

Inteligencia Artificial (IA) es una tecnología digital que combina algoritmos en un programa, con el fin de crear máquinas que proporcionen capacidades como interpretación, decisión y resolución de problemas.

El sofisticado avance de la IA genera controversias en su comparación con el ser humano, sin embargo, es indudable el crecimiento acelerado de proyectos innovadores en sectores estratégicos, que traen consigo un impacto en el desarrollo de la economía a nivel mundial (Céspedes B., E.K. IDTC)¹²

La IA trabaja a través de algoritmos y está muy ligada al Internet de las Cosas y la Robótica

- **Algoritmo** es un conjunto de instrucciones y pasos lógicos necesarios, o reglas definidas, finitas y jerarquizadas, que permiten llevar a cabo una tarea específica, solucionar un problema o situación planteada, procesar datos, analizar, efectuar toma de decisiones y realizar otras tareas o actividades. Por ejemplo: Google cuenta con un algoritmo para su sistema de búsqueda y posición de páginas. Otro ejemplo es el contenido de las Redes Sociales que está regido por algoritmos que permiten la interacción con los usuarios. (Céspedes B., E.K. IDTC)¹³

- Internet de las Cosas

También llamado “IoT” (*Internet of Things*), el creador del “Concepto el Internet de las Cosas” es Kevin Ashton. IoT se refiere a la interconexión digital con Internet, de objetos físicos que por intermedio de circuitos integrados, sensores y conectividad, permiten el intercambio automático de información y datos con otros dispositivos inteligentes y centros de control.

Inicialmente la IoT surgió para interconectar objetos domésticos; pero actualmente se vienen realizando aplicaciones en la vía pública, las instituciones y al interior de las empresas. (Céspedes B., E.K. IDTC)¹⁴

- Robótica

La Robótica es la creación de Robots. Se ocupa del diseño, construcción, operación, estructura, manufactura, y aplicación de los robots que le permita realizar diversas tareas en diferentes áreas, combinando múltiples disciplinas como la mecánica, la electrónica, la Informática, la Inteligencia Artificial, la Ingeniería de Control y la Física.

Es importante mencionar que, dentro de estos conceptos mencionados, con fines académicos, el rol de los Datos

Personales constituye una materia importante en el buen uso de las herramientas digitales y dentro del respeto de los derechos fundamentales de la persona. Es decir, la regulación de la Protección de Datos Personales debe figurar con notable relevancia, dentro del marco jurídico de cada país en paralelo al continuo avance tecnológico actual.

RELEVANCIA DE LA INTERACCIÓN DEL DERECHO Y EL AVANCE TECNOLÓGICO EN EL SIGLO XXI

Una de las formas tradicionales e iniciales de concebir la interacción entre el Derecho y las Tecnologías es a través del contexto de la Informática Jurídica que considera la aplicación de la informática como un instrumento para el Derecho, constituyéndose en un objeto de estudio y reglamentación; de ahí se origina la necesidad de una rama del Derecho que se encargue de regular los efectos y controversias jurídicas originadas por el uso masivo de los sistemas informáticos.

DERECHO INFORMÁTICO

El Derecho Informático, nace como una rama del derecho especializada en el tema de la informática; sus usos, aplicaciones e implicaciones legales, las cuales ameritan el surgimiento de nuevas

normas jurídicas y/o la actualización de las existentes.

El Derecho Informático abarca muchas otras ramas del Derecho partiendo de los principios constitucionales, que protegen los derechos fundamentales de la persona como la intimidad, el honor, la dignidad y el uso ilegal de los sistemas informáticos; que son violados mediante correos electrónicos, mensajerías instantáneas o las redes sociales que se han masificado; en ese sentido el rol del Derecho Penal se hace necesario para salvaguardar la violación de éstos y otros derechos. En el caso del Derecho Civil, tomaré el ejemplo de la regularización de las notificaciones electrónicas que ameritan un gran avance en los procesos judiciales, así como la regulación de la Manifestación de Voluntad por medios electrónicos, (artículo 141-A del Código Civil Peruano), y la firma Digital, en el Perú con la Ley 27269 Ley de Firmas y Certificados Digitales (26may2000); normas que han facilitado el desarrollo del Comercio Electrónico. Cabe resaltar que el Perú es el único país que desde el año 1991, a través del Decreto Legislativo 681 (14oct1991), crea la figura del Fedatario Juramentado con especialidad en Derecho Informático, quien, como dador de Fe Pública, utiliza la Firma y el

Certificado Digital como herramientas necesarias para garantizar la Seguridad Informática y la Seguridad Jurídica.¹⁵ (Céspedes Babilón, E.K)

LA IMPORTANCIA ACTUAL DEL TELETRABAJO

El Teletrabajo es legislado en muchos países pero carente de una previa y adecuada capacitación ha traído innumerables contradicciones al respecto del intempestivo confinamiento domiciliario y obligación de las personas a trabajar desde casa, en ese sentido el Perú cuenta con la Ley 30036 Ley del Teletrabajo (05jun2013) que cubre derechos y obligaciones laborales e indica la voluntariedad del trabajador para tomar ésta alternativa laboral; pero para evitar la propagación del Coronavirus, se publicó el Decreto de Urgencia 026-2020 donde se establecen diversas medidas excepcionales entre las cuales se configura el Trabajo Remoto (art. 16 y 23) el cual establece el deber de realizarlo desde el domicilio del trabajador subordinado, mediante herramientas tecnológicas, según sea el caso. La figura del Trabajo Remoto, trajo consigo innumerables controversias y problemas sociales, que aún siguen en vigencia, debido a la obligatoriedad, el

desconocimiento del trabajador en el uso de las herramientas digitales, la falta de infraestructura del trabajador, el abuso del empleador fuera de las horas laborales, el recargo de las tareas domésticas y familiares, y en general la falta de prevención de seguridad informática o ciberseguridad, que trae consigo la exposición de la privacidad, la protección de datos personales y en general la exposición al trabajador y la empresa extendiéndose a los miembros de las familia debido a la intromisión ilegal de la ciberdelincuencia.

EL CRECIMIENTO DE LOS CIBERDELITOS

En el uso de la Tecnologías es importante destacar la penosa masificación de la intrusión de los Ciberdelincuentes, con actitudes sociópatas,¹⁶ quienes a través de diferentes técnicas y recursos comenten acciones criminales o al margen de la Ley causando graves daños.

Con respecto a los **Ciberdelitos** es importante mencionar al tratado internacional denominado “Convenio contra la Cibercriminalidad”, mejor conocido como el “Convenio de Budapest” cuyo objetivo es la lucha contra la ciberdelincuencia basada en la aplicación

de un marco jurídico y política penal en armonía mundial. El Perú cuenta con la Ley 30096, Ley de Delitos Informáticos y es uno de los países adheridos a este Convenio internacional, por lo que debemos seguir sus lineamientos, y asimismo mejorar y/o adecuar nuestras normativas y políticas públicas para seguir avanzando en el combate contra el cibercrimen, debido a que somos el quinto país de Latinoamérica que recibe mayor cantidad de ataques cibernéticos. Según la División de Investigación de Delitos de Alta Tecnología (DIVINDAT)¹⁷, los ataques que recibe nuestro país son de fraudes electrónicos, abuso sexual infantil, suplantación de identidad. y ataques que en su mayoría afectan al sector financiero.

LA REDES SOCIALES, LA PRIVACIDAD Y VIOLENCIA DIGITAL

La privacidad como factor importante de respeto y derecho de las personas se hace vulnerable por el desconocimiento de la adecuada protección de los contenidos que se publican en los diferentes medios digitales. En este sentido, las Redes Sociales, no sólo se utilizan en el marco de la comunicación, diversión amistad y conocimiento, que fue el inicio de su creación; sino que se han convertido en un foco de Violencia

Digital¹⁸. Estos contenidos voluntarios e indiscriminados son realizados, en general, por los mismos cibernautas, haciendo pública su vida, su familia, amigos, lugares visitados, conexiones, etc., ocasionando una excesiva información que puede ser utilizada y configurada en perfiles sistematizados (Big Data)¹⁹ para el marketing de algunas empresas con el fin de generar aumento en sus ventas; pero también son utilizados por los ciberdelincuentes para sus propios fines delictivos. Los individuos que realizan Violencia Digital se constituyen en el prototipo de persona de bajos instintos, con personalidad agresiva y fines de hacer daño. (Céspedes Babilón, E.K.)

LA DISRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL (IA)

En el caso del sofisticado avance de la Inteligencia artificial, es necesario resaltar que la IA actualmente ayuda a resolver problemas de salud y seguridad y ha sido de gran impacto en la lucha contra la pandemia. Asimismo, ha generado gran avance en la Agricultura con drones y sistemas inteligentes y otros campos y profesiones como el Derecho donde la eficacia y rapidez se constituyen en una mejor atención en los procesos y

resoluciones judiciales. Sin embargo, la IA ha generado muchas controversias con el respecto a la violación de los derechos fundamentales de la persona y los valores humanos como la Moral y la Ética, por otro lado, existe cierto temor de que la IA reemplazará al ser humano. Estas premisas y dudas se fundamentan en que la IA puede ser discriminatoria, y sesgada, como se ha visto en el caso del algoritmo de los vehículos autónomos²⁰ y las resoluciones judiciales del algoritmo “Compass”²¹ en EEUU. Estas controversias sobre su uso y los valores humanos como la Ética se generan en muchos campos y son materia de discusión y necesaria regulación.

Aún no tenemos una normatividad jurídica al respecto de la Inteligencia Artificial; pero existen algunos organismos internacionales que vienen ocupándose de su regulación y la “Ética” que debe primar en su uso. Por ejemplo, en la Unión Europea se ha conformado el Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial (2019), la Comisión Europea para la eficiencia de la Justicia (CEPEJ) que emite la Carta Ética Europea (diciembre 2018) y la modernización del Convenio 108 (2018) que incluyen principios y respeto a los derechos humanos. Con ese mismo

objetivo, la UNESCO, lanzó una encuesta sobre ÉTICA, (Julio 2020) cuyos resultados están previstos para fines del 2021.

En el desarrollo de la IA y sus fines regulatorios, también es conveniente y necesario enfocarla, desde el marco de la Responsabilidad Civil, teniendo en cuenta que es el ser humano quien crea el algoritmo.

En este punto, cabe resaltar que la Inteligencia Artificial está conformada por los Algoritmos y los Datos. Por lo tanto, es importante mencionar que los Datos Personales, son un tema sensible y su utilización es primordial, no sólo en la Inteligencia Artificial, sino además en muchas materias dentro del avance tecnológico.

IMPORTANCIA DE LA PROTECCIÓN DE DATOS PERSONALES Y LA CIBERSEGURIDAD

Actualmente, la dinámica galopante de las TIC demanda un mayor reto al Derecho Informático para garantizar el marco jurídico de protección y respeto a las leyes en aras de un orden social que garantice el desarrollo, innovación y aplicación de las nuevas tecnologías.

PROTECCIÓN DE DATOS PERSONALES

Uno de los temas más relevantes es la vulnerabilidad de la Privacidad y la Protección de Datos Personales en el uso de las tecnologías, cuando no se toman las medidas de seguridad preventivas para evitar ser víctimas del ataque de los ciberdelincuentes, de ahí la importancia de la Ciberseguridad.

Es importante mencionar al Reglamento General de Protección de Datos Personales de la Unión Europea (RGPD 2016/679) del Parlamento Europeo y del Consejo del 27 de Abril 2016 relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de Datos Personales y a la Libre Circulación de estos datos y por el que se deroga la Directiva 95/46/CE, el cual marca los lineamientos del que se rigen muchos países para la adecuación de su normativa jurídica y políticas de seguridad. El Perú ha tomado sus lineamientos y contamos con la Ley 29733 Ley de Protección de Datos Personales (03jul2011) y el Decreto Supremo 003-2013-JUS (22mar2013). Cabe mencionar que todo esfuerzo regulatorio es insuficiente, si se obvia la sensibilización de las medidas preventivas

para cumplir el objetivo de la ley; y en ese sentido, es necesaria la interacción e intervención de profesionales multidisciplinares, así como del gobierno y el Estado.

IMPORTANCIA DE LA CIBERSEGURIDAD

Las TIC fueron creadas para cubrir las necesidades y demandas de las personas, mediante herramientas que nos proporcionan enormes ventajas; pero debemos resaltar, también, que ha facilitado el ataque de ciberdelincuentes quienes utilizan estas herramientas tecnológicas para cometer sus delitos.

Las intrusiones dañinas cometidas por los ciberdelincuentes a través de diferentes modalidades pueden afectar seriamente a una persona²², una empresa, un gobierno (infraestructura crítica) o todo un país²³. Es por lo que debemos tener presente el resguardo de nuestra información y datos mediante sistemas de seguridad que nos proporcionen una navegación segura, desde nuestros hogares, centros laborales y gobierno. En ese sentido toma especial relevancia la **Ciberseguridad** como una prioridad a ser aplicada en todos los ámbitos del uso de las tecnologías, desde el ámbito personal hasta en las organizaciones, instituciones

y empresas privadas y públicas. Pero es necesario que para implantar políticas de ciberseguridad se realice una capacitación previa que involucre a todas las personas, ejecutivos y funcionarios en general creando una cultura de seguridad que parta desde la familia y los Centros Educativos para evitar intromisiones ilegales y ataques delictivos. En el caso de las empresas, la Ciberseguridad debe convertirse en una prioridad y actividad crítica para la protección de la información y cumplimiento de los objetivos empresariales, que asimismo pueden crecer con la utilización adecuada de la Inteligencia Artificial y evitar lo que indica el Ing. Leonett: *“El déficit de las medidas de seguridad y mal cumplimiento de los protocolos de ciberseguridad ha orillado al sector IT en la solicitud y socorro de la Inteligencia Artificial para corregir y mermar estos errores”*

Como vemos resulta insuficiente el marco jurídico aplicado a las nuevas tecnologías, y debemos enfrentarnos a nuevos retos, como el desarrollo vertiginoso de la Inteligencia Artificial, la Neurociencia, Computación Cuántica, el avance del Blockchain, el Bioderecho, crecimiento del Big Data, Red Cloud y otros, donde la justicia, los valores humanos y la educación deben priorizarse.

APORTES E IMPORTANCIA PRIORITARIA DE LA CONCIENTIZACIÓN DIGITAL

Para lograr una conciencia digital en la población debemos asegurarnos previamente de la Alfabetización y Educación digital que versa en la enseñanza y aprendizaje sobre el buen uso de Internet y la aplicación de las herramientas digitales. Este proceso debe incluir el marco de prevención contra las acciones lesivas a los derechos fundamentales de la persona en congruencia con la Inclusión Digital y creando una Cultura Digital, a nivel país, en favor de lograr las metas y objetivos de cada disciplina.

Por tanto, indico que “La Concientización Digital versa en el Saber Humano, que consiste en conocer, analizar, reflexionar e interiorizar el impacto del desarrollo e innovación de las ciencias tecnológicas que interactúan en nuestras vidas; asimilando a plenitud sus efectos, consecuencias e interacción en la vida de todas las personas, sea en el ambiente familiar, social, profesional, empresarial, y, en general, como ciudadanos, para lograr un cambio cultural positivo y una Transformación Digital que nos permita un

desarrollo socio económico a nivel mundial”.

En este proceso y para la objetiva reducción de la brecha digital, debe partirse por la conectividad desde la ciudad hasta las zonas más alejadas, por eso es necesario la aplicación de políticas sostenibles pero ejecutables a corto plazo donde se involucre el Estado, el Gobierno, el Sector Privado y los ciudadanos en general; porque “No podemos hablar de Transformación Digital sin Concientización Digital”

En ese sentido reitero mi convocatoria, desde aquí a ese abogado “apasionado” en su carrera profesional, que supera obstáculos y limitaciones; investigando, conociendo y compartiendo información; incentivado por ese “espíritu hacker”²⁴ que puede aplicarse a los juristas, que crean, mejoran y perfeccionan el marco legal, con el fiel objetivo de contribuir al Derecho y la Justicia. (Céspedes B., E.K.)

Asimismo, me atrevo a proponer una vez más, una Reforma Educativa que incluya cursos de valores humanos, patriotismo y desarrollos de tecnologías en el marco de la Concientización Digital, desde las aulas preescolares hasta las Universidades e Institutos Superiores.

Aún hay mucho por versar y mucho por hacer, pero nos queda asumir el reto, y difundir el respeto por la justicia, los valores y los derechos fundamentales de la persona, desde nuestra vida cotidiana y en el buen uso de las Tecnologías, para forjar, seres humanos conscientes de una cultura digital en favor de la sociedad, así como el crecimiento y desarrollo de nuestro país.

BIBLIOGRAFÍA

1. BARZANALLANA, Rafael - Biografía de Joseph Licklider “Uno de los Padres de Internet” – Departamento Informática y Sistemas – Universidad de Murcia, España

<https://www.um.es/docencia/barzana/BIOGRAFIAS/Biografia-JCR-Licklider.php>

2. CASTELLS, M. “Internet y la sociedad Red”. Lección inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento. <http://www.uoc.edu/web/esp/articulos/castells/castellsmain1.html>

3. CÉSPEDES BABILÓN, Edda Karen “Interactuemos, Derecho Tecnología y Ciencia – IDTC EKCB - Lima, Perú

<https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaIDTC>

4. CÉSPEDES BABILÓN, Edda Karen “El Fedatario Informático en el Perú” XV Congreso Iberoamericano de Derecho e Informática – FIADI 2011 Buenos Aires, Argentina

http://www.eldial.com/nuevo/congreso_iberoamericano/EL%20FEDATARIO

[%20INFORM%3%81TICO%20EN%20EL%20PER%3%9A.pdf](#)

5. CÉSPEDES BABILÓN, Edda Karen. Conferencia: “Violencia Digital y sus implicancias en el Derecho de las Personas” III Congreso Internacional de Derecho. Facultad de Derecho. Universidad San Tomás. Villavicencio, Colombia. 2017

6. CÉSPEDES BABILÓN, Edda Karen. “El Hacker del Derecho” XIX Congreso Iberoamericano de Derecho e Informática FIADI 2015 Medellín, Colombia <http://fiadi.org/wp-content/uploads/2015/08/Edda-Karen-Cespedes.pdf>

7. COMISIÓN EUROPEA – Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y social Europeo y al Comité de las Regiones – Plan coordinado sobre la Inteligencia Artificial – Bruselas 2018 <https://ec.europa.eu/transparency/regdoc/ep/1/2018/ES/COM-2018-795-F1-ES-MAIN-PART-1.PDF>

8. GUILLEN TORRES, Beatriz “El verdadero padre de la Inteligencia Artificial” <https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/el-verdadero-padre-de-la-inteligencia-artificial/>

9. INTERNET SOCIETY: “Breve historia de Internet”

<https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#:~:text=Or%C3%ADgenes%20de%20Internet,concepto%20de%20%E2%80%9CRed%20gal%C3%A1ctica%E2%80%9D.>

10. LEONETT, JOSE R. Observatorio Guatemalteco de Delitos Informáticos – OGDI – <https://ogdi.org/>

11. PRESIDENCIA DEL CONSEJO DE MINISTROS Perú se adhiere al Convenio de Budapest para luchar contra la Ciberdelincuencia

<http://www.pcm.gob.pe/2019/02/peru-se-adhiere-al-convenio-de-budapest-para-luchar-contra-la-ciberdelincuencia/>

12. UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA CSIRT Seguridad de la Información <https://csirt.utpl.edu.ec/10-consejos-para-evitar-ataques-de-phishin5>

NOTAS

1 Red Galáctica: Conjunto de ordenadores interconectados globalmente a través de los que todo el mundo rápidamente a datos y programas desde cualquier

2 Joseph Carl Robnnet Licklider uno de los padres

3 MIT: Instituto Tecnológico de Massachusetts – Universidad Privada en Cambridge, Massachusetts.

4 Web: World Wide Web o Red Informática de alcance mundial que permite interconectar sistemas de hipertexto. Para utilizar la Web se necesita un navegador como Google Chrome, Mozilla Firefox, Microsoft Edge, etc.

5 Sextorsión: Chantaje sexual por la posesión de una imagen íntima.

6 https Protocolo seguro de transferencia de texto *Hypertext Transfer Protocol Security*

7 ONU – Que es Información sensible?

8 Malware: Software malicioso diseñado para infiltrarse, sin autorización, en un dispositivo

9 Ransomware (secuestro de datos): Programa que impide el acceso a un sistema operativo, pidiendo un rescate a cambio de quitar la restricción.

10 John MacCarthy organiza la Conferencia de Dartmouth en 1956 donde por primera vez acuña el concepto de IA, reconocido como el Padre de la Inteligencia Artificial.

11 Comisión Europea - Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Consejo social Europeo y al Comité de las Regiones – Plan coordinado sobre la Inteligencia Artificial – Bruselas 2018

12 <https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaDTC/posts/586553578544387>

13 <https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaDTC/posts/824613844738358>

14 <https://www.facebook.com/InteractuemosDerechoTecnologiayCienciaDTC/posts/842837086249367>

15 El Fedatario Informático en el Perú

http://www.eldial.com/nuevo/congreso_iberomericano/EL%20FEDATARIO%20INFORM%C3%81TICO%20EN%20EL%20PER%C3%9A.pdf

16 Actuación con dolo. (José R. Leonett 17 Policía Nacional del Perú – Ministerio del Interior MININTER

18 Ciberacoso, Grooming, Cyberbullying, Phishing,

19 Grandes volúmenes de Datos estructurados para

20 Automóviles que disponen de tecnologías

frenar, adelantar, estacionarse, necesidad de la conducción de una persona.

21 Algoritmo que analiza el historial delictivo y predice la reincidencia en un delito.

22 Ciberacoso, Grooming, Cyberbullying, Phishing,

23 Ciberguerras, Ciberterrorismo.

24 “El Hacker del Derecho” Céspedes Babilón, Edda Karen