

Interpretación de la ciberseguridad y los derechos digitales

Armendáriz Sigala, Alma Rosa
Delgado López Mónica
Juan Armando Márquez Enríquez

monica.dl@chihuahua.tecnm.mx

armendarizsigala@yahoo.com

juan.me@chihuahua.tecnm.mx

*Tecnológico Nacional De Mexico, Campus Tecnológico De Chihuahua
Av. Tecnológico No. 2909, Col. 10 de mayo
Chihuahua, Chihuahua, México, C.P 31200*

Recibido:

2025/02/28

Aceptado para su publicación: 2025/02/28

Publicado: 2025/06/30

Resumen: La internet ha transformado profundamente nuestra vida diaria, convirtiéndose en una herramienta esencial para la comunicación, el trabajo y la educación. Sin embargo, con su crecimiento también han surgido desafíos relacionados con los derechos humanos, la privacidad y la protección de los datos personales. Es fundamental que todos los actores involucrados, tanto públicos como privados, se comprometan a garantizar la seguridad digital, implementando algoritmos de ciberseguridad que protejan los derechos digitales, como la igualdad, accesibilidad, confidencialidad y justicia social.

El uso de internet ha experimentado un auge, especialmente durante la pandemia de COVID-19, creando un ambiente digital hiperconectado donde la información se multiplica constantemente. Este fenómeno ha generado una discontinuidad generacional, ya que las nuevas generaciones se desarrollan en un entorno digital con un volumen de interacciones sin precedentes, lo que cambia la forma en que procesan la información en comparación con las generaciones anteriores. Sin embargo, este crecimiento también ha incrementado los riesgos asociados con la vulneración de datos personales y el uso no autorizado de la información.

La ciencia de datos juega un papel clave en este contexto, ya que mediante el análisis de Big Data se pueden generar predicciones sobre el comportamiento de los usuarios, pero siempre con el compromiso de proteger su privacidad y derechos fundamentales. Es esencial que se desarrollen algoritmos responsables que protejan los intereses de los usuarios y promuevan un entorno digital seguro.

Palabras Clave: Ciberseguridad, Protección de datos personales, Derechos digitales

Abstract: The Internet has profoundly transformed our daily lives, becoming an essential tool for communication, work and education. However, with its growth, challenges have also arisen related to human rights, privacy and the protection of personal data. It is essential that all actors involved, both public and private, commit to ensuring digital security, implementing cybersecurity algorithms that protect digital rights, such as equality, accessibility, confidentiality and social justice.

Internet use has boomed, especially during the COVID-19 pandemic, creating a hyper-connected digital environment where information is constantly multiplying. This phenomenon has generated a generational discontinuity, as new generations are developing in a digital environment with an unprecedented volume of interactions, which changes the way they process information compared to previous generations. However, this growth has also increased the risks associated with the breach of personal data and the unauthorized use of information.

Data science plays a key role in this context, as Big Data analysis can generate predictions about user behavior, but always with the commitment to protect their privacy and fundamental rights. It is essential to develop responsible algorithms that protect the interests of users and promote a safe digital environment.

Key Words: cybersecurity, protection of personal data, digital laws.

Desafíos y Procedencia¹, El apogeo del uso de internet ha extendido la información que se genera segundo a segundo, pareciera que se multiplica factorial cada minuto que hacemos una consulta en la internet. Vivimos en un ecosistema y/o ambiente digital hiperconectado que fue en aumento por el confinamiento obligado a causa de la pandemia COVID19.

Hoy en día no solo cambia gradualmente con respecto al pasado; el modo de convivencia, la ropa que usamos, los estilos de vida, como ha ocurrido entre generaciones, hoy en día se vive una discontinuidad, como resultado de un entorno global en el que los derechos digitales y la ciberseguridad solo son temas de estudio para especialistas en la materia.

Es innegable que las generaciones actuales se desenvuelven en un entorno omnipresente con un gran volumen de interacciones en el universo digital, piensan y procesan la información de manera diferente a sus predecesores. Esto avanza y el uso de las herramientas digitales se convierte en un descuido de sus datos personales, llegan más lejos y más profundamente de lo que los conocedores saben o sospechan, sea cierto o no se puede observar con certeza que los patrones de conocimiento y pensamiento han cambiado de manera exponencial vulnerando la información de los usuarios en algunos casos en el uso no autorizado e ilegal de sus datos personales. La ciencia de Datos para el análisis de información cotidiana, laboral, académica y social etc. debe consistir en el desarrollo de algoritmos para recopilar y analizar la información Big Data con la finalidad de crear predicciones de comportamiento de los usuarios garantizando a los usuarios la privacidad y con ellos salvaguardar los derechos fundamentales.

Con motivo de la pandemia de covid19 el uso y abuso de las redes sociales, aplicaciones tecnológicas, plataformas digitales presentes en la Internet, que si bien es cierto facilitaron las actividades cotidianas y laborales, de manera individual y colectiva tanto que se creó la necesidad de echar mano de lo que no se tenía al alcance e invertir en nuevas tecnologías para estar interconectados, lo que desencadenó un abuso en el uso de la internet y por consiguiente un estado vulnerable para ser cautivo del mal uso de datos personales, robo de identidad por el desconocimiento de los derechos digitales y la ciberseguridad.

Marc Prensky (2001)², una “singularidad”: un acontecimiento que cambia las cosas de manera tan fundamental que no hay vuelta atrás, es la llegada y rápida propagación de la tecnología digital en las últimas décadas del siglo XX. Prensky, se refiere a la nuevas generaciones como “generación-N (por Net) o generación-D (por Digital), pero la designación que se ha utilizado en la actualidad es Nativos Digitales, por su lenguaje digital de los ordenadores, los videojuegos, redes sociales e Internet, esto nos convierte a los mayores de 50 años que no nacimos en el ecosistema y/o entorno digital que fascinados adoptamos todos o amemos casi todos aquellos aspectos de la tecnología y seremos siempre Inmigrantes Digitales, que acudimos a Internet en ocasiones como segundo recurso manteniendo un pie en el pasado y otros con una socialización mas avanzada por así requerirlo su entorno laboral apreciaran las nuevas habilidades de la interacción y práctica.

Estar consciente que es poco probable volver hacia atrás, iríamos en contra la migración cultural, Así que, es mejor enfrentar los desafíos en la cuestiones de derechos Digitales y ciberseguridad, cambiar el significado de lo que es importante, pero que si significa ir mas rápido, las metodologías y contenidos del futuro sorprendente digital y tecnológico que incluye robótica, nanotecnología, hardware, software etc, también incluye políticas publicas, ética, sociología, idiomas y, muchas otros aspectos que van de la mano con la actual generación.

Carta de los derechos humanos y principios para a internet (2015)³, La Coalición Dinámica por los Derechos y Principios de Internet es una red internacional abierta de personas y organizaciones que trabajan para hacer cumplir los derechos humanos en el ambiente online y en todo el espectro de ámbitos de creación de políticas para internet.

¹ Dra- Alma Rosa Armendáriz Sigala, Catedrática del Tec N M campus Chihuahua

² Marc Prensky Nativos Digitales Inmigrantes Digitale En On the Horizon (MCBUniversity Press, Vol. 9 No. 6, December 2001) s, .

³ Carta de los derechos humanos y principios para Internet. (Enero 2015)– 1ª edición Internet Rights and Principles Dynamic Coalition UN Internet Governance Forum. (<http://internetrightsandprinciples.org/wpcharter>).

En 2008 la Coalición IRP promovió los principios basados en los derechos y principios para la gobernanza de Internet en el IGF global. En 2011 la coalición lanzó diez principios⁴, y para el 2013 se llevó a cabo la primer reunión de revisión WSIS+ 10” de UNESCO emprendiendo así la segunda fase de la Carta de los derechos y principios para la internet “ Carta 2.0 “ con un objetivo doble, aumentar la concientización acerca de la Carta a la luz creciente preocupación pública nacional e internacional respecto de la protección y el goce de los derechos humanos tanto Online como Offline y, abrir la participación y la opinión, ya ca actualizar partes de la carta para destacar los derechos humanos y principios contenidos en ella para proveer principios de regulación de internet en el IGF y mas allá.⁵

La internet ofrece variadas oportunidades sin precedentes, no podemos imaginar hoy en día la vida sin Internet, sin redes sociales sin software, sim hardware, sin plataformas digitales, esto es innegable desempeña un papel importante en nuestras vidas, por lo que es necesario, esencial que todos los individuos, agentes de cambio públicos y privados respeten y hagan respetar, protejan y hagan proteger los derechos humanos en internet, Lo mismo que preocuparse y ocuparse por tomar las medidas que garanticen la privacidad en la protección de nuestros datos personales, implementar algoritmos en ciberseguridad que garantice que funcione y evoluciona de manera paralela con las necesidades de uso y cumpla con la protección en derechos digitales de; universalidad e igualdad, justicia social, accesibilidad, diversidad, expresión y asociación, normas y reglamentos, confidencialidad protección de datos y gobierno.

Libertad y seguridad en Internet, como lo consagra el artículo 3 de la Declaración Universal “ Toda persona tiene derecho a la vida, la libertad y la seguridad de su persona” todas las medidas preventivas de seguridad deben estar en concordancia con el derecho y lar normas jurídicas nacionales e internacionales y los derechos humanos- Que quiere decir esto; que aquella medida que restrinja otro derecho humano, por ejemplo el derecho a la intimidad o el derecho de expresión, excepto en circunstancias excepcionales. La internet tiene un papel vital hoy en día para el logro de la efectividad plena de los derechos humanos y la protección contra todas las formas de delitos cibernéticos, incluyendo el ciber-acoso, tráfico de personas y el uso indebido de datos personales o de la identidad digital.

Toda persona tiene el derecho a disfrutar del ecosistema digital, estar interconectados en el ciberespacio, disfrutar de conexiones seguras en el internet, incluyendo protección de servicios y protocolos que pudieran poner en peligro el adecuado funcionamiento de la internet como por ejemplo los virus, códigos indebidos y maliciosos, y phishing de aquí que podemos hacer referencia a la Libertad de expresión e información en internet como lo acuña el artículo 19 de la Declaración Universal de los Derechos Humanos “ Todo individuo tiene derecho a la libertad de opinión y de expresión; ese derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y difundirlas, sin limitación de fronteras, por cualquier medio de expresión”.

En cuanto a la privacidad en internet, el contenido que consagra el artículo 12 de la declaración universal; “ Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilios o su correspondencia, ni de ataques a su honra o a su reputación de la ley con tales injerencias o ataques” En internet el derecho a la privacidad incluye; La legislación nacional sobre la privacidad, Políticas de configuración de la privacidad, Normas de confidencialidad e integridad de los sistemas de las TIC”s, Protección de la personalidad virtual, Derecho al anonimato y a utilizar cifrado, La libertad ante la vigilancia y la libertad ante la difamación. Tal y como lo consagra el artículo 12 d en la (DDH), Declaración de los Derechos Humanos, todos tienen derecho a la intimidad, Aspecto importante de este derecho es que toda persona tiene derecho a la Protección de sus Datos Personales. En Internet, el derecho a la protección de Datos personales incluye; Protección de datos personales, Obligaciones de los colectores de datos, Normas mínimas sobre el uso de datos personales y Monitorización de la protección de datos.

En términos de Internet es muy amplio el espectro sobre los derechos, esto significa que toda persona tiene libertad de usar internet, esto significa que niños y niñas y personas con alguna

⁴ Ten Punchy Principles; ([http:// internetrightsandprinciples.org/site/campaign](http://internetrightsandprinciples.org/site/campaign)), un compendio de diez principios y valores clave subyacentes en la Carta.

⁵ UNESCO, a principios de 2013 ([https://www.unesco-ci.org/cmscore/events/51- rights-based-principles-and-internet-takingstock-and-moving-forward](https://www.unesco-ci.org/cmscore/events/51-rights-based-principles-and-internet-takingstock-and-moving-forward)),

discapacidad tienen los mismos derechos que establece la Carta y el Artículo 4 de la Convención de las Naciones Unidas sobre Derechos de las personas con Discapacidad (CDPD), disponibilidad y fácil acceso a Internet, libertad de usar internet y a su vez deben estar protegidos de los peligros asociados con internet, el equilibrio de los derechos digitales y la ciberseguridad estará asociado con el uso o abuso de la internet y dependerá de las capacidades de los usuarios en primer plano, el Estado debe respetar los derechos y las responsabilidades que a cada quien corresponda y proporcionará la orientación apropiada para una mejor evolución de las facultades que los individuos desarrollen en el uso y disfrute de la nuevas tecnologías de la información.

En resumen, la carta, explica las normatividades universales de DDHH en un contexto actual, el ciberespacio, insiste en dar debida relevancia a los derechos que deben observarse en el entorno on-line y off-line, congruente con la definición en el derecho internacional de gran espectro social, económico, político, civil y cultural.

El Derecho a la Protección de Datos Personales de manera expresa como principio de máxima publicidad es reconocido en México en la reforma que se efectuó en julio del 2007 al artículo 6to constitucional (CPEUM)⁶, estableciendo como condición el principio vigente de acceso a la información, siempre que este no atente contra el derecho fundamental de privacidad y la protección de datos personales. Posteriormente el 1ero de junio del 2009, se reconoce de manera textual el derecho de protección de datos personales en la reforma constitucional del artículo 16, incorporando un segundo párrafo, que establece; “ toda persona tiene derecho a la protección de sus datos personales, al acceso, su rectificación, cancelación y oposición”, en este mismo año se dio la modificación del artículo 73, que faculta al Congreso de la Unión en materia de protección de datos personales en posesión de particulares ⁷, por consiguiente en el 2010 se publica en el DOF (diario oficial de la federación) la Ley de Protección de datos personales en Posesión de Particulares (LFPDPPP) y con ello se dan importantes reformas y armonizaciones con leyes locales y federales en el contexto de la aplicación para el derecho de la protección de datos personales.

En este contexto la reforma constitucional en materia de Derechos Humanos en México , el 10 de junio del 2011 y publicada en el Diario oficial de la Federación (DOF), la cual representa un gran avance jurídico importante para optimizar el ejercicio y goce de los derechos humanos, en sus principales cambios la reforma incorpora todos los derechos humanos de los tratados internacionales como derechos constitucionales, surgiendo como figuras jurídicas en esta reforma del 2011, y que pareciera que aún hoy en día son poco conocidas para algunos o muchos, son; el principio pro persona, principio de interpretación conforme, control de convencionalidad y bloque de constitucionalidad, modificando la forma de proteger los derechos humanos de todas las personas (artículos que la reforma modificó fueron ; 10, 3º, 11. 15, 18,29,33,89, 97,102 apartado B y 105), atendiendo a los derechos fundamentales a los principios de universalidad, interdependencia, indivisibilidad y progresividad. En la plena aplicación para proteger los datos personales en el 2009, y con la reforma del artículo 6to. Constitucional efectuada el 07 de febrero del 2014 se le otorga al Congreso de la Unión la facultad de expedir leyes generales reglamentarias en materia de; acceso a la información pública, protección de datos personales y archivos; con lo cual, en mayo de 2015 se publicó la Ley General de Transparencia y Acceso a la Información Pública (LGTAP), dando entrada al estudio y puesta en práctica en enero del 2017 la Ley General de Protección de Datos personales en Posesión de Sujetos Obligados (LGPDPPSO) y en ejercicio de las facultades otorgadas al Congreso de la Unión en junio del 2018 entra en vigor la Ley General de Archivos (LGA).

Simultáneamente a la creación de leyes locales y federales, de reformas y modificaciones a la normativa continuamos la vida en un ecosistema hiperconectados en donde la especie humana experimenta un cambio sustancial no solo en la comunicación digital, sino que presenta un cambio en el cerebro, en los sentidos por la codependencia de las TICs, aunque al mismo tiempo nos desconecta para ver la realidad de manera directa. Fue Marshall McLuhan (1964) la idea de Aldea Global, sus palabras sobre la difusión masiva y la sociedad de la información, de la que trata en su obra “La galaxia Gutenberg” (1962), que inmortaliza su frase “el medio es el mensaje” a finales de

⁶ Decreto por el que se reforma el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos publicada en el Diario Oficial de la Federación el 20 de julio de 2007.

⁷ Decreto por el que se reforma la fracción XXIX-O del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos publicada en el Diario Oficial de la Federación el 30 de abril de 2009.

los 70s, le haría pasar como visionario de la internet ⁸, los desafíos de la aldea global, la sobrecarga de información y la pérdida de privacidad son preocupaciones en nuestra aldea global, debemos comprender todas sus implicaciones, aprovechar al máximo las oportunidades que nos ofrece y así poder enfrentar los desafíos con seguridad.

Y tratándose de ciberseguridad y confianza en el uso de las redes sociales, plataforma digitales, internet, etc. el aislamiento por la pandemia de covid19, incremento exponencialmente el uso y por la tanto el abuso, el acoso digital, el robo de identidad a través de dispositivos inteligentes digitales y los delitos cibernéticos en internet se incrementaron, el abuso en redes sociales se disparó y se presentaron casos en los que hubo padecimientos de ansiedad, de depresión si no estaban conectados o como dicen coloquialmente “enchufados”, el uso desmedido o sin control de las redes puede provocar un aislamiento del mundo real, de las personas físicamente, convirtiendo nuestro ambiente en un entorno vacío nosotros, aunque saturado de mundos interconectados virtualmente lejanos, pasamos de un estado de hiperconectividad digital a un estado de desconexión de las personas que tenemos enfrente.

No hay duda que la ciencia y la tecnología digital son una gran aportación en el desarrollo de alternativas innovadoras del ser humano que con la capacidad suficiente para no convertirse en codependiente de la internet sigue su instinto creador e innovador estimulando sus sentidos y manteniéndose cercano a la persona que tiene enfrente.

La nueva generación de los derechos digitales, permiten digitalizar miles de millones de datos en fracción de minutos en tiempo real que se transfieren a cualquier ordenador en cualquier parte del mundo, un nuevo algoritmo tecnológico en la sociedad del conocimiento, de la información, comunicación, almacenamiento y procesamiento a gran velocidad de la información que conduce a un estudio profundo en la reorganización de nuevos modelos en el quehacer cotidiano, económico, social, laboral, político y democrático.

Estamos frente a una nueva revolución tecnológica 5.0 (término acuñado en 2021 por la Comisión europea) la cual pretende potenciar en espacios inteligentes basados en internet of Things y computación cognitiva, esto trata de poner la inteligencia artificial al servicio de las personas, uniendo máquinas y humanos que generen un impacto positivo en la sociedad ⁹. La transformación digital pasó a ser una necesidad apremiante, se acelera y no hay vuelta atrás, llegó para asentarse en los hogares, no solo en las empresas, la educación y los gobiernos, a estas fechas del 2023 podemos estar entablando la movilidad mundial de una 6.0 revolución industrial.

Estas revoluciones industriales tratan acerca de un recurso tecnológico para imitar las capacidades intelectuales humanas, así lo afirma el Dr. González San Juan, que la inteligencia artificial (IA) es un software que por medio de los algoritmos pretende sustituir la capacidad intelectual humano¹⁰, en cuanto a la posverdad, La RAE la define como una “distorsión deliberada de una realidad, que manipula creencias y emociones con el fin de influir en la opinión pública y en actitudes sociales” por lo que se puede intuir un conflicto o doble papel de la Inteligencia Artificial, ya que por un lado el término posverdad engloba a las fake news, y a la vez las fake news son el combustible que alimenta la posverdad.

Los derechos digitales y la ciberseguridad también son del interés de manera simultánea en el combate a las fake news, a la desinformación, rumores o mentiras en las redes sociales, combustible de la posverdad. La inteligencia artificial al pretender la dualidad de funciones, crea una confusión al entrar al terreno de la emoción humana, lo que hoy se conoce como “ansiedad por la inteligencia artificial” conocida como “AI-Anxiety”, que se expresa en un tipo de estrés y ansiedad laboral por el miedo de ser remplazados (AI) y perder en poco tiempo el trabajo.

En el aspecto laboral existen datos que reflejan que se remplazarán 85 millones de puestos de trabajo por el año 2025 por la aplicación de la inteligencia artificial, la OCDE calcula que hasta el 46 % de los empleos corren riesgo de automatización y se crearán unos 97 millones de nuevos puestos de trabajo¹¹ en más de 26 países con parámetros de esas herramientas, ejemplo concreto los servicios bancarios que presionan a los clientes a que instalen aplicaciones- como la banca móvil, en

⁸ La aldea global de Mc Luhan; Una visión profética del mundo conectado, septiembre 13 de 2023

⁹ Revolución Industrial 5.0, advancedfactories.com/industria_5.0_caracteristicas/fira_barcelona

¹⁰ El papel de la inteligencia artificial en la era de la posverdad, Dr. José Luis Gonzáles San Juan, (González, 2022: pág. 595). Fake news combustible que afecta la posverdad (navarro, 2022.pág148)

¹¹ RRHHDigital, Foro económico mundial, Javi Pastor, director de Big Data Conversión.

<https://www.rrhhdigital.com>

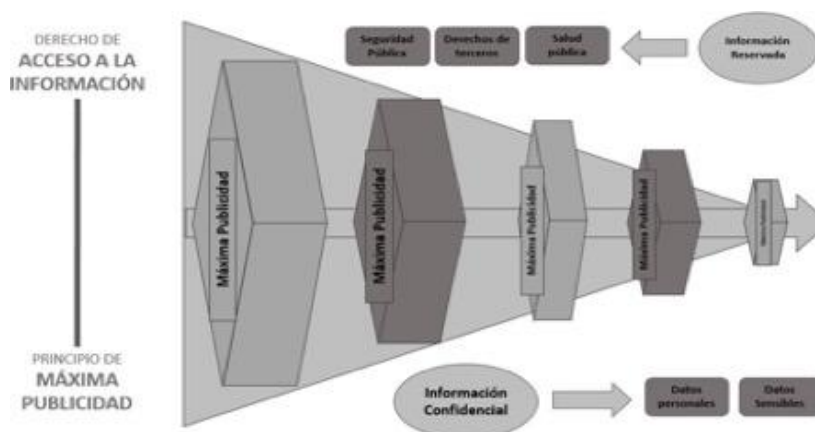
sus teléfonos celulares y que realicen por ellos mismos todas sus operaciones, mismas que hacían los empleados bancarios, esto también da oportunidad a que los dispositivos de ciberseguridad sean mas efectivos y eviten el robo de identidad, fraudes, extorsiones etc. resultado mas inteligencia artificial , mas tecnología, mas redes sociales, derivan en un nuevo factor de riesgo psicosocial que también ya fue creada una NOM-035-STPS-2018 para tratar el nuevo factor de riesgo dando lugar al concepto del “ tecnoestrés” o estrés derivado del efecto de la incertidumbre en el uso de las llamadas nuevas tecnologías de la información y ña comunicación.

Y podemos tomar como respuesta que la relación entre la Inteligencia artificial, la tecnología, las redes sociales, la internet es desafiante, por un lado, podemos argumentar que son el fruto del ingenio humano que contribuye al bienestar, al desarrollo, a progreso y realización de todo ser humano, facilitándole desde la tarea mas sencilla hasta la mas difícil, peligrosas e imposibles de realizar, incrementado su conocimiento, o si por el contrario los amenaza la perdida de control humano sobre las decisiones y acciones de los sistemas de inteligencia artificial, especialmente si adquirieran autonomía, o autoconciencia, esta muy lejano aún la sustitución o desplazamiento de los humanos por los ecosistemas del entorno digital.

Con todo lo anterior surge la imperiosa necesidad de reconocer que debemos aplicar los derechos digitales y por ende poner en practica la normatividad en ciberseguridad confiable de las personas ante el uso de las TICs y la interconectividad digital mediante la internet, big data, la nube, machine learnig e inteligencia artificial que permita la garantía de la protección personalidad y la dignidad humana, teniendo presente que en nuestro país la regularización de la protección de datos personales en el sector privado se efectúa a través de la (LFPDPPP) Ley Federal de protección de datos personales de particulares, mientras que, en el sector público se cuenta con la (LGPDPSSO) Ley General de Protección de datos personales en posesión de los sujetos obligados, que tienen como objetivo garantizar el derecho que tiene toda persona a la protección de sus datos personales. Dentro de todas estas tendencias se producirán importantes cambios no solo en las tecnologías de la información en cuanto a las habilidades, requiriéndose capacidades nuevas como pueden ser del pensamiento crítico y el análisis y la resolución de problemas, la autogestión, el aprendizaje activo, la tolerancia al estrés la accesibilidad a personas con capacidades diferentes la resiliencia y la flexibilidad, estimando que se requerirá de una formación no solo académica, o para nuevos puestos de trabajo sino para la observancia y cumplimiento de la normatividad vigente que regule todos los derechos digitales y que sea una realidad confiable la ciberseguridad en la portabilidad, procesamiento, manejo de los datos personales, la privacidad la integridad de las personas y la protección a la dignidad humana.

En este sentido los seres humanos tiene adherida a su dignidad un bien que debe protegerse en todo momento, conforme evoluciona la sociedad, simultáneamente evolucionan los derechos para atender en tiempo y forma las necesidades políticas, económicas y sociales, es así que podemos transitar armónicamente en el ambiente digital, poniendo en práctica los derechos digitales, atendiendo que toda la información que fluye en el ciberespacio es operada por seres humanos, resaltando que aún y cuando la información es automatizada y existen manuales de operaciones, e instrucciones etc, que son creadas por humanos y, por ende se debe establecer los limites en el tratamiento de los datos personales en el entorno digital, ya que se multiplica factorial las personas que se interconectan e intercambian información de todo tipo, para lograr sus objetivos y llevar a cabo actividades profesionales, académicas, económicas, políticas y sociales, en la actualidad casi todos o todos contamos con un dispositivo inteligente digital, con ese dispositivo estamos conectados al mundo de la internet, e intercambiamos información, mensajes, videos, fotos, de todo tipo de contenido digital, por lo que los derechos digitales son derechos que deben proteger a las personas en ecosistema o entorno digital, tener derecho a la privacidad, derecho a la intimidad, derecho a la imagen, derecho a la libertad de expresión y derecho al Internet, considerando la vigencia en el principio de máxima publicidad que es fundamental para el ejercicio del derecho de acceso a la información (DAI), sin dejar de lado que atiende a la naturaleza de la información, se debe revisar que no se actualice el supuesto de clasificación y en su caso realizar la prueba de daño correspondiente, así garantizar la procedencia de limitar el Derecho de Acceso a la Información, cuando se comprometa la salud y la seguridad como información confidencial cuando se refiera a información o datos personales, tales como aprecia en la figura 1.

Figura 1



La protección de datos personales se reconoce como un derecho también en el entorno digital, considerando que los datos personales consisten en cualquier información que identifica o hace identificable a una persona; por tanto, este derecho es el medio para garantizar la protección de la intimidad y privacidad de los individuos al otorgar el poder de uso, disposición y control de sus datos¹². En este sentido, la confidencialidad es una cualidad que consiste en decir, hacer o intercambiar información en un marco de confianza, a fin de que esta solo sea accesible a personas autorizadas, obligando a no revelar la información que se obtiene en ese marco de confianza; por tanto, dicha cualidad incluye la intimidad como el núcleo central de protección, la privacidad como el derecho de excluirse de los demás, a través del derecho de protección de los datos personales, tal y como se aprecia en la figura 2.



Figura 2

En el entorno digital, el Derecho de Protección de Datos Personales (DPDP) obedece también a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; así como, a los deberes de confidencialidad, integridad, disponibilidad y seguridad previstos en la LFPDPPP y la LGPDPPSO; el deber de confidencialidad consiste en que la información no se puede poner a disposición, ni ser revelada a individuos, entidades o procesos no autorizados.

No obstante, en el ámbito del proceso de clasificación de la información, es procedente considerar la confidencialidad como un principio, ya que en el proceso de análisis para determinar si se actualiza algún supuesto de clasificación como información reservada o confidencial, se deben cumplir reglas mínimas para proteger los bienes jurídicos superiores como la salud y seguridad pública o el derecho de terceros, considerando que la información confidencial es aquella que se refiere a información privada y datos personales; sin embargo, no todos los datos personales son confidenciales atendiendo a las obligaciones de transparencia y el interés público de conocer cierta información, destacando que los organismos garantes en el ámbito de sus atribuciones de verificación, investigación y sanción, tienen la potestad de determinar la aplicación de la prueba de

¹² Dr. Javier Martínez Cruz. Director General de JMC Datapretium, Consultores Asociados.

interés público para permitir el acceso a la información que por su naturaleza tiene el carácter de confidencial. Es posible, plantear el principio de máxima confidencialidad como un parámetro para permitir la apertura de información confidencial, como se muestra en la figura 3.

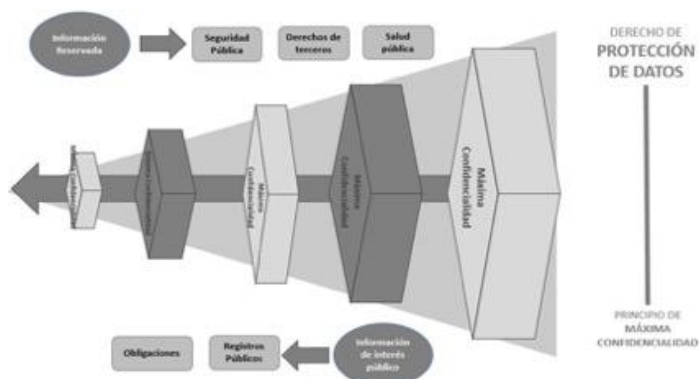


Figura 3

El reto que implica atender el DAP y el DPDP como derechos digitales, nos compromete a lograr alcanzar el equilibrio de los derechos fundamentales de DAP y DPDP en el ecosistema o ambiente digital (ciberespacio), considerando los criterios principales para determinar los derechos constitucionales fundamentales; la persona humana y el reconocimiento expreso, el primero contiene una base material y el segundo una formal; como se hace en el espacio físico a partir de un ejercicio de ponderación o balanceo de derechos considerando las teorías de Robert Alexy¹³ “cuando mayor es el grado de la no satisfacción o de afectación de uno de los principios, tanto mayor debe ser la importancia de a satisfacción del otro” y Ronald Dworkin¹⁴, con la finalidad de contar con parámetros medibles que sienten las bases para que ambos derechos coexistan y se aplique el derecho que más favorezca a la persona.

Se identifica de igual manera en entorno digital, la interacción del DAI y el DPDP bajo los Principios de Máxima Publicidad en el caso del DAI y de Máxima Confidencialidad en lo que corresponde al DPDP, considerando que *la prueba de daño* se aplica cuando se actualiza algún supuesto de clasificación como información reservada y *la prueba de interés público* se aplica para permitir la apertura de información confidencial, como se aprecia en la figura 4.

¹³ Alexy, Robert. Derechos sociales y ponderación. Madrid, España. 2010: Editorial Fontamara.

¹⁴ Dworkin, Ronald. Una cuestión de principios. Buenos Aires, Argentina, 2017: editorial Siglo veintiuno editores.

Figura 4



La correcta ponderación o balanceo de los (DD.HH.) Derechos humanos, en el ciberespacio, nos obliga a atender que el principio de proporcionalidad es la técnica jurídica y argumentativa encaminada a determinar si un derecho fundamental se ajusta o no a la Constitución, el cual, se integra por los sub-principios de idoneidad, necesidad y proporcionalidad en sentido estricto, cuya aplicación se refleja en el ejercicio de ponderación entendido como el método que tiene como objetivo resolver una colisión de derechos, considerando que no debe realizarse desde un enfoque rígido de anteponer un derecho sobre otro; es decir, se debe aplicar el derecho que más favorezca a la persona, de manera que los derechos coexistan y se determine su ejercicio a través del medio que resulte menos lesivo para satisfacer, en el caso del (DAI), Derecho acceso a la información, el interés público, o bien, en lo que corresponde al (DPDP) Derecho a Protección de Datos Personales, la confidencialidad de la información¹⁵.

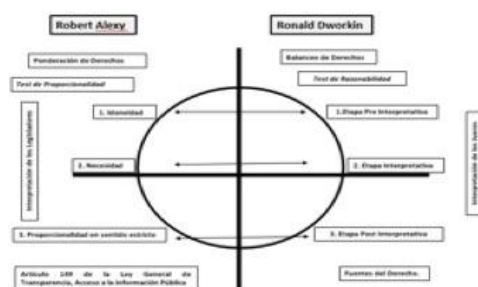
En el mismo entorno digital; se puede aplicar la teoría de Ronald Dworkin ¹⁶, bajo la perspectiva del juzgador a cargo del Poder Judicial, destacando que la reforma constitucional de 2011 al artículo primero, trajo consigo la expedición de la actual Ley de Amparo que brinda los elementos necesarios para garantizar los derechos fundamentales de los mexicanos, tal es el caso del (DAI), Derecho de Acceso a la Información y el (DPDP), Derecho a Protección de Datos Personales. Además, es importante considerar que la jurisprudencia como una fuente formal del derecho se crea por reiteración de criterios, contradicción de tesis y por sustitución, la cual consiste en la aplicación e interpretación de las leyes, cuya aplicación resulta obligatoria.

En complemento a lo anterior, el diagrama que se aprecia a continuación refleja las posturas de Alexy y Dworkin; por un lado, Alexy plantea una ponderación de derechos bajo la interpretación de los legisladores al aplicar el test de proporcionalidad, al aplicar una prueba de interés público con base en los elementos de idoneidad, necesidad y proporcionalidad. Por otro lado, Dworkin plantea un balanceo de derechos bajo la interpretación de los jueces, al aplicar el test de razonabilidad, atendiendo a las fuentes del derecho y las etapas de interpretación.

¹⁵ Alexy, Robert. Derechos sociales y ponderación. Madrid, España. 2010: Editorial Fontamara

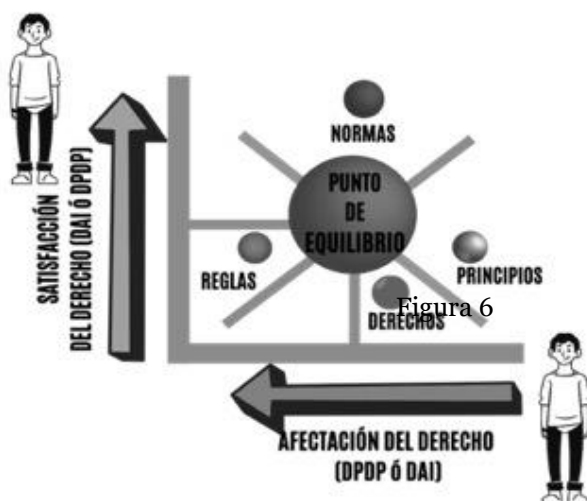
¹⁶ Dworkin, Ronald. Una cuestión de principios. Buenos Aires, Argentina, 2017: editorial Siglo veintiuno editores

Figura 5



Ahora bien, para contar con una metodología efectiva que sirva en el ciberespacio, y que permita determinar parámetros medibles en la ponderación de derechos, como se aprecia en la Figura 6.

Figura 6



En la imagen se aprecia la convergencia de normas, reglas, derechos y principios en el entorno digital; el círculo representa el punto de equilibrio; cabe destacar, que el objetivo de esta gráfica es visualizar que la ponderación se realiza desde un enfoque flexible, a fin de maximizar el beneficio de un derecho, minimizando la afectación del otro, aplicando siempre el derecho que más favorezca a la persona con la implementación de un medio alternativo que resulte menos lesivo para satisfacer el interés público y/o la confidencialidad de la información.

Finalmente, es importante precisar que la ponderación en el ciberespacio, no debe realizarse desde un enfoque rígido de anteponer un derecho sobre otro; es decir, se debe aplicar el derecho que más favorezca a la persona, de manera que los derechos coexistan y se determine su ejercicio a través del medio que resulte menos lesivo; por ende, la importancia de aplicar la ponderación con la premisa de analizar caso por caso, mediante la implementación de acciones que permitan garantizar en todo momento el respeto a los (DD.HH.), derechos humanos. En términos de la ley de la ponderación, cuanto mayor es el grado de satisfacción o afectación de uno de los derechos, tanto mayor debe ser la importancia de satisfacer el otro, a través de la aplicación de la fórmula del peso, precisando que

estos tienden a unirse en un punto que representa el punto de equilibrio ante la colisión de los derechos fundamentales.

Para Dworkin¹⁷ el tema y la problemática de casos difíciles, estos encuentran una solución correcta, ante algún caso extraordinario en el ciberespacio es posible que se pueda aplicar ninguna norma, sin embargo esto no debe descalificar la posibilidad de aplicar para el mismo caso un principio, una interpretación, reinterpretación o extensión de la ley o el precedente existente, en el caso de la ciberseguridad entendida esta como la puesta en práctica de la protección de equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales, los primeros en tomar acciones responsables proteger los datos de los usuarios que a través de la internet se interconectan con las organizaciones para obtener un bien o servicio, el primer contacto tiene responsabilidad proteger los datos del usuario para mantener la confianza.

En Resumen, los derechos digitales son una extensión de los derechos recogidos en la Declaración Universal de los Derechos Humanos (DUDH) de la Organización de la Naciones Unidas (ONU) cumpliendo con el objetivo primordial de garantizar el acceso a Internet evitando la denominada **brecha digital**¹⁸, y un adecuado uso de la red como bien común que pertenece a toda la humanidad. La falta de un consenso internacional sobre la resolución de los derechos humanos en Internet, ha dejado abierta la puerta para que cada país desarrolle su propia carta de derechos digitales.

La Unión Europea ha estado proponiendo y marco común, relativo al derecho a la protección de los datos personales. Por ejemplo, el Reglamento General de Protección de Datos (GDPR), que entro en vigor en el 2018 y que obliga a los Estados miembros a preservar los datos personales de los ciudadanos, como el permitir la libre circulación de datos, por el contrario, en Estados Unidos, no existe una Ley Federal de protección de datos y por ende cada Estado aplica su propia regulación. Hoy en día mas de 120 países disponen de alguna normatividad con fuerza de Ley que protege los datos personales y el acceso a la información en Internet. El pasado año 2022 la comisión europea realizó una declaración de protección de los derechos de sus ciudadanos en el mundo digital en ella se cubre los derechos de todos los ciudadanos europeos. Existen líneas generales para que cada países desarrolle su propia Carta de Derechos Digitales como por ejemplo; Establecer una red de internet gratuita, para cumplir con el acceso universal e igualitario, o cuando los derechos humanos básicos se ven amenazados en internet por algún gobierno que bloquea los sitios web o redes sociales, lo cual es una violación del derecho de comunicación y libre asociación, aquí el legislador en la carta de derechos digitales debe dejar plasmada la garantía de la libertad de expresión, información y comunicación.

El derecho a la intimidad cada vez se ve mas amenazado en internet por el robo de identidad, credenciales, apropiación de datos personales, hackeo de whatsapp, que medidas tomar en cuanto a la privacidad y protección de datos, el ciudadano debe tener el control sobre quién almacena sus datos personales. Existen países en donde esta prohibido enviar mensajes cifrados, esto es importante para realizar transacciones fiables y seguras en internet, el derecho al anonimato y el cifrado de comunicaciones no debe verse amenazado. Hablar de propiedad intelectual se debe garantizar el reconocimiento de los autores sobre sus obras, académicas, artísticas, literarios etc., la protección del menos a un acceso seguro sin infringir los derechos de los menores y el derecho al olvido, derecho a que la información privada de una persona se elimine de las búsquedas de internet, bases de datos y directorios. En la Unión Europea se le reconoce en el GDPR (reglamento general de protección de datos) como “derecho al borrado” involucrando así a países cercanos a México como Argentina, Estados Unidos.

“La tecnología no es nada. Lo importante es que tengas fe en la gente, que sean básicamente buenas e inteligentes, y si les das herramientas, harán cosas maravillosas con ellas”. Steve Jobs, cofundador y presidente ejecutivo de Apple Inc.

Por ende, debemos tener una noción de cómo vamos actual si se vulneran los derechos digitales. La seguridad cibernética (ciberseguridad) es fundamental en la sociedad actual en donde casi todas las actividades las realizan en el ecosistema digital, la seguridad cibernética detecta; vulnerabilidades, fisuras de seguridad y establece las medidas de corrección y reparación pertinentes contra accesos no autorizados a los centros de datos y otros sistemas informáticos, en

¹⁷ Hart y Dwoeki casos difíciles, casos perplejos (art. Johann benfeld), estudios histórico-jurídicos, ISSSN0716-5455; <http://dx.doi.org/10.4067/S0716-5455201000015>

¹⁸ La protección de los datos en la era digital; iberola.com/innovación/que_son_derechos_digitales_

conclusión la ciberseguridad es de suma importancia en el mundo digital, ya que esta conformado por herramientas destinadas a proteger los sistemas desde un ordenador a un servidor pasando por cualquier tipo de dispositivo inteligente digital conectado, protegiendo las redes que los unen.

Citas y referencias

- ¹ Dra- Alma Rosa Armendáriz Sigala, Catedrática del Tec NM campus Chihuahua.
- ² Prensky, Marc, (December 2001). Nativos Digitales, Inmigrantes Digitales. En On the Horizon (MCB University Press, Vol. 9 No. 6).
- ³ Franklin, Marianne, Bodle, Robert, Hawtin, Dixie. (Enero 2015). Carta de los derechos humanos y principios para Internet. 1ª edición: Internet Rights and Principles Dynamic Coalition UN Internet Governance Forum. (<http://internetrightsandprinciples.org/wpcharter>).
- ⁴ Franklin, Marianne, Bodle, Robert, Hawtin, Dixie. (Enero 2015). 10 Derechos y Principios de Internet; ([http:// internetrightsandprinciples.org/site/campaign](http://internetrightsandprinciples.org/site/campaign)).
- ⁵ UNESCO, (2013), ([https://www.unesco-ci.org/cmscore/events/51- rights-based-principles-and-internet-taking-stock-and-moving-forward](https://www.unesco-ci.org/cmscore/events/51-rights-based-principles-and-internet-taking-stock-and-moving-forward)).
- ⁶ Decreto por el que se reforma el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos publicada en el Diario Oficial de la Federación el 20 de julio de 2007.
- ⁷ Decreto por el que se reforma la fracción XXIX-O del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos publicada en el Diario Oficial de la Federación el 30 de abril del 2009.
- ⁸ La aldea global de Mc Luhan; Una visión profética del mundo conectado, septiembre 13 de 2023
- ⁹ RevoluciónIndustrial5.0, advancedfactories.com/industria_5.0_caracteristicas/fira_barcelona
- ¹⁰ González San Juan, José Luis, (2022). El papel de la inteligencia artificial en la era de la posverdad. (González, 2022: pág. 595). Fake news combustible que afecta la posverdad (navarro,2022. pág148).
- ¹¹ Javi Pastor, director de Big Data Conversión. RRHHDigital, Foro económico mundial, <https://www.rrhhdigital.com>
- ¹² Martínez Cruz, Javier. Director General de JMC Datapretium, Consultores Asociados.
- ¹³ Alexy, Robert, (2010). Derechos sociales y ponderación. Madrid España: Editorial Fontamara.
- ¹⁴ Dworkin, Ronald, (2017). Una cuestión de principios. Buenos Aires, Argentina: Editorial Siglo veintiuno editores.
- ¹⁵ Alexy, Robert, (2010). Derechos sociales y ponderación. Madrid, España: Editorial Fontamara.
- ¹⁶ Dworkin, Ronald, (2017). Una cuestión de principios. Buenos Aires, Argentina: editorial Siglo veintiuno editores.
- ¹⁷ Hart y Dwoeki, Casos difíciles, casos perplejos (art. Johann benfeld), estudios histórico-jurídicos, ISSN0716-5455; <http://dx.doi.org/10.4067/S0716-5455201000015>.
- ¹⁸ La protección de los datos en la era digital; [berola.com/inn ovación/que_son_derechos_digitales](https://berola.com/innovación/que_son_derechos_digitales).

Frase celebre

"El único sistema verdaderamente seguro es el que está apagado, fundido en un bloque de hormigón y sellado en una habitación forrada de plomo con guardias armados." - Bruce Schneier /.

"La ciberseguridad no es sólo tecnología, sino también personas." - Kevin Mitnick.

Chihuahua, Chih., enero 15 de 2025.