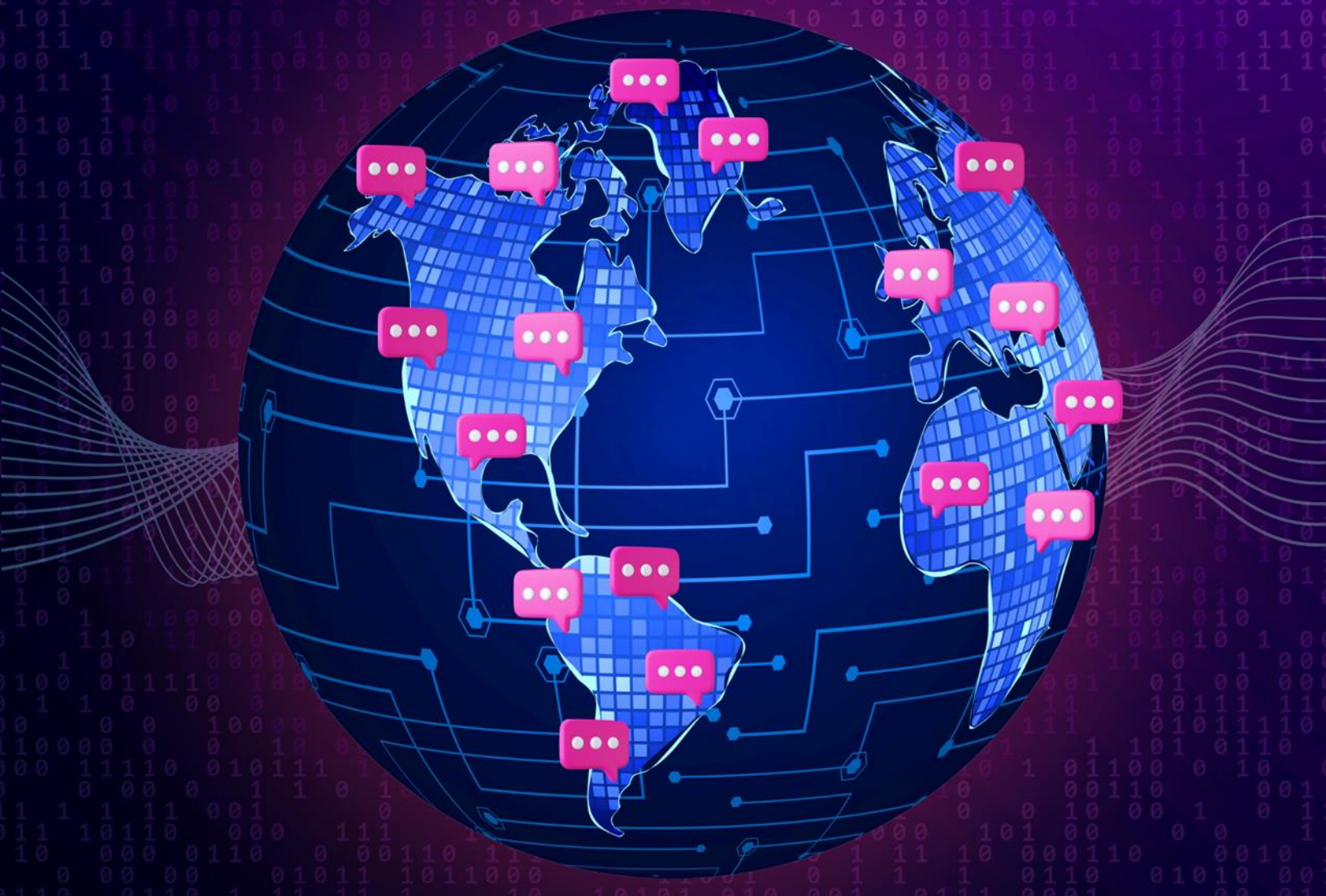
Sistema Nacional de Transparencia
Acceso a la Información Pública y Protección de Datos Personales

Comisión de Vinculación, Promoción, Difusión y Comunicación Social

Comisión de Protección de Datos Personales

IDENTIDAD Y CIUDADANÍA DIGITAL



Av. Insurgentes, Sur No. 3211, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Ciudad de México. C.P. 04530.

Primera edición octubre 2023

INTEGRANTES DEL SNT QUE PARTICIPARON

Dra. Norma Julieta del Río Venegas
Coordinadora de la Comisión Permanente de Vinculación, Promoción, Difusión y Comunicación Social con el SNT y Comisionada del Instituto Nacional de Transparencia, Acceso a la Información pública y Protección de Datos Personales (INAI)

Dr. Luis Gustavo Parra Noriega
Coordinador de la Comisión de Vinculación, Promoción, Difusión y Comunicación Social del SNT y Comisionado del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM)

Mtro. Adrián Alcalá Méndez
Comisionado del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI)

Dra. Josefina Román Vergara
Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

Mtra. Amelia Lucia Martínez Portillo
Comisionada Presidenta del Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública (ICHITAIP)

L.A. Evelia Elizabeth Monribot Domínguez
Comisionada del Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo (ITAIH)

Mtro. Francisco Javier Diez de Urdanivia del Valle
Comisionado del Instituto Coahuilense de Acceso a la Información Pública (ICAI)

Dr. Julio César Bonilla Gutiérrez
Comisionado Ciudadano del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX)

Mtra. Laura Lizett Enríquez Rodríguez
Comisionada Ciudadana del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX)

Dra. María de los Ángeles Guzmán García
Comisionada de La Comisión De Transparencia y Acceso a la Información del Estado de Nuevo León (INFONL)

Mtra. Naldy Patricia Rodríguez Lagunes
Comisionada del Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales (IVAI)

Dr. Salvador Romero Espinosa
Comisionado del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI)

Mtra. Xitlali Gómez Terán
Comisionada del Instituto Morelense de Información Pública y Estadística (IMIPE)

Lic. Xóchitl Elizabeth Méndez Sánchez
Comisionada del Órgano Garante de Acceso a la Información Pública, Transparencia y Protección de Datos Personales y Buen Gobierno del Estado de Oaxaca (OGAIPO)

Mtra. Yolidabey Alvarado de la Cruz
Comisionada del Instituto Tabasqueño de Transparencia y Acceso a la Información Pública

ESPECIALISTAS INVITADOS

Mtra. Adriana Yadira Cárdenas Tagle
Directora General de Transparencia, Acceso a la Información Pública y Gobierno Abierto
Coordinadora Editorial del Documento Orientador

Dra. Anahiby Anyel Becerril Gil
Vicepresidenta de la Academia Mexicana de Ciberseguridad y Derecho Digital

Dr. Carlos Languendik Muñoz
Presidente de Abrazando Vidas y Construyendo Sueños, Asociación Civil

Dr. Erik Alejandro Cancino Torres
Catedrático de la Facultad de Derecho y Ciencias Sociales Victoria de la Universidad Autónoma de Tamaulipas

Dr. Guillermo Antonio Tenorio Cueto
Director de la Escuela de Gobierno y Economía de la Universidad Panamericana

Mtro. Héctor Guzmán Rodríguez
Director de la Red de Protección de Datos Personales y Privacidad en Firma BGBG

Dr. Iván Díaz González
Socio de la Academia Mexicana de Derecho Informático

Mtro. Javier Brown César
Especialista en Ética Pública
Asesor en el Senado de la República

Documento Orientador de Identidad y Ciudadanía Digital

Introducción 6

I. FUNDAMENTOS DE LA IDENTIDAD DIGITAL 9

Definición de identidad digital 9

Impactos del reconocimiento de la identidad digital en la primera infancia hacia una ciudadanía digital 11

Análisis sobre la construcción y gestión de la identidad digital 15

Importancia de la protección de datos personales (vulneraciones) 18

Riesgos asociados con la identidad digital, como violencia digital, algunos tipos y ejemplos 20

Consejos para proteger la identidad digital y mantener la privacidad en línea 23

Huella digital 28

¿Qué es la huella digital y cómo se genera? 30

Concienciación sobre la importancia de cuidar la huella digital y cómo afecta la reputación en línea 33

II. CIUDADANÍA DIGITAL RESPONSABLE 36

Definición de ciudadanía digital 36

Ciudadanía e identidad digital: protegiendo la privacidad en el mundo virtual 40

Ciudadanía digital, derechos y responsabilidades 43

Enumeración de los aspectos clave de la ciudadanía digital, como el respeto, la ética y la participación cívica en línea 46

Fomento de los beneficios de la gobernanza digital 50

Descripción de ejemplos de comportamientos positivos y negativos en línea 53

Consejos para evaluar la calidad de la información en línea y evitar la difusión de noticias falsas 56

Discriminación tecnológica en el mundo de la ciudadanía digital, una contradicción lógica en la sociedad de la información y del conocimiento 67

Ciudadanía digital y protección de datos desde una perspectiva de la academia 71

III. COMPORTAMIENTO ÉTICO EN LOS ENTORNOS DIGITALES 74

Contexto de responsabilidad en línea 74

¿Cuáles son los principios éticos que deben regir el actuar en los entornos digitales? 77

¿Qué es la inteligencia artificial? 81

Comportamiento ético en el uso de la inteligencia artificial 84

Explicación de la importancia de desarrollar habilidades de alfabetización mediática y digital 87

Concienciación sobre la importancia de ser ciudadanos digitales responsables a nivel global 93

IV. DERECHOS DIGITALES 96

Derechos fundamentales de las personas en el entorno digital 96

Enumeración de los derechos fundamentales de las personas en el entorno digital, como la libertad de expresión y la privacidad 101

Descripción de las responsabilidades de las personas en el entorno digital, como el respeto a los demás y la protección de la seguridad en línea 106

Desinformación y ciberseguridad 108

Descripción de cómo contribuir positivamente a la sociedad en línea y promover la igualdad y la inclusión 112

¿Cómo considera que debe ser este engranaje de comunicación entre autoridades y sociedad civil para que la información llegue a la ciudadanía digital? 115

Introducción

Luis Gustavo Parra Noriega

El Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) desde su consolidación como instancia de coordinación y deliberación encargada de garantizar el ejercicio y respeto de los derechos de acceso a la información y de protección de datos personales, se ha encargado de proveer y fomentar una educación y promoción de estos dos derechos en todo el territorio nacional.

A través de las Coordinaciones Nacionales se han realizado esfuerzos de socialización cuya importancia permea en los tejidos más sensibles de nuestra sociedad actual; en razón de ello es que la Comisión de Vinculación, Promoción, Difusión y Comunicación Social del SNT, a través de su plan de trabajo 2022-2023, propuso la realización de foros de difusión en torno a la importancia de la ciudadanía digital; cuya realización derivó en la necesidad de construir de manera conjunta un Documento Orientador que nos permita la generación de conocimiento colectivo con la ciudadanía a fin de que conozcan de manera más práctica, las implicaciones y retos de vivir en una sociedad digital, generar conciencia para estar informados y comprender los desafíos y las implicaciones que conlleva vivir en un entorno altamente conectado.

Es así que este documento pretende explorar aspectos clave que nos llevarán a construir conceptos de identidad y ciudadanía digital de la mano de personas expertas, en la búsqueda de destacar la importancia que se debe dar a la educación digital adecuada para que las personas puedan comprender y utilizar de manera responsable las tecnologías digitales.

Esto incluye el conocimiento sobre la privacidad en línea, la seguridad cibernética, el uso responsable de las redes sociales y la capacidad de discernir información confiable de la desinformación.

En una sociedad digital nuestros datos personales y privacidad están constantemente expuestos y es precisamente a través de ellos que va construyendo nuestra identidad digital, en ese sentido, es necesario advertir y conocer nuestros derechos digitales y a la privacidad, generar conciencia sobre la importancia de proteger nuestra información personal y aprender a usarla para nuestro beneficio.

Nuestros datos están tan expuestos y hay tanta información disponible en la Web, lo cual implica desarrollar habilidades de alfabetización mediática para poder evaluar críticamente la información, identificar noticias falsas y comprender de qué manera los medios digitales pueden influir en nuestras percepciones y opiniones.

En cuanto a la ciudadanía digital, teniendo a la vista el concepto de "sociedad líquida", el cual fue acuñado por el sociólogo Zygmunt Bauman para describir una sociedad caracterizada por la falta de estructuras sólidas y estables, podemos afirmar en este contexto que la ciudadanía digital se refiere a los derechos, responsabilidades y comportamientos de los individuos en el entorno digital.

Algunos desafíos que se presentan en una sociedad digital son los siguientes:

1. Ética en línea: Es fundamental concienciar sobre la ética en línea y fomentar comportamientos responsables y respetuosos en el entorno digital, teniendo en cuenta los impactos de la tecnología en el ser humano, incluso en estructuras o situaciones tan flexibles y variables en este tipo de sociedad.

2. Participación ciudadana: La ciudadanía digital implica no sólo consumir contenido en línea, sino también participar activamente en debates y asuntos cívicos y políticos. En una sociedad líquida, donde las estructuras tradicionales pueden ser menos estables, es importante fomentar la participación ciudadana en línea y el uso de la tecnología para promover el bien común.

3. Empoderamiento digital: La tecnología puede ser tanto una herramienta de empoderamiento como de opresión. Es esencial generar conciencia sobre cómo utilizar la tecnología para promover el cambio social positivo y abogar por la igualdad y la justicia para lograr una ciudadanía digital efectiva.

Es así que, desde este Documento Orientador se tiene como objetivo generar un insumo de consulta y difusión que permita generar conocimiento público útil respecto de la identidad y ciudadanía digital, ya que cada vez más aspectos de nuestras vidas se desarrollan en línea, desde la comunicación, búsqueda de información, exigencia de servicios públicos, la realización de trámites en línea, hasta las transacciones financieras, por lo que este documento analiza desde las definiciones, implicaciones en la primera infancia, huella digital, gobernanza y la construcción de ciudadanía digital.

I. FUNDAMENTOS DE LA IDENTIDAD DIGITAL

Definición de Identidad digital

Francisco Javier Diez de Urdanivia del Valle

Actualmente es casi imposible encontrar a una persona que no cuente con mínimo una cuenta dentro de las denominadas "redes sociales del ciberespacio", aunque pareciera redundante porque el término "redes sociales" ya prácticamente sólo se utiliza para hacer referencia a dichas plataformas de Internet. Esto implica nuevos retos y espacios de estudio inexplorados, o poco profundos en su esencia.

Uno de estos grandes retos y espacios poco explorados, que ha causado efectos más allá del ciberespacio, es el relacionado con la personalidad. Esta, por su naturaleza compleja que representa un gran espectro de conceptos de acuerdo a la visión científica desde la que se aborde, es un terreno fértil para la pluralidad de opiniones al respecto, que abren la puerta a visiones individuales más que esquemas sistematizados que busquen la profundidad en su conocimiento. Con esto en mente, hay que comprender que uno de los caminos para abordar los grandes retos, es el de diseccionarlos y analizar cada elemento en lo particular, es por ello que en el presente sólo es menester la idea de identidad y más concretamente la identidad digital de las personas.

Así como todos tenemos una identidad en el mundo material, por llamarle de algún modo al ámbito físico, todos tenemos ese atributo personal que nos dota de una identidad individual registrada y reconocida en el ciberespacio. En el mundo material, es sencillo reconocer ese registro institucional que identifica a una persona, puede ser ante una institución gubernamental o una religiosa, eso depende del sistema social-jurídico al que se haga referencia, pero es relativamente sencillo

seguir el rastro; sin embargo, el registro digital no tiene propiamente una institución delimitada por un sistema social-jurídico claro, si no que existen un sinnúmero de posibles registros con variables que atienden a otro concepto poco explorado para nuestra actualidad, el de autodeterminación informativa.

También en el mundo material es sencillo de identificar el reconocimiento social de terceros frente a la identidad de una persona. Hay muchos elementos que componen la identidad, partiendo de los elementos biológicos o físicos característicos, sin embargo, estos elementos no existen propiamente en el ciberespacio, ahí todo es una construcción de apreciación, puesto que la estructura que da forma es en esencia un código binario que, gracias a grandes mentes, podemos todos visualizarlo en una forma que reconocemos fácilmente.

No obstante que no existen estos elementos de registro y reconocimiento en el ciberespacio, como en el mundo material, cada vez que se utiliza el Internet, se construye una "identidad digital" que le permite a los sistemas y personas que los operan reconocerla prácticamente de inmediato y así etiquetarnos dentro de una clasificación de identificación personalizada. Esto me lleva a una gran pregunta ¿Somos conscientes de qué identidad estamos construyendo en el ciberespacio? Esto es importante preguntarlo y buscar caminos sistematizados que simplifiquen el andar, porque, aunque no se quiera, forma parte de la "identidad material" y, en consecuencia, de la personalidad.

Más allá de la conciencia que se haga de la identidad que se está construyendo en el internet, la realidad es que se puede construir o reconstruir tantas veces como se desee, la diferencia en este momento es que existe la posibilidad de hacer una "identidad digital" a conciencia.

A partir de esta guía orientadora, que permite tener el conocimiento de lo que es una "identidad digital" y sus alcances, se puede establecer una que conecte a la perfección con lo que se pretende obtener de la "identidad del mundo material". También es posible obtener una misma identidad registral, a pesar de la multiplicidad de registros, y conseguir una clara apariencia de lo que somos y buscamos como personas más allá de espacios delimitados.

Impactos del reconocimiento de la identidad digital en la primera infancia hacia una ciudadanía digital

Adriana Yadira Cárdenas Tagle

La identidad digital es un concepto cada vez más relevante en nuestra sociedad, se ha convertido en una parte integral de la vida moderna y su impacto en la primera infancia[1] es un tema que merece nuestra atención, en virtud de que se ve cada vez más expuesta a dispositivos digitales y plataformas en línea, ocasionando efectos durante los primeros años de vida mismos que se tendrán impacto a lo largo de toda nuestra vida, siendo que este contexto digital está moldeando su desarrollo cognitivo, emocional y social.

En primer lugar, es importante destacar que la identidad digital se refiere a la imagen que una persona proyecta en línea, a través de las redes socio digitales y otras plataformas. Según Johnson (2018), la identidad digital puede desempeñar un papel crítico en el desarrollo temprano del autoconcepto en la niñez. La interacción

[1] En general, la primera infancia se define como la etapa inicial de la niñez, es decir, ese periodo de la vida por el que transitan las personas menores a 12 años de edad, de acuerdo con lo establecido en el artículo 5º, tanto de la Ley General de los Niños, Niñas y Adolescentes, como de la Ley de los Niños, Niñas y Adolescentes del Estado de México.

con estos entornos les permite explorar, experimentar y compartir aspectos de sí mismos que pueden no ser tan accesibles en su entorno físico. Esta capacidad de autoexpresión digital contribuye a la formación de su identidad personal y social.

Cuando estamos observando el proceso por el cual la niñez es consciente de su presencia en línea y está involucrada en actividades en el mundo virtual, esto puede tener impactos significativos, ya sean positivos como negativos, afectando potencialmente su desarrollo en diferentes áreas de su vida.

Uno de los impactos positivos es que puede contribuir al desarrollo de habilidades sociales y competencias digitales. Según Mueller (2020), las y los niños que aprenden a manejar su identidad digital desde una edad temprana y tienden a desarrollar una mayor capacidad para interactuar y comunicarse en entornos en línea. Además, las interacciones en línea pueden promover la participación social y la empatía a través del contacto con una diversidad de perspectivas (Subrahmanyam & Šmahel, 2011), lo que implica de manera importante que la niñez aprenda a dominar sus fortalezas en ámbitos digitales lo que podría incidir de forma efectiva en sus entornos como ciudadanos responsables.

En ese sentido, es responsabilidad en primera instancia de los tutores poder apoyar a la integración de aspectos tecnológicos a la vida de los menores, para insertar esquemas de responsabilidad y límites en los entornos digitales para evitar situaciones de riesgo, no obstante; las autoridades escolares tiene un reto mayúsculo sobre cómo migra de ser profesores análogos a profesores híbridos, con las mismas encomiendas al contar con la asistencia presencial del alumnado, pero con una vida que vigilar en entornos digitales, para lo cual hablar de ética en los entornos digitales, alfabetización digital y sobre todo salud mental de las niñas, niños y

adolescentes es la principal área de oportunidad que se ve para que puedan desarrollar una identidad digital saludable.

Como lo mencionaba, existen riesgos y peligros asociados con el reconocimiento de la identidad digital en la primera infancia, como es la exposición prematura a las redes sociales y la identidad digital puede aumentar la vulnerabilidad de los niños a la intimidación, el acoso cibernético (Smith,2019); al tener una huella digital temprana, la niñez podría enfrentar dificultades para controlar su vida privada más adelante, ya que su información personal estará disponible en línea y en un futuro ello podría causarle implicaciones negativas en el ejercicio de sus derechos, desde aplicar para determinadas escuelas, conseguir empleo, e incluso afectar sus derechos político electorales.

Para abordar estos desafíos y aprovechar los beneficios de la identidad digital en la primera infancia, es esencial que madres, padres, educadores, y especialmente la sociedad como engranaje puente de la información, tengamos un enfoque equilibrado que fomente el uso positivo y responsable de la tecnología mientras seamos conscientes de los posibles riesgos y beneficios que conlleva la consolidación temprana de una identidad digital, sobre lo que habría que plantear a los legisladores en estos casos cómo actuará el derecho de cancelación o el llamado derecho al olvido que en México ha causado tanta polémica.

Es necesario hacer este tipo de planteamientos en medida de que cada día hay un incremento considerable de niñas, niños y adolescentes en línea, que están conformando su identidad digital, y que ya son presas de las empresas que poco a poco podrán ir "formando" preferencias en los menores y que posiblemente algunas veces no sea para una toma de decisiones adecuada; es por ello que valdría la pena contar con una red de creación y verificación de contenidos destinado

específicamente para menores, así como incentivar el acceso desde el diseño en las plataformas y buscadores.

No basta con fomentar estrategias educativas digitales sólidas y la adopción de pautas claras maximizando los beneficios y minimizando los peligros, sino que es imperante la vinculación con la sociedad civil para lograr ajustes y controles que lleven a la primera infancia a consolidarse como los ciudadanos más preparados de la época, más conscientes, capaces y empáticos, capaces de conseguir que los objetivos de desarrollo sostenible sean cumplidos.

Referencias

- Johnson, T. (2018). *The Impact of Early Exposure to Digital Identity Formation in Early Childhood*. Journal of Child Development Studies.
- Ley de los Niños, Niñas y Adolescentes del Estado de México. (2015). Legislatura del Estado de México. Obtenido de: https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/ley/vig/leyvig098.pdf
- Ley General de los Niños, Niñas y Adolescentes (2023). Cámara de Diputados. Obtenido de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA.pdf
- Mueller, L. (2020). *Digital Identity and Social Skills in Early Childhood: A New Perspective.* Journal of Early Childhood Development.
- Smith, J. (2019). *Risks and Dangers of Early Digital Identity Recognition in Early Childhood.* Cyberpsychology Review.
- Subrahmanyam, K., & Šmahel, D. (2011*). Digital youth: The role of media in development.* Springer.

Análisis sobre la construcción y gestión de la identidad digital

Julio César Bonilla Gutiérrez

A medida que la sociedad se vuelve más digitalizada, la identidad digital personal se convierte en una extensión fundamental de nuestro ser. Este componente esencial de nuestra interacción en línea plantea tanto oportunidades como desafíos en su construcción y gestión que, en muchos sentidos, recae sobre nosotros.

La identidad digital abarca el conjunto de características, datos e información en línea que representan y definen a un individuo o entidad (van Dijck, 2013). Esta incluye: i) Datos personales: como nombre y fecha de nacimiento; ii) información de redes sociales: perfiles y publicaciones; iii) historial de transacciones: compras y registros bancarios; y, iv) comportamientos en línea: sitios web visitados y aplicaciones usadas.

La construcción de la identidad digital

Autenticidad versus construcción. La naturaleza dualista de la identidad digital se debate entre la representación auténtica y la construcción deliberada (Boyd, 2010). Las personas tienden a:

- Modelar su identidad: Presentando una versión idealizada sobre sí mismos.

- Controlar su narrativa: Decidiendo cuidadosamente qué mostrar y omitir.

- Interactuar estratégicamente: Adaptándose a las normas y expectativas de plataformas específicas.

Sin embargo, la forma en que modelemos y construyamos nuestra identidad digital tiene repercusiones tangibles; por ejemplo, en nuestra reputación, porque las percepciones en línea pueden afectar nuestras oportunidades offline. Asimismo, porque la sobreexposición digital puede conllevar riesgos de seguridad. Otro importante elemento que debemos considerar es nuestro bienestar mental, porque la representación digital puede influir en nuestra autoimagen y autoestima.

Desafíos en la gestión de la identidad digital

En razón de lo anterior, existen diversos desafíos que se relacionan con la identidad digital de las personas y que no son, en forma alguna, irrelevantes. Los mismos, por ejemplo, los tenemos en materia de seguridad y privacidad porque, a medida que crece la amenaza de la ciberdelincuencia, proteger la identidad digital es crucial (Deuker, 2011). Es esencial emplear mecanismos de autenticación robustos, limitar la divulgación de datos sensibles y estar alertas ante potenciales amenazas en línea. La tensión entre realidad y representación puede ser mentalmente desafiante (Turkle, 2011). Por tanto, es vital reconocer y abordar la fatiga digital, fomentar una representación honesta en línea y buscar apoyo cuando la presión de la identidad digital se vuelve o pueda volver abrumadora.

En el contexto anterior, hay invaluables oportunidades susceptibles de ser aprovechadas; por ejemplo, la educación es esencial para capacitar a las personas en la gestión efectiva y segura de su identidad digital (Hargittai & Marwick, 2016). Asimismo, soluciones emergentes como blockchain prometen revolucionar la gestión de identidades (Tapscott & Tapscott, 2016).

Por el lado del empoderamiento de la ciudadanía, controlar nuestra identidad digital puede potenciar la participación cívica y nuestra autodeterminación informativa en el ciberespacio.

Nuestra identidad digital, aunque intangible, tiene consecuencias muy reales. Navegar por sus complejidades requiere tanto comprensión técnica como autoconciencia.

Referencias

- Boyd, D. (2010). *Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications*. Routledge.
- Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press.
- Deuker, A. (2011*). Identity Management for e-Service Ecosystems*. University of Stuttgart.
- Hargittai, E., & Marwick, A. (2016). *The Life Cycle of a Social Media Meme.* Cambridge University Press.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Penguin.
- Turkle, S. (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other.* Basic Books.

Importancia de la Protección de datos personales (vulneraciones)

Norma Julieta del Río Venegas

La protección de datos personales es un tema de suma relevancia con la llegada y evolución del medio tecnológico con el que convivimos, en donde se recaba y almacena información de particulares, la cual, guarda datos sensibles que, de caer en manos equivocadas, pueden poner en alto riesgo a sus propietarios.

Hoy en día, este avance tecnológico nos obliga a brindar nuestra información personal, tanto a servicios privados como aplicaciones o prestación de servicios, así como en plataformas gubernamentales. La privacidad debemos entenderla como una esfera que no es pública y a la cual sólo deben acceder terceros bajo nuestro entero consentimiento, puesto que es un espacio que contiene datos personales que sólo su propietario conoce.

¿Qué es una vulneración de datos personales?

Es un incidente de seguridad de la información que afecta los datos personales en cualquier fase de su tratamiento, sin embargo, recordemos que todas las vulneraciones son incidentes de seguridad de la información, pero no todos los incidentes de seguridad se consideran vulneraciones.

Obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que las áreas propietarias deben cumplir respecto de las vulneraciones. (Cámara de Diputados, 2017)

- Analizar las causas por las cuales se presentó la vulneración e incluir en su plan de trabajo el documento de seguridad, las acciones preventivas y correctivas (Artículo 37).
- Llevar una bitácora de vulneraciones (Artículo 39).

- Informar al titular y al INAI las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales de la persona titular (Artículo 40).

Tipos de vulneraciones

- Pérdida o destrucción no autorizada
- Robo, extravío o copia no autorizada
- Uso, acceso o tratamiento no autorizado
- Daño, alteración o modificación no autorizada
- Divulgación o revelación no autorizada

Principios rectores de la protección de datos personales. (INAI, 2019)

El tratamiento que debe seguir toda persona que emplea datos personales, incluyendo el entorno comunicativo para la no vulneración de datos personales.

- Licitud y lealtad, consentimiento, información, proporcionalidad, finalidad, calidad y responsabilidad.

Para el INAI, el manejo de datos personales relacionados con la identidad de una persona, así como el tratamiento de los otros datos que se recaben, requieren del mayor cuidado posible desde la esfera normativa vigente en nuestro país, puesto que cualquier afectación o vulneración podría generar daños significativos de una difícil o imposible reparación, sobre todo, considerando que los datos personales hacen referencia a aspectos que permiten asociar e identificar de manera única a una persona y que, por ende, constituyen características insustituibles.

Resulta fundamental que el tratamiento de datos personales cumpla con los principios, deberes, derechos, procedimientos y obligaciones, previstos en la normatividad en materia de protección de datos personales, cumpliendo así con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Referencias

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (2017). Cámara de Diputados. Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
- Marcos de competencias. (2019). INAI. Obtenido de https://micrositios.inai.org.mx/marcocompetencias/?page_id=370

Riesgos asociados con la identidad digital, como violencia digital, algunos tipos y ejemplos

Xitlali Gómez Terán

Con los avances tecnológicos que, sin duda alguna, representaron una serie de beneficios para la sociedad, también se acompañaron de diversos riesgos, entre ellos, la violencia digital. El INEGI (2022) señaló que las personas usuarias de Internet (104.2 millones de personas de 12 y más años usuaria de internet) víctimas de ciberacoso[2] se incrementó de 21 % a 21.7 % en 2021 con una mayor prevalencia en el caso de las mujeres (22.8 %) que los hombres (20.6 %) y que la situación más frecuente fue el de contacto mediante identidades falsas (INEGI, 2022).

El Instituto Nacional de Estadística, Geografía e Informática (INEGI) (2022, p.1) realiza una medición mediante el Módulo sobre Ciberacoso (MOCIBA), el cual explora diversas expresiones como:

i. Recibir mensajes ofensivos, con insultos o burlas.
ii. Recibir llamadas ofensivas, con insultos o burlas.

[2] *(…) se refiere a la situación en la que alguien se expone, de manera repetida y prolongada, a acciones negativas por parte de una o varias personas que buscan hacer daño o causar molestias. Los medios que utilizan son electrónicos, como el teléfono celular e internet. INEGI, 2022, p. 1*

iii. Ser criticado(a) por su apariencia (forma de vestir, tono de piel, peso, estatura, etc.) o clase social.
iv. Que una persona se hiciera pasar por usted para enviar información falsa, insultar o agredir a otras personas.
v. Ser contactado(a) por medio de nombres falsos para molestarle o dañarle.
vi. Ser vigilado en sus sitios o cuentas en Internet para causarle molestia o daño.
vii. Ser provocado en línea para que reaccione de forma negativa.
viii. Recibir insinuaciones o propuestas de tipo sexual que le molestaran.
ix. Recibió fotos o videos de contenido sexual que le molestaron.
x. Publicar o vender imágenes o videos de contenido sexual reales o simulados, de usted sin su consentimiento.
xi. Publicar información personal, fotos o videos para dañarlo(a).
xii. Amenazar con publicar información personal, audios o video para extorsionar; y
xiii. Otra situación que lo(a) haya afectado. (INEGI, 2022, p. 1)4

Las consecuencias que pueden derivarse de violencia dependen en gran medida de las características de la persona afectada; pero en términos generales, la violencia digital puede traducirse en conductas de violencia en el mundo real como violencia física, sexual, que incluso puede derivar en la muerte de la persona. Asimismo, puede derivar en que las víctimas puedan iniciar con conductas de autolesionarse y la afectación puede ser tan grave que puede llevar incluso al suicidio. En el caso de personas adultas pueden llegar a perder su empleo, la afectación a su reputación personal y profesional y la cancelación de su proyecto en la esfera pública Fondo de Población de la Naciones Unidas (UNFPA, 2022).

Toda persona que interactúa en el ámbito digital puede ser víctima de violencia en el ciberespacio, no obstante, esta se puede recrudecer cuando pertenecen a grupos históricamente discriminados como mujeres, personas LGBTIQ+ de color, con alguna discapacidad, entre otras. De ahí que este tipo de conductas provengan de conductas de misoginia, racismo y homofobia.

Especial relevancia merece la atención que se debe prestar a la niñez y las juventudes que participan en el mundo digital, quienes tienen una mayor exposición porque pasan un más tiempo en la red de Internet, desconocen los medios para protegerse y las secuelas de la violencia digital puede generar graves daños y limitar su pleno desarrollo.

Referencias

- INEGI (2022), Comunicado de Prensa Núm. 364/22, 13 de julio de 2022. Disponible en: www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/mociba/MOCIBA2021.pdf
- UNFPA (2021). Documento orientativo para informar sobre la violencia digital: Guía práctica de referencia para periodistas y medios de comunicación, Disponible en: https://www.unfpa.org/es/resources/Documento-orientativo-para-informar-sobre-violencia-digital

Consejos para proteger la identidad digital y mantener la privacidad en línea

Iván Díaz González

Antes de iniciar con algún consejo respecto a la forma de protección de la identidad, es indispensable analizar el constructo de la identidad digital. La identidad por sí misma no es un elemento finito, ya que, dependiendo del contexto, lugar e interacciones, abordara un conjunto de elementos que permitirán la identificación de un individuo en un espacio-tiempo finito, de ahí que la identidad debe ser tomada como un conjunto de componentes (de identidad), que permiten distinguir a un individuo o entidad del resto de los entes que se encuentran en el mismo espacio-tiempo, dichos componentes de la identidad están basados en características físicas, psicológicas, documentales, procedimentales y de comportamiento.

Ya cuando se aborda el tema de digital, comúnmente se aborda el contexto de que sea utilizará la identidad en los medios electrónicos o cualquier otra tecnología, sin embargo, quiero abordar que más allá del uso de una tecnología, el tema digital crea un espacio-tiempo distinto en un dominio de operación denominado ciberespacio que si bien, corre paralelo que el espacio-tiempo físico, en el ciberespacio podemos encontrar una gran cantidad de herramientas para modificar el contexto, ya que el lugar no está claramente definido al no haber una delimitación territorial y las interacciones se pueden ver alteradas de tiempo en tiempo.

Una vez que se ha contextualizado la definición de identidad digital, quiero destacar que para poder llevar a cabo una protección de la identidad no basta simplemente con comprar un conjunto de herramientas, comprar un software para el manejo de credenciales, guardar y aprenderme mis contraseñas o no permitir las cookies, para

la protección de la identidad se requiere un gran compromiso de cada uno de los individuos, de ahí que se propone que los entes de los que se requiere proteger su identidad deben cumplir con un conjunto de controles que permitirán alinear los esfuerzos de protección de forma adecuada a las necesidades del ente, su contexto y el conjunto de componentes de la identidad.

Para esta protección se recomienda seguir 4 sencillos pasos que están descritos en el marco de trabajo de protección de robo de la identidad también denominado KAOS (sigla de palabras en inglés referentes a conocimiento, valoración, organización y seguridad) (Identity Management Institute, s.f.). De este marco de referencia se desprende que lo primero que debemos hacer para cuidar la identidad es saber qué componentes de la identidad tengo y donde se encuentran distribuidos estos componentes, para lo cual es importante tener un inventario de todos los componentes y saber a quién o a qué le hemos compartido dichos componentes.

El siguiente paso es valorar el tratamiento que se tiene sobre los componentes de la identidad y para ello es necesario que se evalúe si cada uno de los componentes que han sido entregados a terceras partes están justificados en su tratamiento, si están siendo tratados correctamente, que los componentes se encuentren actualizados y con ello aclarar cada una de las entregas y elementos del inventario de componentes de identidad.

Ya que tenemos un inventario claro lo siguiente es categorizar la información, la cual se puede realizar por prioridad de protección o por importancia dentro del contexto; sin importar la forma de categorizarla, de este proceso se puede obtener un orden que permitirá no sólo tener el control de los componentes de la identidad que se encuentran en poder de la entidad sino también con terceros, lo cual permitirá el

monitoreo de los movimientos que se realizan con los componentes de la identidad y con ello poder actuar justo al tiempo en cuando la información potencialmente se pueda poner en riesgo y saber qué hacer.

Por último, se deben implementar controles de seguridad como puede ser limitar el acceso a la información en un espacio-tiempo, no compartir los componentes de la identidad con cualquier persona o entidad, no conectarse a sitios que son dudosos en sus procesos, así como cualquier otro proceso de control que hagan sentir que la información de su identidad se encuentra en un estado aceptable de procesamiento y de seguridad.

En conclusión, la identidad digital se puede proteger con el esfuerzo de cada persona mediante un adecuado control de sus componentes de identidad y estableciendo la interacción con cada una de las personas, entidades o sitios con las que se comparte información.

Referencias

- Identity Management Institute. (s.f.). *Identity Management Institute center for Identity Gobernance.* Obtenido de *https://identitymanagementinstitute.org/kaos-identity-theft-protection-framework/*

Consejos para proteger la identidad digital y mantener la privacidad en línea

Xitlali Gómez Terán

Para prevenir los riesgos del robo de identidad o el mal uso de las cuentas de redes sociales, así como el ciberacoso, según el proveedor de servicios UANATACA[3] (2020) es importante implementar las siguientes medidas:

1. Actualizar el software regularmente: mantener actualizados nuestros equipos y aplicaciones es uno de los factores que fortalece la seguridad e impide el ataque de nuevos virus informáticos.
2. Tener precaución al navegar en Internet: revisar los enlaces antes de hacer clic sobre ellos, en especial con las noticias falsas (las famosas "fake news") que se han convertido en un método frecuente para llevar a cabo ciberataques.
3. Navegar sólo en sitios seguros**:** evitar facilitar datos personales hasta verificar el nivel de seguridad del portal. La indicación “https” antes de la URL indica que se trata de una conexión segura, protegida por una tecnología encriptada.
4. Es importante estar al día en medidas de seguridad cibernética. Los expertos en ciberseguridad descubren nuevos métodos para proteger los datos personales de los internautas.
5. Utilizar conexiones WI-FI protegidas de cifrado WPA: evitar redes inalámbricas como las que ofrecen lugares públicos, ya que puede dejar sus datos expuestos.

[3] Compañía internacional experta en identidad digital, perteneciente al grupo empresarial Bit4id, que nace con la vocación de generar valor y confianza en las transacciones digitales.

6. En caso de enfrentar acoso digital mediante redes sociales se cuenta con diversos recursos; por ejemplo, en Facebook[4] disponen de recursos que pueden ayudar, Twitter[5], así como en Instagram[6] y TikTok[7]. (UNICEF, s/f).

Referencias

- UANATACA, seis consejos para protegerla. Disponible en: https://web.uanataca.com/es/blog/transformacion-digital/proteger-identidad-digital

- UNICEF (2020), Ciberacoso: Qué es y cómo detenerlo. Disponible en: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

[4] https://www.facebook.com/safety/bullying
[5] https://help.twitter.com/en
[6] https://about.instagram.com/es-la/safety y https://about.instagram.com/es-la/community/anti-bullying
[7] https://support.tiktok.com/es/safety-hc/report-a-problem/report-a-video y https://www.tiktok.com/safety/es-es/bullying-prevention/

Huella digital

Laura Lizette Enríquez Rodríguez

El uso de Internet en la actualidad se ha convertido en una de las actividades más comunes para las personas, tanto así que actualmente se habla de la generación de una identidad digital, derivada del conjunto de información acerca de nosotros en línea, que se traduce en "el conjunto de atributos que vinculan una entidad personal con sus interacciones online" (Álvarez, 2018); es decir, que tras nuestro paso en Internet se va creando una imagen o reputación que se alimenta de los datos que ahí vertemos.

Es así que todas las actividades que efectuamos en las redes generan una huella digital, un rastro que dejamos cada vez que accedemos a Internet y que puede aportar beneficios en nuestra vida cotidiana, pero también está relacionada con preocupaciones sobre la privacidad y riesgos asociados a la protección de nuestros datos personales.

Desde información que compartimos en las páginas que visitamos, sobre los productos que compramos, nuestra ubicación, información laboral, académica y de nuestras relaciones personales, hasta la identificación por medio de nuestra dirección IP que permite reconocer nuestro dispositivo de manera única en Internet, entre muchas más, constituyen una red más compleja, identificándonos como usuarios y formando así nuestra identidad digital.

Asimismo, lo que posteamos en redes sociales como Facebook, en Linkedin, lo que Google dice de nosotros y lo que a mediano o largo plazo crea una reputación (e-reputación) sobre nuestra persona en el ámbito virtual.

Es importante que, como personas usuarias, sepamos que esta huella digital, bien puede crearse de manera directa o indirecta, es decir por nosotros mismos siendo quienes compartimos voluntariamente nuestra información o bien, la generada por terceros.

Específicamente, la huella digital se genera de manera directa cuando nosotros como personas usuarias del Internet somos conscientes de crear un rastro en ciertos sitios, como cuando por voluntad propia dejamos la información de nuestras tarjetas de crédito o débito, cuando aceptamos los avisos de privacidad de los sitios que visitamos o, cuando ingresamos nuestros correos electrónicos en los mismos.

Por el contrario, la manera indirecta se da cuando incluso sin nuestro conocimiento, las páginas de Internet o las redes sociales están guardando datos sobre nosotros, como historiales de búsqueda, actividades recientes o sitios que visitamos.

Como resultado, nuestra huella digital genera lo que se conoce como "filtros burbuja", que predicen y seleccionan la información que al usuario le podría interesar, ajustándose a nuestras preferencias basándose en nuestra información personal.

Sin embargo, ante estos filtros se genera información que queda fuera de nuestra voluntad, por lo que nuestra percepción de la información buscada, la ideología construida y hasta nuestra propia identidad digital pudieran estar sesgadas por el delimitado universo de resultados arrojados por el filtro, generando como consecuencia negativa una posible manipulación y propagandas engañosas, así como la falta de libertad para acceder a una cantidad de contenido más amplia.

En este contexto, el ideal sería llegar a lo que Christopher Allen denomina como "identidad soberana", es decir, al siguiente paso de la identidad digital, en la cual el titular tiene el control absoluto de su información personal.

Referencias

- Allen, C. (2016). *The Path to Self-Sovereign Identity.* Coindesk. Disponible en: https://www.coindesk.com/path-self-sovereign-identity
- Álvarez, C. (2018*). Identidad digital: ¿Qué es y cómo protegerla?* Regulación Financiera. BBVA Research. Disponible en: https://www.bbva.com/es/identidad-digital-protegerla/
- Pariser, E. (2017). *El filtro burbuja: cómo la web decide lo que leemos y lo que pensamos.* España: Taurus.

¿Qué es la huella digital y cómo se genera?

Naldy Patricia Rodríguez Lagunes

Casi todas las actividades de la vida cotidiana están relacionadas con el uso de Tecnologías de la Información y la Comunicación (TIC). Cuando las personas se encuentran navegando, usando algún dispositivo electrónico para visitar sitios web, interactuar en aplicaciones, foros y archivos, dejan rastros de datos. Estos rastros de datos constituyen su huella digital.

Esta huella digital puede ser una herramienta útil para quienes pretenden indagar sobre la actividad en línea de las personas, así como obtener datos sobre sus dispositivos electrónicos.

Cabe señalar que una huella digital por sí sola no tiene mucho sentido si la apreciamos de forma aislada, es decir, si comparamos esto con una migaja de pan (un punto de datos) no revela mucho, pero cuando se considera un conjunto de huellas digitales, a través de una recopilación de éstas, podemos obtener la red de datos personales más grande que existe, ya que se contaría con una historia detallada de las personas, incluidas las direcciones web que visita, las búsquedas efectuadas, los textos que envía, así como las fotos y los archivos que carga y descarga, por tanto, si una persona utiliza Internet, no puede evitar dejar una huella digital.

¿Cuánto dura una huella digital? Su duración dependerá de la superficie donde se plasme; si la huella se estampa sobre concreto (fotos o vídeos subidos a Internet) su duración será mucho mayor que una huella dibujada en la arena de mar (el historial de búsquedas o de navegación), por lo que es responsabilidad de cada persona el cuidar de su huella digital, ya que esta constituye la base de su reputación en línea.

Es preciso señalar que existen dos tipos de huellas digitales, las pasivas y activas, distinguiéndose, una de la otra, por el consentimiento informado de las personas.

Así, cuando las personas realizan actividades de intercambio de datos en línea de manera intencional o con consentimiento, ello conformará su huella digital activa, como pudiera ser: el llenar formularios, sus publicaciones en redes sociales, la utilización de su correo electrónico, entre otros; mientras que la huella digital pasiva, será aquella que refiere a los datos recopilados cuando se rastrean sus actividades en línea sin su consentimiento, como por ejemplo, los datos sobre el uso de sitios

web (cuántas veces visita un sitio web, dirección IP, cómo llega a un sitio web), registros financieros, etc.

En suma, nuestra huella digital podría utilizarse para evaluar el tipo de persona que somos, para bien o para mal. Por muy anónimo que parezca, lo que hacemos en Internet se vigila y queda grabado de forma pasiva.

Aunque no es pronosticable cuándo serán utilizados nuestros datos para alguna estafa o suplantación de identidad, los peligros que conllevan tener una huella digital, sin conocimiento de lo que implica, pueden ser desastrosos si se hace un mal uso de ella, por ejemplo del doxing, el cual se define como la práctica de publicar información personal de terceros con la intención de intimidar, extorsionar o afectar de alguna otra manera (Lameiras). Esto a través de revelar información identificadora de una persona en línea, como su nombre real, dirección, lugar de trabajo, datos financieros, número teléfono y cualquier otra información personal.

Por ello que "*una huella digital podría considerarse sensible si a través de un uso indebido de la misma se puede tener acceso a información privilegiada que pudiera poner en riesgo la seguridad o estabilidad patrimonial o financiera de una persona o incluso su condición jurídica*". En conclusión, nuestra huella digital es tan importante como nuestros datos personales, ya que ella constituye nuestra identidad digital.

Referencias

- Amor, J.R., Villegas, C. (2022) *Huella digital ¿Servidumbre o servicio?.* Editorial Tirant Humanidades. Valencia.
- Ibañez, R, (1989) *La huella digital y el derecho mexicano.* México, D.F.: Sista.
- Instituto Nacional de Transparencia y Acceso a la Información Pública (INAI) (2018) *Guía para el Tratamiento de los Datos Biométricos.* Ciudad de México. https://home.inai.org.mx/wpcontent/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf
- Lameiras, L. (2022) ¿Qué es el doxin y cómo protegernos? Noticias, opiniones y análisis de la comunidad de seguridad de ESET. Obtenido de: https://www.welivesecurity.com/la-es/2022/09/16/que-es-doxing/
- Maldonado Fabián, N. I. (2021). Huella digital - Biblioteca central UNAM. consultable en la siguiente liga electrónica: https://www.bibliotecacentral.unam.mx/index.php/desarrollo-de-capacidades-informativas-digitales-y-comunicacionales/huella-digital

Concienciación sobre la importancia de cuidar la huella digital y cómo afecta la reputación en línea

Miriam Josefina Padilla Espinosa

Cuando una persona usuaria realiza una publicación en sus redes sociales, brinda un comentario en un video, sube una fotografía o etiqueta los lugares que visita con frecuencia, genera información que se encuentra disponible en Internet y otorga detalles sobre las diferentes actividades que realiza en este espacio.

Es importante saber que esta información puede ser generada y consultada por la persona usuaria o por terceras personas y que el conjunto de estos datos genera una reputación digital que es importante cuidar, dado que se convierte en el primer contacto que las personas desconocidas tendrán sobre la persona usuaria.

En algunos casos esta información puede ser decisiva para brindar o no un apoyo académico o una oportunidad profesional y también es utilizada por las empresas que a partir de la información de los datos de las huellas digitales crean perfiles de las personas usuarias que puedan ser comercializados con otras empresas.

Algunas formas en que las empresas recolectan datos de las personas usuarias en Internet son a través de las "cookies", que son pequeños archivos que se almacenan en sus dispositivos y que contienen información sobre la navegación, los anuncios que ha visualizado, la zona horaria, la ubicación geográfica y hasta contraseñas.

Dado el tipo de información que es almacenadas en las cookies es importante su protección considerando que los ciber delincuentes pueden realizar acciones ilícitas para obtenerlas como son: el robo o secuestro de sesión, redirigir a tiendas en línea fraudulentas o explotar vulnerabilidades en los programas del equipo o en el navegador.

Adicionalmente esta información de la huella digital puede ser utilizada por los atacantes para recolectar datos sobre la persona usuaria que le puedan ser útiles para realizar ataques de ingeniería social más efectivos.

Por lo anterior, es de suma importancia que las personas usuarias conozcan que información de ellos está disponible en Internet, esto les permitirá saber qué

configuraciones de privacidad y seguridad requieren ser revisadas y fortalecidas, para esto pueden consultar diferentes guías y recomendaciones.

Además, las personas usuarias pueden utilizar la navegación en modo incógnito de tal forma que el navegador no almacenará ningún tipo de información sobre las páginas web visitadas.

Otra recomendación importante es analizar si las autorizaciones que se brindan a los sitios para recolectar cookies son permanentes o transitorias.

Es primordial que las personas usuarias generen una conciencia sobre la importancia de conocer y proteger la información que de ellos está disponible en Internet y fomentar la cultura de la denuncia para reportar aquellas páginas que expongan información personal sin su consentimiento.

Referencias

- Agencia Española de Protección de Datos. (2019). *Guía de privacidad y seguridad en Internet.* AEPD. https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-y-seguridad-en-internet.pdf
- INCIBE. (2018). *Entre cookies y privacidad*. INCIBE Ciudadanía Blog. Recuperado de https://www.incibe.es/ciudadania/blog/entre-cookies-y-privacidad
- Ministerio de Justicia y Derechos Humanos de la Nación. (s/f). *¿Qué es la huella digital en Internet?* Convocatorias en la Web - Situaciones. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-huella-digital-en-internet

- UNICEF (2020). *Guía sobre Convivencia Digital*. UNICEF Argentina. https://www.unicef.org/argentina/media/9481/file/Gu%C3%ADa%20sobre%20Convivencia%20Digital-2020.pdf

II. CIUDADANÍA DIGITAL RESPONSABLE

Definición de ciudadanía digital

María de los Ángeles Guzmán García

El concepto ciudadanía digital está cada vez más presente en la discusión de políticas públicas y del mundo académico, por lo que para hablar de ciudadanía digital primero es necesario comprender que se entiende por este concepto; la UNESCO la define como un conjunto de competencias que faculta a la ciudadanía a acceder, recuperar, comprender, evaluar y utilizar información con fines creativos.

A partir de esta definición, es importante resaltar que la ciudadanía digital se refiere al conjunto de derechos, competencias y obligaciones que permiten a las personas el uso, participación libre y responsable de las tecnologías digitales, permitiéndoles comprender, navegar, participar e interactuar entre la sociedad civil y el gobierno de forma ética y segura.

La ciberciudadanía forma parte del sistema del gobierno electrónico o democracia digital, que consiste en la administración de los recursos del Estado mediante las nuevas tecnologías, para hacer la vida más fácil. Asimismo, agiliza diversos trámites y servicios proporcionados por el gobierno, pues se llevan a cabo de forma electrónica desde cualquier lugar con acceso a Internet; por ejemplo, solicitar actas de nacimiento, CURP, trámites catastrales, denuncias ante la fiscalía, entre otros.

En materia de acceso a la información y protección de datos personales conocidos como derechos ARCO[8], resulta importante señalar que estos se pueden ejercer mediante la ciudadanía digital, a través de la Plataforma Nacional de Transparencia (PNT), implementada a partir del 2016, en la que las personas pueden ejercer sus derechos, solicitando información pública de interés general, así como requerir acceso a los datos personales que resguardan las instituciones públicas.

La ciudadanía digital trae consigo los beneficios de rapidez en los trámites gubernamentales sin salir de casa en tiempo real, mayor participación en la realización de denuncias y contacto con autoridades. Otra forma es el acceso a la educación digital mediante las tecnologías de la información y comunicación (TIC), que ayudan a la formación de personas críticas, conscientes del uso de estas tecnologías y de los riesgos, así como sus beneficios y posibilidades. Todo ello aumenta en gran medida la comodidad y la mejoría de la calidad de vida de las personas, así como la reducción de tiempos de traslado, en aquellos que anteriormente se realizaban presencialmente.

Pero no todo resulta ideal al momento de utilizar los medios digitales, por ejemplo, en el ámbito educativo, durante la pandemia de COVID-19, quedó demostrada la falta de una infraestructura digital eficiente por parte de las universidades mexicanas y de muchos otros lugares del mundo, para llevar a cabo las clases a través de medios electrónicos seguros y eficaces. Esto se solucionó gracias a una rápida acción por parte de las autoridades universitarias, dichas deficiencias se subsanaron, logrando la impartición de la educación en línea de modo seguro, transparente y privado.

[8] Acceso, Rectificación, Cancelación y Oposición.

Por otro lado, si bien la tecnología ha avanzado a pasos agigantados, aún existen áreas de oportunidad, como las desigualdades en el acceso a Internet entre los grupos vulnerables en México, que se determinan con base a criterios económicos, culturales, geográficos, por género, edad, etc.; ya que no toda la ciudadanía tiene acceso físico a la telefonía e Internet, esto a pesar de que hoy en día sean considerados servicios básicos humanos.

Otro de los riesgos, es la brecha digital generacional, principalmente por la edad, que se refiere a la distancia entre quienes utilizan las tecnologías como parte de su vida diaria y aquellas que no tienen acceso a ellas, o que, aunque lo tengan, no saben cómo utilizarlas. Esto ocurre en muchos casos, debido a que la mayoría de la población mayor de 55 años, aproximadamente, no tiene competencias o habilidades en el mundo digital.

La ausencia de políticas públicas, normas de privacidad digital, así como la falta de una adecuada regulación al derecho a la propia imagen, honor y ciberseguridad, representa un peligro para la ciudadanía; ya que se puede afectar la vida privada de manera irremediable si no se toman las medidas pertinentes a tiempo. En México no hay una regulación normativa, efectiva y homogénea que proteja la privacidad, pues sólo existen leyes y reglamentos respecto a la protección de datos personales, y el contenido de estos derechos es diferente.

En nuestro país, particularmente en la Ciudad de México, a través de su Constitución se regula el derecho a la propia imagen, en su artículo 6, inciso c) numeral 1, el cual establece que toda persona, grupo o comunidad tienen derecho al nombre, a la propia imagen y reputación, así como al reconocimiento de su identidad y personalidad jurídica.

Existen avances legislativos de gran trascendencia y evolución del derecho como la Ley Olimpia, consistente en un conjunto de reformas legislativas a los códigos penales locales, que reconocen la violencia digital como un tipo de delito y se sanciona con multas económicas o penas de cárcel para quien viole la intimidad de las personas a través de medios digitales. Sin embargo, México aún no cuenta con la normativa suficiente y necesaria para la protección de derechos en materia de tecnologías digitales.

Definitivamente, es necesario que se produzca un andamiaje legislativo de normativas encaminadas a proporcionar garantías a la ciudadanía con respecto a la protección de su información personal en plataformas digitales, a fin de que las personas puedan utilizar la tecnología de manera segura y protegida. Para ello es necesario promover prácticas y comportamientos seguros en el uso de las herramientas digitales. Esto sólo se puede lograr con la implementación de políticas públicas y trabajos legislativos. Igualmente, se debe impulsar una cultura de concientización y divulgación para promover esquemas de protección de la información y de sus derechos, así como conocimientos tecnológicos básicos.

Referencias

- INAI (2017). Plataforma Nacional de Transparencia. Disponible en: https://www.rendiciondecuentas.org.mx/wp-content/uploads/2017/06/SAI_INFOMEX-Y-PLATAFORMA-NACIONAL_FINAL-5_Junio.pdf (consultada el 11 de septiembre de 2023).
- INEGI (2022) Encuesta Nacional sobre disponibilidad y uso de tecnologías de la información en los hogares (ENDUTIH) 2022. disponible en: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22.pdf (Consultada el 11 de septiembre de 2023)

- Morduchowicz, R. (2020) La ciudadanía digital como política pública en educación en América Latina. UNESCO Página electrónica: https://unesdoc.unesco.org/ark:/48223/pf0000376935
- Suprema Corte de Justicia de la Nación. (2011). Producción y Servicios. Los motivos usados por el Legislador que reformó y adicionó la Ley del Impuesto Especial Relativa, con vigencia a partir del dos mil diez, son razonables para justificar el gravamen a los Servicios de Telecomunicaciones y para Exentar el acceso a Internet. Semanario Judicial de la Federación. Disponible en: https://sjf2.scjn.gob.mx/detalle/tesis/162316

Ciudadanía e Identidad Digital: Protegiendo la privacidad en el mundo virtual

Josefina Román Vergara

En la era digital en la que vivimos, la ciudadanía e identidad digital se han convertido en conceptos fundamentales que impactan profundamente en la vida de las personas. La interconexión global y la creciente dependencia de la tecnología han dado lugar a nuevas formas de interactuar, comunicarse y participar en la sociedad.

Sin embargo, este avance también ha llevado consigo desafíos en cuanto a la privacidad y la seguridad de nuestros datos personales. En el presente texto, exploraremos la ciudadanía e identidad digital, las recomendaciones más relevantes para proteger la privacidad en el entorno digital, así como las mejores prácticas globales tendientes a garantizar los derechos digitales de las personas.

Ciudadanía e Identidad Digital: Definición y Significado

La ciudadanía digital se refiere a la participación activa y responsable de las y los individuos en el mundo digital. Al igual que en el mundo físico, donde la ciudadanía forma parte de una sociedad y tienen derechos y responsabilidades, en el entorno digital, las personas también forman parte de una comunidad en línea y deben

asumir responsabilidades similares. La identidad digital, por su parte, se compone de la información que una persona comparte en línea, incluyendo datos personales, actividades en redes sociales y más.

Carta de derechos de la persona digital. Código de buenas prácticas

En un mundo donde las interacciones en línea son cada vez más frecuentes y las transacciones digitales son moneda corriente, la ciudadanía e identidad digital son aspectos esenciales de la vida moderna. La identidad digital puede afectar la forma en que somos percibidos por otros, nuestras oportunidades laborales, nuestras relaciones sociales y más. Por lo tanto, es crucial considerar cómo proteger nuestra privacidad en este contexto.

La ciudadanía e identidad digital son aspectos clave de nuestra vida contemporánea. A medida que participamos en el mundo digital, es esencial tomar medidas para proteger nuestra privacidad y seguridad.

En este contexto, el 21 de agosto del 2023, la Comisión de Protección de Datos del Sistema Nacional de Transparencia, previo a la opinión de la sociedad civil, expertos y el Instituto Federal de Telecomunicaciones, se aprobó la "Carta de derechos de la persona digital: Código de buenas prácticas".

Este documento representa un esfuerzo conjunto para difundir los derechos que tiene cualquier persona usuaria de Internet, así como las buenas prácticas que podrían implementar instituciones públicas y privadas.

Cabe señalar que dicho documento no tiene efectos vinculantes, pues, como se ha dicho, no pretendemos ser legisladores; más bien, en ella se señalan los derechos básicos para el desarrollo de la persona digital y que ésta alcance plenamente la

realización de muchas de las actividades diarias ya sea de ocio, trabajo, gestiones administrativas, etc. y, por otro lado, señala las obligaciones que debe asumir el Estado y las buenas prácticas que podrían implementar las organizaciones para garantizar estos derechos.

Esta Carta nos ayuda a visualizar y crear conciencia y comprensión del impacto y consecuencias de los entornos y espacios digitales, adaptando los derechos humanos reconocidos en la Declaración Universal de Derechos Humanos, la Constitución Política de los Estados Unidos Mexicanos y los tratados y acuerdos internacionales de los que México forma parte, al entorno del mundo digital.

Resulta pues necesario y urgente, que todos los actores y las voces en el entorno digital, nos desarrollemos plenamente en este contexto, pero a su vez asumamos compromisos y obligaciones para una convivencia armónica. De esta suerte, el propósito de esta Carta es proveer un código de buenas prácticas, ajustado al marco de los Derechos Humanos internacionales para el cumplimiento y el avance de los Derechos Humanos en el ambiente online.

La Carta que se integra por 9 capítulos, a saber, Igualdad Digital, Libertades en el entorno digital, Derechos de seguridad social y protección de datos personales, Derechos de participación a la democracia y al buen gobierno digital, Derechos de las personas en situación de vulnerabilidad, Neuroderechos, Ética en el uso de inteligencia artificial, y Medios de defensa y Derechos de las víctimas del delito cibernético, violencia digital y violaciones de Derechos Humanos.

En suma, con este documento, México se constituye como uno de los precursores de la conversación sobre derechos digitales; ante la interconectividad y el acelerado uso de tecnologías de la información.

Ciudadanía digital, derechos y responsabilidades

Guillermo Antonio Tenorio Cueto

En su estupendo libro "Privacidad es poder", Carissa Veliz responde a una pregunta que se lanzó desde hace muchos años con el advenimiento acelerado de los nuevos desarrollos tecnológicos sobre si todavía existía la privacidad. Para ella, sigue existiendo y hay que defenderla bajo el nuevo ecosistema digital. Y es que hoy, al parecer, no existe un resquicio de nuestra vida que no sea susceptible de captura por los entornos digitales. Piense la persona lectora en las mediciones de sueño con los relojes inteligentes o en las veces en las que se limpia el piso de su casa con una aspiradora robot. Al parecer toda la vida humana está llamada a ser convertida en datos que nos perfilan, nos segmentan y predicen nuestro comportamiento.

¿Es inevitable este proceso? Me parece que sí. En los siguientes 10 años observaremos transformaciones más profundas vinculadas a los llamados metaversos de realidad inmersiva donde el llamado internet de los sentidos o de las emociones serán una realidad cotidiana. Probar un café colombiano (sin realmente probarlo) vivir la experiencia de una final de un mundial (sin realmente estar en ella) o escalar una montaña (con sudoración y cansancio incluidos) irán apoderándose cada vez más de nuestras rutinas alejando al ser humano de la realidad vivencial para sumergirlo cada día en una realidad virtual donde todo es medible, todo es predecible y donde sin duda, las sensaciones, reacciones y emociones serán medibles dentro del sistema.

Todos los casos narrados tienen un común denominador que es la obtención, manejo, transferencia y almacenamiento de los datos. En ese sentido es pertinente asumir que en la era digital nuestro comportamiento tiene que estar dirigido por

responsabilidades digitales. Esto implica no sólo estar consciente a quien le compartimos nuestros datos informándome adecuadamente de sus procesos, sino también respetar la privacidad de otros y desde luego el saber rechazar procesos de captura de datos cuando claramente son desproporcionados o abusivos. Es ahí donde la llamada ciudadanía digital comienza a forjarse.

La profunda responsabilidad de ella supone para todos nosotros la obligación a estar debidamente informados de los procesos que llevan a cabo todas las organizaciones que procesan datos emanados de nuestra vida privada. El informarnos debidamente de los términos contemplados en un aviso de privacidad ya no es un ejercicio del cual podamos evadirnos, sino que constituye el mecanismo idóneo para abandonar la victimización en el tratamiento de los datos. También es necesario que esta ciudadanía digital se robustezca a partir del establecimiento de medidas que tomamos para proteger nuestra información de posibles ataques o vulneraciones. La candidez de años pasados ya no tiene cabida dentro de un verdadero ciudadano digital.

La vida privada, como derecho que es, es una elección que supone el ensanchamiento o debilitamiento de la misma. Está en cada uno de nosotros tomar esa elección. El conocimiento pleno de lo que ocurrirá con nuestra información personal habilita necesariamente los posibles medios de defensa que tendremos en caso de que la misma sea vulnerada, maltratada o bien compartida de manera ilícita.

La ciudadanía digital supone conocer y ejercer mis derechos vinculados al desenvolvimiento que cada uno de nosotros tenemos en los entornos digitales.

Construir la ciudadanía digital a partir de un sano manejo de la información que compartimos permite expandir los horizontes de la misma a otras áreas del

comportamiento humano en aquellos entornos, pues derivado de la conciencia que supone la prevención y la reacción ante un mal manejo de la información, podemos construir una imagen digital responsable en todas sus facetas. La persona que asume, practica y vive ello, es capaz de relacionarse de manera oportuna, a partir del sano cuidado que hace de la información que comparte en línea. En otras palabras, la ética en el comportamiento digital se construye a partir de la forma en la que nosotros nos relacionamos con nuestra información y se proyecta en la forma en la que nos relacionamos con la información de los demás.

Sin conciencia en todo ello, difícilmente transitaremos hacia una sólida ciudadanía digital.

Referencias

- Castellanos, J. en Arellano Toledo, Wilma (2022) Derecho a la privacidad y derecho a la información desde una perspectiva comparada, Tirant lo Blanch, México.
- García, D. (2022) La libertad de expresión 4.0 en el sistema del Convenio de Derechos Humanos. Tirant Lo Blanch, Valencia.
- Quijano, C. (2022) Derecho a la privacidad en Internet. Tirant lo Blanch, México
- Tenorio, G. (2022) Asumamos la ciudadanía digital, El Economista. Consultado en: https://www.eleconomista.com.mx/opinion/Asumamos-la-ciudadania-digital-20220624-0033.html. Última visita el 1º de octubre de 2023.
- Veliz, C. (2021) Privacidad es poder, DEBATE, España.

Enumeración de los aspectos clave de la ciudadanía digital, como el respeto, la ética y la participación cívica en línea

Evelia Elizabeth Monribot Domínguez

La sociedad actual se caracteriza por ser dinámica, altamente tecnológica, centrada en la información, el conocimiento y la comunicación, pero en su lado opuesto muestra lazos frágiles, cambios constantes y falta de valores estables, lo que recuerda al concepto de sociedad líquida de Zygmunt Bauman. Este escenario exige que un ciudadano cuente con competencias básicas como aprender a resolver problemas, tomar decisiones, saber comunicarlas y participar.

Según la UNESCO, la ciudadanía digital se conforma a partir de un conjunto de habilidades con las cuales las personas usuarias pueden "acceder, recuperar, comprender, evaluar y utilizar, crear y compartir información de manera crítica, ética y eficaz para participar y comprometerse en actividades personales, profesionales y sociales". Además, no basta estar conectado a Internet, sino que implica contar con habilidades para saber navegar en la web y utilizarla de manera responsable.

Existen personas nativas e inmigrantes digitales. Marc Prensky define a los primeros como aquellos que están inmersos en la tecnología y que nacieron con ella y los inmigrantes son aquellos que les cuesta más adaptarse al mundo digital.

Continuando con la conceptualización de la UNESCO, existen dos grandes categorías de habilidades que hacen más amable y seguro el uso del ecosistema digital: las *fundamentales* y las *instrumentales*.

Las primeras promueven el uso reflexivo, ético y creativo de las tecnologías, teniendo como eje de formación al pensamiento crítico en el uso de la web,

construyendo así capacidades que implican analizar, inferir, resolver problemas, argumentar, tomar decisiones, comunicar, crear y usar ese pensamiento para mostrar una postura participativa con relación a los diversos temas que representan un desafío con el uso de Internet:

- Privacidad, identidad y huella digital.
- Confiabilidad y relevancia de la información.
- Funcionamiento de algoritmos y su incidencia en la vida diaria.
- Comunicación en el universo online, interacción en redes sociales.
- Creación de contenidos digitales con lenguaje eficiente y empático.
- Utilización de Internet para la participación en la resolución de problemas.

La segunda categoría corresponde a las habilidades digitales instrumentales que son aquellas que se encuentran vinculadas al manejo de las herramientas para tener la capacidad de responder a necesidades específicas y proponen un uso práctico de los dispositivos. Dentro de esta categoría las habilidades más frecuentes son:

- La generación y uso del correo electrónico.
- La utilización de hojas de cálculo y planillas.
- La realización de presentaciones digitales.
- La descarga e instalación de aplicaciones.

En suma, las habilidades digitales fundamentales colocan a los ciudadanos en mejores condiciones para entender la realidad. Esta alfabetización busca empoderar a las personas en todos los ámbitos de la vida, con el fin de que alcancen sus metas personales, sociales, educativas y ocupacionales y estén en condiciones de participar activamente en la sociedad. Se trata de un derecho básico en un mundo digital, que promueve la inclusión social de todas las naciones."

Desde el punto de vista educativo existen fundamentos que se pueden agrupar en tres grupos con el propósito de enseñar y aprender sobre tecnología y su utilización y son: respetar, educar y proteger.

Respetar

- Acceso digital: La ciudadanía digital comienza por la igualdad de derechos y acceso digitales.
- Etiqueta digital: Son los estándares de conducta o manera de proceder con medios electrónicos.
- Ley digital: Es fundamental que los usuarios entiendan cómo usar y compartir adecuadamente la propiedad digital de los demás.

Educar

- Comunicación digital: Elegir las herramientas adecuadas para un intercambio de información seguro y eficaz.
- Alfabetización digital: Se trata de cómo encontrar, evaluar y citar materiales digitales.
- Comercio digital: Se relaciona con la posibilidad de adquirir o vender bienes o servicios a través de las TIC, o incluso de asociarse empresarialmente a través de ellas.

Proteger

- Derechos y responsabilidades digitales: Los ciudadanos deben comprender sus derechos digitales básicos a la privacidad y libertad de expresión.
- Seguridad digital y seguridad: Los ciudadanos digitales necesitan saber cómo proteger su información.

- Salud y bienestar digital: Un aspecto importante de vivir en un mundo digital es saber cuándo desconectar a través de la priorización del tiempo y actividades en línea y fuera de ella.

Referencias

- Bauman, Z. (2015). *Modernidad líquida*. Fondo de Cultura Económica.
- Ciudadanía Digital - Concepto, valores, riesgos y beneficios. (2022). Concepto. https://concepto.de/ciudadania-digital/#ixzz8CZq3YLFo
- Delgado, P. (2020). *¿Somos o no ciudadanos digitales? La realidad de la conectividad en la pandemia*. Observatorio / Instituto Para El Futuro De La Educación. https://observatorio.tec.mx/edu-news/ciudadania-digital-pandemia/
- Expansión. (2022). ¿Qué es la ciudadanía digital y cuáles son sus características? Expansión. https://expansion.mx/tecnologia/2022/05/03/que-es-la-ciudadania-digital-y-cuales-son-sus-caracteristicas
- Prensky, M. (2010). Nativos e inmigrantes digitales. Obtenido de: https://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20(SEK).pdf
- Morduchowicz, Roxana. (2021). UNESCO - Competencias y habilidades digitales.
  Obtenido de: https://unesdoc.unesco.org/ark:/48223/pf0000380113.locale=en

Fomento de los beneficios de la Gobernanza Digital

Naldy Patricia Rodríguez Lagunes

En los últimos años se han incluido en el lenguaje de la administración pública diversos conceptos como el de gobernanza, gobierno abierto, gobierno digital, parlamento abierto, entre otros. Todos, con independencia de su materia específica, tienen la misma finalidad: satisfacer las necesidades de las personas, dar respuesta a problemas sociales y asegurar el respeto a los derechos humanos.

Gobernanza es una forma de gobierno cuya característica es que la toma de decisiones - acciones en materia de educación, salud, medio ambiente, impartición de justicia, entre otras- sean el resultado de un proceso de comunicación entre autoridad y población. Es el cambio de la relación vertical y de subordinación entre el gobierno y gobernados, por una horizontal y de colaboración de ambos actores. Si bien la autoridad ejecuta las políticas, éstas derivan del diálogo y vigilancia de la sociedad civil, es decir se trata de un empoderamiento ciudadano.

Podemos pensar en la gobernanza como el género (comunicación entre población y gobierno) y las políticas específicas como la especie, como los Consejos Consultivos de Gobierno Abierto (regulados por leyes de Transparencia), parlamento abierto (comunicación para proponer y vigilar la expedición de leyes) y Contralorías Ciudadanas (vigilancia de obras públicas y servicios), instrumentos que implican la gobernanza.

“El modelo de gobernanza para la administración pública comprende una idea de la democracia más amplia que la de cualquiera de los otros enfoques contemporáneos (Peters, 2004: 69)”.

Entonces, ¿Qué es la gobernanza digital?

Es innegable que las interacciones sociales son cada vez más comunes en el mundo digital: educación en línea, "home office", reuniones por medio de plataformas electrónicas, compras por internet, interacción en redes sociales y más, por lo que resulta difícil imaginar el mundo actual sin el uso de dispositivos inteligentes cuya función es acercar a las personas y satisfacer sus necesidades.

La gobernanza digital permite que la relación entre gobierno y población se dé a través de las Tecnologías de la Información y la Comunicación (TIC). Así, una ciudadana o ciudadano digital utiliza estas herramientas para participar en la toma de decisiones. Los beneficios son muchos: acceso a servicios públicos, mejora en los procesos gubernamentales, reducción de costos, eliminar la necesidad de transportarse, fomentar la transparencia y rendición de cuentas y facilitar la participación ciudadana. Todas las ramas de la administración pública pueden ser objeto de la gobernanza digital.

Vamos a los ejemplos, un estudiante se inscribe en su escuela de manera remota, digitalizando y remitiendo sus documentos, sin necesidad de acudir a la institución educativa. Un paciente puede programar y acceder a una consulta médica a través de una video llamada. Las partes en un juicio reciben notificaciones electrónicas y promueven actuaciones por la misma vía. Las autoridades ponen a disposición de la población cualquier tipo de trámite para acceder a los servicios que ofrecen. Los ciudadanos pueden interponer quejas, realizar denuncias, llevar a cabo pago de derechos y obligaciones. Cualquier persona está en posibilidad de consultar o requerir información pública a través de plataformas digitales.

De acuerdo con la Organización de las Naciones Unidas, el 40% de la población mundial no tiene acceso a utilizar una computadora. Entonces, el mayor problema al que nos enfrentamos es hacer llegar a la población, en especial a las zonas marginadas y rurales, el servicio de Internet, que éste sea gratuito y que las personas cuenten con dispositivos para utilizarlo, lo que obliga a las autoridades a adoptar medidas para expandir esta herramienta y explotar sus bondades. Sin embargo, con el trabajo conjunto entre población y gobierno, la gobernanza digital se convertirá en una de las principales herramientas para localizar, proponer soluciones y resolver problemas sociales, además de asegurar el ejercicio de los derechos humanos.

Referencias

- Juan y Giraldo Palacio, María Elena (2017). Gobernanza, rendición de cuentas y transparencia en los gobiernos locales. En Aguilera Hintel, Rina Marisa (Coordinadora). Aguilera Hintelholher, Transparencia y gobernanza en los gobiernos locales en México. La Biblioteca. Página 50. Recuperado el 18 de septiembre de 2023 en

  https://www.researchgate.net/profile/Maria-Giraldo-47/publication/348419802_Gobernanza_rendicion_de_cuentas_y_transparencia_en_los_gobiernos_locales/links/5ffe3e3745851553a03d5b87/Gobernanza-rendicion-de-cuentas-y-transparencia-en-los-gobiernos-locales.pdf

- García, M. (2021) *Transparencia, Acceso a la Información y Gobernanza Subnacional en México.* Gedisa, México.
- Peters, G. (2005) *Gobernanza y burocracia pública: ¿nuevas formas de democracia o nuevas formas de control?*, El Colegio de México, A.C., disponible en línea en el vínculo https://www.redalyc.org/pdf/599/59911177001.pdf.

- United Nations. (s. f.). *El papel de la gobernanza electrónica en la reducción de la brecha digital* | Naciones Unidas. https://www.un.org/es/chronicle/article/el-papel-de-la-gobernanza-electronica-en-la-reduccion-de-la-brecha-digital

Descripción de ejemplos de comportamientos positivos y negativos en línea.

Yolidabey Alvarado de la Cruz

El comportamiento en línea del usuario son los actos o acciones de las personas dentro de una web, chats, apps y redes sociales. Ante el constante uso de las tecnologías de la información, deben observarse reglas éticas en el entorno digital para generar interacciones respetuosas. A continuación, se destacan algunos ejemplos de los comportamientos positivos y negativos en línea.

Comportamientos positivos:

- Comunicación respetuosa en Internet: La comunicación que realizamos en línea con otras personas debe ser respetuosa, ya que, nuestros comentarios pueden incidir de forma positiva o negativa en su entorno familiar, social o laboral.
- Responsabilidad y cuidado en los contenidos que se comparten y promocionan: La información que difundimos debe estar fundamentada y contrastada antes de compartirla, porque difundir o replicar información en las redes sociales sin constatar su veracidad, puede causar daños a otras personas o cometerse delitos.
- Respeto a la privacidad de otras personas: Es importante cuidar la privacidad de las personas, pidiéndoles su autorización antes de subir o etiquetarlas en

una foto o un vídeo. Esta acción evita que alguna persona sea expuesta sin su consentimiento.

- Hacer uso responsable de las herramientas digitales: Es indispensable que se conozca el alcance de las herramientas digitales, los beneficios, pero también los perjuicios que pueden ocasionarse si se hace uso indebido de estas.
- Fomentar relaciones positivas: Las herramientas digitales permiten estar conectados con la comunidad, por lo que debemos respetar la diversidad de opiniones, evitando emitir comentarios agresivos que puedan afectar a terceras personas.

Comportamientos negativos:

- Violación a la privacidad: El derecho a la privacidad es aquel que toda persona tiene a separar aspectos de su vida privada del escrutinio público; sin embargo, con el uso de las nuevas tecnologías, todos nuestros movimientos como transacciones financieras, comunicaciones, etc., generan datos que quedan registrados en internet, por lo que, en ocasiones se obtienen, compran y venden sin el consentimiento del titular, lo cual constituye una violación a la privacidad.
- Noticias falsas: Son conocidas también como "Fake News" y se trata de información falsa o engañosa que se crea, presenta o divulga con el fin de engañar deliberadamente a la población y que puede causar un perjuicio público.
- El ciberacoso con intención sexual: Consiste en aquellas acciones preconcebidas que lleva a cabo un adulto a través de Internet para

ganarse la confianza de un o una menor de edad y obtener su propia satisfacción sexual mediante imágenes eróticas o pornográficas que consigue del o la menor.

- Suplantación de identidad: La suplantación de identidad consiste en hacerse pasar por otra persona en Internet. Se realiza accediendo a la cuenta del usuario o creando un perfil falso con la información personal de la persona suplantada.

Referencias

- García Ricci, D. (2013). Artículo 16 Constitucional. Derecho a la privacidad. Derechos Humanos En La Constitución. Comentarios de Jurisprudencia Constitucional e Interamericana, t. I, 1045–1079. Obtenido de: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf
- Equipo de Respuesta ante Incidentes y Seguridad Informática (CSIRT). (2021). Fake News, Los peligros de la desinformación. Obtenido de: https://www.csirt.gob.cl/media/2021/05/FAKE-NEWS-los peligros-de-la-desinformacio%CC%81n-ok-.pdf
- Panizo Galence, V. (2011). El ciber-acoso con intención sexual y el child-grooming. Quadernos de Criminología: Revista de Criminología y Ciencias Forenses, Obtenido de: https://dialnet.unirioja.es/descarga/articulo/3795512.pdf
- Universidad Veracruzana (2016.). Qué hacer ante una suplantación de identidad. Obtenido de: https://www.uv.mx/infosegura/general/conocimientos_suplantacion/.

Consejos para evaluar la calidad de la información en línea y evitar la difusión de noticias falsas

Oscar Raúl Puccinelli Parucci

La difusión de información falsa, incompleta, errónea, distorsionada o intrusiva es un fenómeno que se remonta a la antigüedad, pero que se ha disparado inusitadamente en el marco de la web 2.0, de las redes sociales, de la ingeniería social que se realiza a través de ellas, del big data y de la inteligencia artificial generativa.

Las fake news, en su acepción restringida, refieren a historias falsas que parecen ser noticias, difundidas en Internet u otros medios a sabiendas de su falsedad, con la finalidad de influir sobre la población o sobre ciertos sectores de ella con el objetivo de lograr que sus recipiendarios hagan dejen de hacer algo (p.ej., votar por alguien o no votar), generando beneficios para quienes realizan esa difusión o para quienes contratan esos servicios, que pueden ser de tipo personal (p.ej., la cancelación social de una persona), económico (desprestigiar a un producto de la competencia) o político (v.gr., ganar una elección).

En una acepción más amplia, las fake news comprenden a las difundidas con ignorancia de su falsedad y a las creadas en un contexto humorístico (donde se recurre a la parodia con fines de entretenimiento del receptor), pero nos centraremos en la primera tipología, por ser la más preocupante en clave de protección de los derechos humanos y del sistema democrático y estar actualmente potenciada por la inteligencia artificial generativa, que al permitir la creación directa de imágenes y sonidos cuya inautenticidad es prácticamente indetectable, conduce al muy preocupante fenómeno de las deepfakes.

La reciente irrupción de las fake news a escala mundial, se explica por factores tecnológicos, epistemológicos, económicos, afectivos y políticos que favorecen su difusión especialmente en las redes sociales a partir de mensajes dirigidos a personas influenciables escogidas a través técnicas de ingeniería social -que incluyen las de perfilado- a quienes se les ofrece información acorde con sus convicciones a través de "cascadas sociales" (cuando se sigue lo dicho o hecho por personas influyentes) y de la "polarización grupal" (cuando grupos se unen para defender una versión más extremista que la que sostenían).

Esta acuciante problemática ha merecido respuestas tanto del sector público (los Estados y la comunidad internacional) como del privado (la sociedad civil, las asociaciones, los proveedores de servicios de la sociedad de la información), dirigidas a detectar las informaciones falsas y operar sobre ellas y sus creadores y difusores. Desde luego, esa labor no es simple, pues determinar si una noticia es falsa depende de qué se considera verdadero en un momento y lugar determinado y lleva a considerar diversos factores –v.gr., el consenso social sobre algo, que puede variar con el tiempo, como les ha ocurrido históricamente a los "terraplanistas", otrora mayoritarios-. Además, a poco que se determine que una historia es falsa, se enfrentan, por un lado, diversos derechos fundamentales de las personas afectadas por la difusión de esas noticias, y por el otro, la libertad de expresión de sus emisores, que es una libertad preferida que protege incluso al discurso falso o erróneo. Esto obliga a realizar un prolija "ponderación de derechos", para lo cual se requiere atender a los subprincipios de adecuación, necesidad y proporcionalidad.

Las respuestas estatales a las fake news se centran en detectarlas y sancionar administrativa o penalmente sus autores o difusores, y también apuntan a la

concienciación de la población, intentando proteger la "identidad digital" de las personas y tender a la formación de una "ciudadanía digital" fuerte que empodere a los miembros de la sociedad.

En esa dirección, la comunidad internacional ha adoptado un sin número de documentos (motivados especialmente por los coletazos del escándalo Facebook-Cambridge Analytica en el marco del plebiscito por el Brexit y la elección de Donald Trump de 2016), entre los cuales se destacan los emitidos anualmente desde 2017 de manera conjunta por las relatorías especiales para la Libertad de Expresión de la ONU y de la OEA.

En cuanto a las respuestas privadas, los medios y las grandes plataformas en su mayoría crearon herramientas específicas en sus servicios, sitios web, blogs, extensiones para navegadores y aplicaciones, etiquetados de advertencia, eliminación de contenidos, suspensiones o eliminaciones de cuentas, etc. Por su parte, desde la sociedad civil se ofrecen servicios gratuitos, principalmente en Internet, donde se comprueba la calidad de los contenidos que pueden tener impacto social y se advierte sobre su posible falsedad.

Entre los distintos tipos de reacciones se encuentran las siguientes: a) respuestas de identificación de contenidos; b) respuestas legales y de políticas respecto de productores y distribuidores de información, que incluyen respuestas legislativas, prelegislativas y políticas; c) campañas nacionales e internacionales de "contra desinformación", a partir de la construcción de contra narrativas; d) respuestas específicamente dirigidas a una problemática determinada, como las relacionadas con las elecciones, y e) respuestas dentro de los procesos de producción y distribución de los servicios de la sociedad de la información, concretamente las

curatoriales (principalmente de políticas editoriales y de contenido que se reflejan en los denominados estándares de la comunidad); las técnicas y algorítmicas implementadas por las plataformas de publicación de contenidos, los motores de búsqueda y otros terceros relacionados (por ejemplo, complementos de navegador), las que pueden incluir métodos experimentales de investigación con Inteligencia Artificial para detectar y limitar la difusión de desinformación, o proporcionar contexto o información adicional sobre artículos y publicaciones individuales); las de desmonetización y desincentivación, que eliminan las ganancias de los sitios infractores de las políticas de publicación, y las de apoyo a las víctimas de la desinformación, a través de respuestas éticas, normativas y educativas, incluyendo pautas, recomendaciones, resoluciones, alfabetización mediática y de datos y etiquetados de credibilidad de contenidos.

En esta dirección, este tipo de actores adoptaron los siguientes tipos de medidas: a) acciones de sensibilización: a través de políticas incluso compartidas con otros actores, campañas de educación, alfabetización digital y mediática, etc., todas dirigidas a construir un ecosistema positivo frente a la desinformación, empoderando a quienes decidan combatirla y aportando estrategias eficaces frente al fenómeno; b) cambios en el código de las plataformas, incluidos los de algoritmos, mediante recomendaciones; c) cambios de política y acciones de moderación, tanto en el ámbito interno como en el externo para la eliminación de contenido reportado como ilegal o contrario a las pautas de la comunidad, y d) acciones de transparencia y relaciones públicas, que provean información sobre el funcionamiento de la plataforma y sobre cómo enfrentar el desafío de la desinformación

Finalmente, en cuanto a los consejos para la ciudadanía acerca de cómo detectar noticias falsas, cabe tener presente que la información falsa puede materializarse toda vez que se observen los siguientes contenidos:

a) Contenido satírico o paródico (publicación realizada con potencial engañoso, aunque no se busque causar daño con la publicación).

b) Conexiones falsas (títulos, imágenes y citas infieles al contenido).

c) Contenido engañoso (información distorsionada para crear una realidad diferente).

d) Contextualización falsa (información genuina ubicada en un contexto fáctico o temporal diferente al real).

e) Contenido impostor (se suplanta la identidad de las fuentes genuinas).

f) Contenido manipulado (información o imágenes manipulados para engañar); y

g) Contenido fabricado (contenido totalmente falso, diseñado para engañar y causar daño).

Teniendo presente estas diferentes posibilidades de manipulación, y en tren de diferenciar las noticias reales de las que no lo son, se aconseja poner atención a las siguientes características de la publicación dubitada:

I. Mensaje y lingüística:

a) Factualidad: información verificada e imparcial, uso de apellidos para citar;

b) Evidencia: datos estadísticos, basados en investigaciones;

c) Calidad del mensaje: estilo periodístico, editado y corregido,

d) Léxico y sintáctico: uso frecuente de "hoy" o del tiempo pasado,

e) Interés de actualidad: conflicto, interés humano, protagonismo.

II. Fuentes e intenciones:

a) Fuentes del contenido: fuentes contrastadas, citas y/o atribuciones, heterogeneidad de fuentes,

b) Pedigree: sitio u organización conocido o no, reputación del autor,

c) Independencia: afiliación del periodista a la organización.

III. Estructura:

a) URL: tipo de formato escogido en la registración,

b) Sección "Acerca de nosotros" (about us): claridad y verificabilidad de autores y editores, disponibilidad y formato de la sección "Contáctenos" (contact us), tipo y profesionalidad de los correos electrónicos y métodos de contactos de la organización profesional.

IV. La red:

a) Metadatos: Metadatos indicadores de autenticidad.

En la misma dirección, se sugiere poner especial atención a las siguientes claves para detectar fake news:

a) Tener cuidado con los titulares: Las noticias falsas a menudo tienen titulares llamativos en mayúsculas con signos de exclamación y, a menudo, información impactante e inaudita.

b) Examinar siempre la URL: Una dirección web falsa o una que copia una real puede indicar noticias falsas. Revisa bien los caracteres de la URL porque siempre son pequeños detalles.

c) Investigar la fuente de la noticia: especialmente antes de compartirla o difundirla. Algunas redes sociales como Facebook o Google han habilitado el botón Fact Checking para que los usuarios puedan certificar la veracidad de la información.

d) Prestar atención al formato: Muchos sitios de noticias falsas tienen errores ortográficos o diseños extraños.

e) Mirar de cerca las fotos y hacer una búsqueda de imágenes: Las noticias falsas a menudo contienen imágenes o videos manipulados, incluso basados en fotos auténticas tomadas fuera de contexto.

f) Consultar las fechas: Las noticias falsas pueden tener una línea de tiempo sin sentido o incluir fechas alteradas.

g) Verificar los hechos y las fuentes del autor para confirmar que son exactos: Si no se menciona la identidad de supuestos expertos, es posible que la noticia sea falsa.

h) Consultar otras noticias: Si ninguna otra fuente de noticias informa la misma historia, puede ser falsa.

i) Considerar que la historia puede ser una broma, especialmente cuando la fuente de la noticia es conocida por sus parodias: Si los detalles y el tono sugieren que ha sido escrito con humor, no se trata de una fake news.

j) Ser crítico: Algunas historias son falsas a propósito y con fines ocultos o maliciosos.

Referencias

- AECOC Innovation hub (2022) *Facebook lucha contra las fake news*. Asociación Española de Codificación Comercial. https://www.aecoc.es/innovation-hub-noticias/facebook-lucha-contra-las-fake-news/.
- Álvarez, R. y Del Campo, A. (2021), *Fake news en Internet: acciones y reacciones de tres plataformas*, Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Universidad de Palermo. https://www.palermo.edu/Archivos_content/2021/cele/papers/Fake-news-on-the-Internet-2021.pdf.
- Botero, C. (2017). *La regulación estatal de las llamadas "noticias falsas" desde la perspectiva del derecho a la libertad de expresión*, en "Libertad de expresión: A 30 años de la Opinión Consultiva sobre la colegiación obligatoria de periodistas". http://www.oas.org/es/cidh/expresion/docs/publicaciones/OC5_ESP.PDF.
- Broadband Commission for Sustainable Development (2021), *Balance Act: Countering Digital Disinformation while respecting Freedom of Expression.* UNESCO. https://en.unesco.org/publications/balanceact.
- Centro de Estudios sobre Libertad de Expresión y Acceso a la Información de la Universidad de Palermo (2021). *¿Las mentiras de los funcionarios públicos son*

insostenibles o tienen efectos trascendentales? Estudio sobre las obligaciones del Estado y sus funcionarios para prevenir la proliferación de la desinformación. https://www.palermo.edu/Archivos_content/2021/cele/papers/Disinformation-and-public-officials.pdf).

- Comisión Europea (2018) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "*Hacer frente a la desinformación en línea: un enfoque europeo*", COM/2018/236 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236).
- Comisión Europea (2018) Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "*Informe sobre la aplicación de la Comunicación Hacer frente a la desinformación en línea: un enfoque europeo*"; COM/2018/794 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0794.
- Comisión Europea (2022), *The Strengthened Code of Practice on Disinformation 2022*. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.
- Cortés, C. e Izasa, L.F. *The New Normal? Disinformation and Content Control on Social Media during COVID-19*". Centro de Estudios sobre Libertad de Expresión y Acceso a la Información de la Universidad de Palermo. https://www.palermo.edu/Archivos_content/2021/cele/papers/Disinformation-and-Content-Control.pdf.
- Khan, I. (2021). *Informe de la Relatoría Especial para la promoción y protección del derecho a la libertad de opinión y expresión "Disinformation and freedom of opinion and expression"*. A/HRC/47/25. https://undocs.org/en/A/HRC/47/25.

- Melo, V. (2022). *Fake News*. La Ley, Buenos Aires.
- Molina, M. D. et al (2021). *Las noticias falsas no son simplemente información falsa: una explicación conceptual y una taxonomía del contenido en línea*. American Behavioral Scientist, 2021, vol. 65(2) 180–212. https://doi.org/10.1177/0002764219878224https://journals.sagepub.com/doi/full/10.1177/0002764219878224
- Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión y otros (2017). *Declaración Conjunta sobre Libertad de Expresión y Fake News, Desinformación y Propaganda* y *Estándares sobre Desinformación y Propaganda.* https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y *Expresión y otros (2018). Declaración conjunta sobre la independencia y diversidad de los medios en la era digital.* https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión y otros (2019). *Vigésimo Aniversario de la Declaración Conjunta: Desafíos a la Libertad de Expresión en la Próxima Década.* https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión y otros (2020). *Declaración conjunta sobre libertad de expresión y elecciones en la era digital*.

https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.

- Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión y otros (2021) *Declaración conjunta sobre políticos y funcionarios públicos y la libertad de expresión*. https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión y otros (2022) *Declaración conjunta sobre libertad de expresión y justicia de género*. https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- Santos-D'Amorim, K. y Fernandes, M. K. (2021) *Misinformation, disinformation, and malinformation: clarifying the definitions and examples in disinfodemic times*. Revista electrónica de biblioteconomia e ciência da informação, vol. 26, e76900. https://www.redalyc.org/journal/147/14768130011/html.
- Wardle, C. y Derakhshan, H. (2017) *Trastorno de la información: hacia un marco interdisciplinario para la investigación y la formulación de políticas.* Consejo de Europa: https://www.europapress.es/sociedad/noticia-informe-encargado-consejo-europa-alerta-amenazarepresenta-desinformacion-mundo-20171031174624.html.

Discriminación tecnológica en el mundo de la ciudadanía digital, una contradicción lógica en la sociedad de la información y del conocimiento

Massimiliano Solazzi

La ciudadanía digital (o ciberciudadanía) es un concepto que refiere a un mundo en constante cambio, un campo de nuevos derechos en un entorno digital caracterizado por el rol hegemónico de las Tecnologías de la Información y la Comunicación (TIC), misma que se desarrolla en un marco contextual de la Sociedad de la Información y del Conocimiento (SIC). Este contexto dinámico de globalización nos ofrece cambios generacionales, tecnológicos, sociológicos, con una creciente interdependencia y comunicación entre los distintos países de todo el mundo, una nueva ciudadanía que forma parte de una sociedad más abierta e interconectada, donde se resalta el concepto polisémico, así como el papel crucial y destacado de la información siendo la materia prima para generar conocimientos.

En este escenario, las TIC han irrumpido para quedarse en la vida cotidiana de cada persona, una cultura digital que se desenvuelve en un cambio acelerado en los hábitos individuales y sociales, en el trabajo, en el estudio e investigación, hasta en los consumos, pero también en la forma de comunicarse y, por ende, en las relaciones interpersonales. Hablar de ciudadanía digital, es hablar de tecnología y de un espacio público como Internet, en el cual se generan un conjunto de derechos y responsabilidades que nos pertenecen a todas y todos, pero también al conjunto de normas de comportamiento relacionadas con la tecnología, un estudio complejo que abarca las áreas sociales, políticas y culturales.

Entre los años ochenta y noventa del siglo pasado, en todo el mundo asistimos a cambios sin precedentes a la estructura global de las sociedades, una etapa de la

historia definida como era digital, caracterizada por la revolución digital, con muchas nuevas oportunidades, pero también con muchos desafíos, un periodo que se extiende hasta la actualidad y que no permite vislumbrar su final. La inclusión de las TIC trae consigo un cambio paradigmático, con implícitos retos e impactos en el ámbito social, por ejemplo, en el acceso a la información, ahora con fuentes ilimitadas, generando y forjando ambientes de aprendizaje y de nuevos conocimientos mejorando así la comunicación, debido a su capacidad de reducir cualquier distancia geográfica. Una comunicación digital definida sin barreras, con la información digital considerada un insumo fundamental para mejorar la calidad de vida, impulsar la gestión social, la participación ciudadana, así como influir en la actividad económica y desarrollo de cualquier comunidad.

Una nueva cosmovisión administrativa que se refleja en los nuevos modelos de gobernanza y de gestión pública, así como la mejora de trámites burocráticos y de la calidad de los servicios, favoreciendo el proceso de evolución de la Administración Pública (AP), por ejemplo, a través del gobierno electrónico (en inglés, *e-government*) que tiene el propósito propiamente de mejorar la interacción entre ciudadanía y Estado.

De todo lo anterior, surge espontáneamente una interrogante ¿Cualquier persona tiene derecho de acceso a la tecnología? Bajo un punto de vista objetivo o normativo podríamos encontrar una respuesta en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), donde se establece que "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación (...)". Por lo tanto, cualquier persona tiene derecho a ser un ciudadano digital y, por ende, al uso de las tecnologías e Internet.

Desafortunadamente en pleno siglo XXI, asistimos al fenómeno de la Brecha Digital (BD) (en inglés, *digital divide*) y la discriminación tecnológica, una nueva expresión de la estratificación social del siglo XXI y un límite infranqueable para el ejercicio del Derecho de Acceso a la Información (DAI). Por su definición la BD es "la distancia social que separa a quienes tienen acceso a las TIC de aquellos que no la tienen" (Cortés, 2009), al respecto podemos entender que con la BD se profundiza la fragmentación de las desigualdades con respecto a la distribución de la riqueza y su efecto directo en la brecha salarial, así como la existencia de un desequilibrio provocado por las fracturas sociales en la desigualdad del acceso y uso de Internet, haciendo alusión a factores como educación, lenguaje y contenido, en este sentido, la BD como paradoja y contradicción lógica en la sociedad tecnológica y del conocimiento.

Concluyendo, la BD es una asimetría agrupada por diferentes criterios y ámbitos, un conjunto de factores o variables determinantes entre los cuales destacan el nivel económico y educativo, los aspectos geográficos y culturales, el género y la edad, entre otros. De lo anterior, la estratificación social en el mundo de la ciudadanía digital tiene como consecuencia una "estratificación digital", debemos recordar que, las TIC demandan un capital humano más calificado, conocimientos técnicos adecuados, accesibilidad a infraestructuras tecnológicas como, por ejemplo, dispositivos electrónicos y acceso a Internet.

Referencias

- Ávila, D. (2014) *El uso de las TICs en el entorno de la nueva gestión pública mexicana.* México: Andamios vol.11 no.24. Recuperado de

http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-00632014000100014

- Comisión Nacional de los Derechos Humanos (2015). Derecho al acceso y uso de las Tecnologías de la Información y la Comunicación. México: Instituto Nacional de Estudios Históricos de las Revoluciones de México. Recuperado de https://appweb.cndh.org.mx/biblioteca/archivos/pdfs/foll_DerAccesoUsoTIC.pdf
- Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 5 de febrero de 1917, última reforma publicada el 6 de junio de 2023. Recuperada de https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf
- Cortés, J. (2009), *Reseña de "¿Qué es la brecha digital?: una introducción al nuevo rostro de la desigualdad".* México: Investigación Bibliotecológica, UNAM. Recuperado de https://www.redalyc.org/pdf/590/59013270011.pdf
- Martínez, P. y Mesa, A. (s/f). *Gobierno electrónico y ciudadanía digital: una brecha entre políticas y oportunidades.* España: Asociación Española de Ciencia Política y de la Administración. Recuperado de https://aecpa.es/files/view/pdf/congress-papers/11-0/900/
- Olarte, S. (2017), *Brecha digital, pobreza y exclusión social.* España: Temas Laborales No. 138/2017. Recuperado de https://dialnet.unirioja.es/descarga/articulo/6552396.pdf
- Solazzi, M. (2023). *La nueva expresión de la estratificación social del siglo XXI: brecha digital y discriminación tecnológica una paradoja de la sociedad de la*

información y del conocimiento. México: Encrucijada Revista electrónica Del Centro De Estudios En Administración Pública, (45), 45–67. Recuperado de https://revistas.unam.mx/index.php/encrucijada/article/view/86151

Ciudadanía digital y protección de datos desde una perspectiva de la academia.

María de León Sigg

Las innovaciones tecnológicas nos han dado la oportunidad y, en ocasiones, también nos han obligado, a vivir, aprender y trabajar de manera digital (Baltazar-Vilchis, Sámano-Ángeles, Martínez-Garduño, & Garduño-Martínez, 2020). En este sentido, nos hemos convertido en ciudadanos digitales. Esta ciudadanía digital se ejerce en diferentes elementos: acceso, comercio, comunicación, alfabetización, etiqueta, ley, derechos y responsabilidades, salud y bienestar, así como seguridad e integridad (Capuno, y otros, 2022), y la pertenencia a ella debería regirse por principios análogos a aquellos encontrados en la ciudadanía tradicional, incluyendo el respeto, la amabilidad, la responsabilidad y la contribución positiva a la sociedad (Ôztûrk, 2021).

Además, se requiere un conjunto de habilidades fundamentales para desenvolverse de manera exitosa en el mundo digital. Entre ellas, destaca la capacidad de encontrar información en línea, detectar contenido sospechoso, prestar atención a las políticas de privacidad con la información recopilada en línea y usar de manera provechosa la tecnología para participar de forma responsable con otros (Hui & Campbell, 2018).

Sin embargo, la diversidad de perfiles e intereses de los ciudadanos digitales, la variedad de usos y tecnologías de información, la accesibilidad a las mismas y las diferentes legislaciones a nivel local, nacional e internacional, entre otros factores, complican el ejercicio de los derechos digitales y el desarrollo de habilidades suficientes para participar activamente en el entorno digital. Como resultado, es necesario replantear la regulación de la participación en sociedades digitales, así como en los enfoques y objetivos de la educación de los ciudadanos que forman parte de ellas (Pangrazio & Sefton-Green, 2021).

Por tanto, existen varias tareas que la academia debe abordar para fomentar la construcción de una buena ciudadanía digital que abarque el uso adecuado de las tecnologías de la información y la comunicación, y, por ende, la protección de los datos. Estas tareas incluyen el garantizar la instrucción adecuada en temas de ciudadanía digital, generar nuevo conocimiento sobre los elementos de la ciudadanía digital y vincular la academia con todos los agentes involucrados en este tema. Para asegurar la formación en temas de ciudadanía digital, la academia debe colaborar en la identificación de audiencias y sus necesidades específicas, definir contenidos pertinentes para comprender y aplicar los derechos y responsabilidades digitales, desarrollar métodos novedosos para desarrollar habilidades digitales y promover los valores necesarios para ser ciudadanos digitales ejemplares.

Asimismo, aún queda pendiente analizar la integración de los conceptos de ciudadanía digital en la formación de la niñez y juventud en la educación formal, así como también en la educación no formal para la alfabetización de adultos en estos temas. Además, es esencial considerar la formación de formadores e instructores con un fuerte sentido ético.

En cuanto a la generación de conocimiento, la academia tiene como tarea contribuir al desarrollo de tecnologías que mejoren la protección y el acceso a los datos, identificando sesgos que pueden afectar los derechos digitales. Finalmente, la academia debe colaborar de manera constante con la industria, el gobierno, otras instituciones educativas y con los organismos autónomos que trabajan en la regulación de la vida digital.

Referencias

- Baltazar-Vilchis, C. A., Sámano-Ángeles, A., Martínez-Garduño, Y., & Garduño-Martínez, A. (2020). Análisis de la ciudadanía digital en alumnos de una institución universitaria en épocas de pandemia. *In Crescendo, 11*(4), 425-441.
- Capuno, R., Suson, R., Suladay, D., Arnaiz, V., Villarin, I., & Jongoy, E. (2022). Digital citizenship in education and its implication. *World Journal on Educational Technology: Current Issues, 14*(2), 426-437.
- Hui, B., & Campbell, R. (2018). Discrepancy between Learning and Practicing Digital Citizenship. *Journal of Academic Ethics, 16*, 117–131.
- Ôztûrk, G. (2021). Digital citizenship and its teaching: A literature review. *Journal of Educational Technology and Online Learning, 4*(1), 31-45.
- Pangrazio, L., & Sefton-Green, J. (2021). Digital rights, digital citizenship and digital literacy: What's the difference? *Journal of new approaches in educational research, 10*(1), 15-27.

III. COMPORTAMIENTO ÉTICO EN LOS ENTORNOS DIGITALES

Contexto de responsabilidad en Línea

Erik Alejandro Cancino Torres

La tecnología y el internet como componentes fundamentales de la sociedad en las primeras dos décadas del siglo XXI trascienden a todos los ámbitos e influyen en todos los individuos en la construcción de ciudadanía digital, entendida ésta de acuerdo con Mossberger, Tolbert y McNeal (2007) como "la capacidad de participar en la sociedad en línea" (p.1). Sin embargo, ese no es el único y más importante significado que podemos otorgarle a esta condición social propia de aquellos que poseen un alto grado de alfabetización digital.

Al respecto, la UNESCO (2020) afirma que "la ciudadanía digital supone un conjunto de competencias que permite a las personas acceder, comprender, analizar y utilizar el entorno digital, de manera crítica, ética y creativa" (p.9). Por lo tanto, es oportuno destacar que caso contrario, quienes no poseen estas habilidades se les denomina inmigrantes digitales, es decir aquellas personas nacidas entre 1946 - 1960 y 1960 – 1980, y que forman parte de los segmentos generacionales denominados *baby boomers* y generación X, respectivamente; por su parte quienes nacieron inmersos en un entorno digitalizado y se advierten ellos mismos como entes naturales de este contexto electrónico, son los individuos que conforman las generaciones Y, Z y Alfa, nacidos entre 1980 y 2023.

Es por ello, que resulta imprescindible que las y los integrantes de la sociedad en su conjunto se autoevalúen y determinen de acuerdo con sus propias características, demográficas y psicográficas en qué supuesto se identifican, pues de ello dependerá el reconocimiento de sus propias habilidades para ejercer su categoría de

inmigrantes digitales o de ciudadanos digitales (nativos). Sin que ello implique una desvalorización o inferioridad por pertenecer a uno u otro segmento.

La pertinencia de lograr ese auto reconocimiento implica una gran responsabilidad, encaminada al pleno ejercicio del derecho de acceso a la información, establecido en el artículo 3° de la Ley Federal de Transparencia y Acceso a la Información, pues todos, sin excepción, en este país, sin importar nuestras habilidades cognitivas en el contexto tecnológico, estamos facultados para ejercer tan importante prerrogativa.

La ciudadanía o personas nativas digitales, a través del uso efectivo de plataformas electrónicas que, en los últimos años, se han dispuesto para garantizar el acceso a la información pública por parte de la ciudadanía, como es el caso de la Plataforma Nacional de Transparencia, "espacio en el que puedes consultar todo lo que producen o resguardan las instituciones públicas de México, y es también el medio para solicitarles información" (Sistema Nacional de Transparencia, 2023).

Y en su caso los inmigrantes digitales (*baby boomers* y generación X), mediante el impulso de una mayor auto alfabetización digital, para que la brecha tecnológica existente entre ambas clasificaciones no sea el impedimento ordinario para el ejercicio del derecho de acceso a la información de este importante y amplio segmento poblacional en México y en todo el mundo.

En ese sentido, destaca también por su importancia el cuidado y protección de los datos personales de quienes navegamos en la red, tanto ciudadanos digitales como inmigrantes digitales, en un contexto tan vulnerable, en el que la alta especialización de individuos en el conocimiento informático aplicado a actividades deshonestas nos enfrenta a riesgos que debemos de sortear con destreza y responsabilidad, para

que la huella digital que vamos dejando en cada una de las acciones que ejecutamos en la web, no sean empleadas en prácticas ilegales.

La capacidad de navegar a través de Internet sin ser vulnerado será siempre nuestro mayor propósito, siempre y cuando recordemos que la política de privacidad de nuestras redes sociales, la publicidad o privacidad de nuestros perfiles, la autorización al uso de nuestros datos personales y la protección de nuestras contraseñas o claves de acceso, se constituirán en todo momento como las mejores herramientas a nuestro favor para que el ejercicio pleno de nuestros derechos digitales se materialicen con la mayor legalidad, certeza y certidumbre.

Referencias

- Mossberger, K; Tolbert, C, & McNeal, R. (2007). *Ciudadanía digital: internet, Sociedad y participación*. Cambridge: Mit Press.
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2020). *Ciudadanía Digital. Curriculum para la formación docente*. Montevideo: UNESCO.
- Sistema Nacional de Transparencia (2023). Plataforma Nacional de Transparencia. México: SNT.

¿Cuáles son los principios éticos que deben regir el actuar en los entornos digitales?

Javier Brown César

Voy a comenzar mis reflexiones hablando de dos temas cruciales: la ciudadanía y la ética. La idea de ciudadanía nació, como la democracia, en El Ática, específicamente en Atenas en el siglo VI, A.C., gracias a las reformas de Solón y Clístenes.

Es de vital importancia destacar que el nacimiento de las instituciones democráticas se debió a las leyes (nomos). Las leyes son de tal importancia que quienes las crearon o reformaron fueron considerados como seres casi divinos. En el caso de Solón fue uno de los Siete Sabios. Gracias a las leyes, los griegos salieron del régimen de barbarie y crearon la democracia.

Muchas de las principales instituciones de la democracia ateniense, sobreviven y sustentan los sistemas democráticos contemporáneos. Ente estas instituciones encontramos:

La igualdad de todos ante la ley (isonomía).

La libertad para hablar en el espacio público sin restricciones (isegoría).

La rendición de cuentas.

Y como resultado principal la libertad (eleuthería).

Democracia y libertad, desde los atenienses, son un binomio indisoluble, que se mantiene al día de hoy.

Quiero destacar la importancia que daban los atenienses a la rendición de cuentas. Cualquier magistrado que no rendía cuentas era sujeto a la mayor pena posible,

después de la pena de muerte, en el derecho ático: el juicio de pérdida de derechos ciudadanos (atimía). Este juicio implicaba el destierro y la confiscación de los bienes de quien no rendía cuentas.

Una institución fundamental vinculada a la democracia y vital para su desarrollo y prosperidad es la ciudadanía. Aristóteles definió la ciudadanía como la capacidad para participar en cargos públicos. Hay que recordar que, en ese entonces, el gobierno mediante magistraturas se elegía por sorteo, en una Atenas con no más de 40 mil ciudadanos. Además, la ciudadanía original era excluyente: sólo para varones, atenienses, con un patrimonio mínimo para tener una hople (armadura básica del soldado hoplita).

En Atenas también nació la ética, gracias a las nuevas ideas de Sócrates. Antes de Sócrates ya había deliberaciones sobre el actuar humano, pero todas vinculadas a elementos o principios naturales. La ética que sistematiza Aristóteles consiste, en resumen, en la vida feliz gracias a la práctica de las virtudes intelectuales.

Después de esta introducción, me voy a referir al reto de la ciudadanía y de la ética en los entornos digitales.

He comenzado con los griegos, porque lo creado por ellos está en riesgo en el mundo digital. Actualizaré mis reflexiones al milenio que vivimos. Hoy estamos en lo que el filósofo subcoreano llama “El enjambre” metáfora expresiva que refleja el caso informativo que padecemos. En el enjambre todos se mueven febrilmente sin fin claro ni orientación fija. Todos trabajan para una reina ausente o más bien virtual.

El enjambre realiza la pesadilla de la biblioteca total de Jorge Luis Borges, la famosa Biblioteca de Babel, con su proliferación incesante de informaciones que generan

pasmo e incertidumbre. Estamos ante un fenómeno global que lleva a que las personas a una especie de laberinto en el que no tenemos el hilo de Ariadna, o sea, no tenemos forma de salir.

Este caos informativo, cito a Byung-Chul Han: "El socio deja paso al sólo. Lo que caracteriza la actual constitución social no es la multitud, sino más bien la soledad… Esa constitución está inmersa en una decadencia general de lo común y lo comunitario. Desaparece la solidaridad. La privatización se impone hasta en el alma. La erosión de lo comunitario hace cada vez menos probable una acción común" (p31-32). Y esto erosiona en sus bases a la democracia, que hoy, a decir de Chul Han, deviene infocracia y surge la infodemia: "El intento de combatir la infodemia con la verdad está… condenado al fracaso. Es resistente a la verdad" (p 42). Además: "El conocimiento digital hace que el discurso sea superfluo" (p. 61).

Voy a dejar aquí las citas para concentrarme en los retos de la ética de cara a la irreversible digitalización.

En primer lugar, la desigualdad, lo digital, como los sistemas sociales crea y profundiza las desigualdades. La brecha digital no se cierra sino se amplía y esto obliga a un proceso de ilustración colectiva en el que sólo puede haber participantes, porque el dirigismo autoritario aniquila el pensamiento libre.

En segundo lugar, la superficialidad. El mundo digital nos priva del fondo, es estético, pero no lógico. Crea apariencias, pero no permite que aflore la verdad o la oculta y es aquí donde las instituciones que revelan lo oculto, como el INAI, son vitales e indispensables, porque revelan las verdades de los arcanos gubernamentales.

En tercer lugar, el imperio de la mentira. Ya no hablamos más de post-verdad

En cuarto lugar, la ética. Hoy día la ética se ha recluido a códigos especializados, a mera deontología. Ha perdido así su raíz originaria, griega. *Ethos* para los griegos eran más que comportamientos, es la morada de la que nacen los actos buenos y nobles, virtuosos, en fin.

Hay que recuperar la ética individual y el imperativo de la constitución del sujeto. Tenemos que regresar al imperativo de convertir a la vida en una obra de arte, a pesar e incluso en contra de un mundo digital que trivializa al arte, deconstruye al sujeto y nos lleva a lo que hoy se llama posthumanismo.

La idea del ser humano y principalmente la idea del ser humano ilustrado que Kant fraseó como salir de la minoría de edad y aprender a saber por sí mismo, está en crisis. De ahí la crucialidad de recuperar la dinámica de la subjetivación, o sea, de la constitución del sujeto ético que lleva su vida a la máxima realización. Clave es en este sentido, garantizar el derecho a la identidad. En los sistemas democráticos esto conlleva la máxima transparencia del actuar del Estado, su sujeción a controles ciudadanos y su subordinación al poder de la ciudadanía; y, por otro lado, el celoso resguardo de datos personales de cualquier posible ataque o revelación imprudente.

Esto conlleva recuperar la capacidad del lenguaje para constituir un espacio público hoy degradado como en 1984 de Orwell. Termino con una cita de Byung-Chul Han y una reflexión posterior: “El vocabulario se reduce de forma radical y los matices lingüísticos se eliminan para impedir el pensamiento diferenciado. Los individuos quedan privados de la capacidad de reflejar en el pensamiento una realidad, un mundo, que no sea el del partido” (p. 80).

El ser humano habita en el lenguaje y el vaciamiento del lenguaje es un vaciamiento del yo. Debemos recuperar la palabra en el espacio público, luchar contra el imperio de la falsedad, y recuperar la democracia a partir de la revelación del poder. Volvemos a los griegos y a elementos constitutivos de la democracia original: el imperio de la ley y el que sea igual para todas y todos, la libertad para hablar en el espacio público y la sujeción de quienes gobiernan a un régimen de rendición de cuentas que los subordina y los amarra a una ciudadanía que debe salir de la indiferencia para regresar a la participación.

Los atenienses denominaban polites a quien era ciudadano y se interesaba por lo público; la contracara eran los ideotes: ciudadanos ajenos al espacio público. Fue la proliferación de ideotes lo que, junto con otros factores, llevó al colapso de la democracia; es la emergencia de sujetos que han vuelto a los imperativos éticos originales de constitución de la vida propia como obra de arte y que se activan, informan y participan, la base para que nuestras democracias sean sustentables.

¿Qué es la inteligencia artificial?

Norma Julieta del Río Venegas

Se trata de un conjunto de disciplinas de software, lógica, informática y filosofía que están destinadas a realizar funciones que se pensaba eran exclusivamente humanas, como percibir el significado en el lenguaje escrito o hablado, aprender, reconocer expresiones faciales; todo esto con la finalidad de resolver problemas ante condiciones dadas, de que contrasten información y lleven a cabo tareas lógicas.

De acuerdo con la Red Iberoamericana de Protección de Datos (RIPD), la inteligencia artificial (IA) en un concepto "sombrilla", pues incluye una variedad de técnicas

computacionales y procesos enfocados a mejorar la capacidad de las máquinas para realizar diferentes actividades, los que comprenden desde modelos algorítmicos, pasando por los sistemas de "machine learning". (Frontanilla, 2020)

Tipos de inteligencia artificial (INAI, 2022).

Máquinas reactivas: Son el tipo más básico de IA; son incapaces de evolucionar y se basan en decisiones sobre el presente (no tienen memoria).

Memoria limitada: A diferencia de las máquinas reactivas, aprenden del pasado utilizando experiencias previas propias o transmitidas y reglas de comportamiento e información de escenarios almacenados en su memoria para la toma de decisiones.

Autoconciencia: Sigue siendo una idea hipotética, pero constituye la fase final de los tipos de IA. Su objetivo es la creación de máquinas autoconscientes con capacidades para construir una representación de sí mismas, de su entorno y de su propio comportamiento.

Teoría de la mente: Presenta sistemas o máquinas cuya IA les permite entender cómo funciona su entorno, es decir, las personas, objetos y otros sistemas que los rodean. Además de dotar de medios para interpretar la expresión de pensamientos, emociones e ideas, así como para evaluar procesos de razonamiento y de conducta.

El INAI desarrolló las recomendaciones específicas para el tratamiento de datos personales derivado del uso de la inteligencia artificial, las cuales resaltan los riesgos y la responsabilidad proactiva en el diseño de tecnologías de la información con enfoque en este tipo de inteligencias, lo que permitirá, crear prácticas, procedimientos y herramientas de control de manera eficaz para el manejo y

cuidado de los datos personales de los usuarios que hacen o hagan uso de dichas tecnologías. (INAI, 2022)

Estas recomendaciones contemplan a aquellas tecnologías que manejan grandes cantidades de información y datos personales para operar, puesto que son estas esencialmente las que requieren el garantizar la seguridad de la información con observancia en la normativa en la materia. En México se discuten diversas iniciativas en materia de ciberseguridad y de regulación de inteligencia artificial. Recientemente la Cámara de Diputados recibió la iniciativa para la creación de la Ley para la regulación ética de la inteligencia artificial, la cual propone desarrollar un marco legal para México que regule el uso ético de la inteligencia artificial y la robótica.

La propuesta busca crear el Consejo Mexicano de Ética para la Inteligencia Artificial y Robótica (CMETIAR), conformado por representantes del gobierno, organismos de derechos humanos, el congreso y actores del sector privado.

El INAI se encuentra protegido a través de soluciones integrales (software y hardware), con un despliegue arquitectónico de seguridad en capas que permite mantener disponible y seguro el tráfico que viaja por los enlaces a internet, tanto de entrada como de salida, mediante el uso de dispositivos de nueva generación para el control de acceso, protección de intrusos y ataques de nueva generación. El instituto cuenta con un sistema de seguridad perimetral, el cual sirve para contener los intentos de ataques que son dirigidos a sus sistemas internos.

Referencias

- Frontanilla, M. C. (11 de junio de 2020). Estudio Codas. Obtenido de http://www.estudiocodas.com/2020/06/11/la-inteligencia-artificial-y-el-derecho/

- INAI. (1 de mayo de 2022). *Biblioteca digital INAI.* Obtenido de https://home.inai.org.mx/wpcontent/documentos/DocumentosSectorPublico/RecomendacionesPDP-IA.pdf

Comportamiento ético en el uso de la inteligencia artificial

Carlos Languendik Muñoz

La inteligencia artificial (IA) está teniendo un rápido desarrollo, además, un extraordinario progreso en años recientes, superando el desempeño humano en tareas complejas como reconocimiento de imágenes y juegos estratégicos. Sin embargo, la creciente integración e implementación de la IA en distintos ámbitos como salud, justicia y finanzas conlleva riesgos éticos significativos (Mittelstadt et al., 2016) que deben ser abordados.

Los sesgos algorítmicos, la falta de transparencia y las amenazas a la privacidad son los principales desafíos éticos en el uso de la AI; el primero de estos, atiende a la posibilidad de amplificar sesgos humanos, debido a que los algoritmos aprenden de datos que reflejan estereotipos y prejuicios sociales (Cath, 2018). Esto puede conducir a discriminación algorítmica en perjuicio de ciertos grupos.

Otro reto clave es la falta de transparencia en los sistemas de IA, lo que dificulta la evaluación de sus impactos éticos y sociales. También, el uso de IA presenta

amenazas a la privacidad, por la gran cantidad de datos personales que utilizan estos sistemas. Por último, la IA puede tener consecuencias negativas imprevistas al automatizar decisiones en ámbitos complejos como atención médica y justicia criminal.

Es por ello, que se deben explorar enfoques éticos, a efecto de promover un comportamiento ético en el desarrollo y uso de IA, en virtud, de que es crucial para que cumpla su potencial como herramienta que beneficie a la sociedad; por lo cual, una idea central, es el diseño centrado en humanos, toda vez que, antepone el bienestar de las personas en todas las etapas del ciclo de vida de los sistemas de IA (The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 2019).

De la misma forma, la gobernanza algorítmica participativa, aboga por la inclusión de múltiples actores en la evaluación de tecnologías de IA, como expertos, usuarios y grupos potencialmente afectados (Katzenbach, Ulbricht, 2019). Estos enfoques buscan asegurar que la IA respete la dignidad y derechos humanos.

A partir de este análisis, se proponen varias recomendaciones para promover un comportamiento ético en el uso de IA:

- Auditar algoritmos para detectar sesgos, evaluar sus impactos y aumentar la transparencia.
- Fomentar equipos de desarrollo de IA diversos e inclusivos.
- Adoptar regulaciones específicas para IA en ámbitos de alto impacto ético.
- Integrar consideraciones éticas en todas las etapas del diseño y despliegue de IA.
- Mejorar la educación sobre principios éticos de IA entre desarrolladores y usuarios.
- Promover la participación ciudadana en la gobernanza de IA.

- Priorizar la privacidad y autonomía de los individuos.

Conclusión

La IA presenta profundos desafíos éticos que deben abordarse para que esta tecnología se desarrolle de forma alineada con valores humanos. La adopción de enfoques éticos, regulaciones adecuadas y mejores prácticas por parte de múltiples actores puede promover un uso ético de la IA que maximice sus beneficios para la sociedad. Un comportamiento ético es la clave para que la IA cumpla su promesa de mejorar la vida humana.

Referencias

- Cath, C. (2018). Governing Artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A*, https://doi.org/10.1098/rsta.2018.0080
- IEEE Advancing Technology for Humanity (2019) "Ethical Aspects of Autonomous and Intelligent Systems "https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE19002.pdf
- Katzenbach, C., Ulbricht, L. (2019) "Algorithmic governance", *Internet Policy Review*, https://policyreview.info/concepts/algorithmic-governance
- Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The Ethics of Algorithms: Mapping the debate. *Big Data & Society*, https://doi.org/10.1177/2053951716679679

Explicación de la importancia de desarrollar habilidades de alfabetización mediática y digital

Naldy Patricia Rodríguez Lagunes

Hasta el 2022, se estima que en México existen 93.1 millones de personas usuarias de Internet, lo que representa -en general- el 78.6 % de la población de seis años o más. Datos que representan un aumento de 3.0 puntos porcentuales respecto a 2021. Estas estadísticas se modifican y reducen de acuerdo con el territorio. En el ámbito urbano, 83.8 % de la población de 6 años o más utilizó Internet, mientras que, en el ámbito rural, 62.3 % de la población usó esta herramienta, según la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares del INEGI de 2022. Es decir, existe aún una brecha digital que se mantiene en el país entre una región urbana y una rural.

La disparidad también se observa en la conformación del territorio: las entidades federativas que observaron los valores más altos en la proporción de usuarios de Internet fueron Baja California y Ciudad de México con un 89 %; mientras que los estados que registraron los valores más bajos fueron: Guerrero (67.5 %), Oaxaca (62.5 %) y Chiapas (56.7 %)

Las condiciones sociales aumentan la brecha de desigualdad. Durante la pandemia internacional generada por el COVID-19 se estima que en el país 26 millones de estudiantes menores de 16 años dejaron de asistir a la escuela durante un año y medio que no acudieron a las aulas de manera presencial. Una cifra mayor de las familias tuvo dificultades para darle seguimiento a las actividades escolares, lo que mermó los aprendizajes para la niñez mexicana.

En 2022, el grupo de edad que concentró el mayor porcentaje de personas usuarias de internet fue el de 18 a 24 años, con una participación de 95.1 por ciento. Siguieron los grupos de 25 a 34 años y de 12 a 17 años, con 92.8 y 92.4 %, respectivamente.

En cuarto lugar, se ubicó el grupo de las y los usuarios de 35 a 44 años, quienes registraron 87.1%, mientras que el grupo de personas que menos usó internet fue el de 55 o más años, con una participación de 47.6 %.

Hay que analizar dos indicadores más: El uso que le dan las personas al Internet y desde qué dispositivos se conectan.

Los tres principales medios para la conexión de personas usuarias a Internet: celular inteligente con 96 %, computadora portátil con 33.7 % y con televisor con acceso Internet 22.2 %.

Mientras que las principales actividades que realizan los usuarios de Internet son: para comunicarse (93.8 %), acceder a redes sociales (90.6 %) y el entretenimiento (89.6 %). La realización de pagos vía Internet incrementó de 18.3 %, en 2019, a 26.9 %, en 2022. En contraste con lo anterior, leer periódicos, revistas o libros disminuyó de 47.1 a 39.9 %, en el mismo periodo.

A la carencia de Internet y equipo tecnológico en zonas rurales de México, debemos sumarle la falta de alfabetización mediática de quienes son madres, padres o tutores, quienes en general tienen un menor uso de las plataformas digitales.

Como advierte la Corte Interamericana de los Derechos Humanos en el Caso Gomes Lund y otros vs. Brasil (2010) “en una sociedad democrática es indispensable que las autoridades estatales se rijan por el principio de máxima divulgación, el cual establece la presunción de que toda información es accesible”.

Los Estados tienen, como parte de sus obligaciones generales, un deber positivo de garantía con respecto a los individuos sometidos a su jurisdicción. Ello supone

tomar todas las medidas necesarias para remover los obstáculos que puedan existir para que los individuos puedan disfrutar de los derechos que la Convención Americana sobre Derechos Humanos reconoce. (Caso Cantos vs. Argentina, 2002)

México y sus familias viven realidades tan distintas y condiciones asimétricas que se hace necesario realizar acciones diferenciadas en cada región y zona geográfica para poder dar las herramientas idóneas a toda la población con la finalidad de que usen de manera correcta y eficiente las tecnologías de la información y la comunicación.

Como lo indican las estadísticas, los esfuerzos de la alfabetización digital deben enfocarse en los adultos que están en proceso de adaptación al cambio. Y en el caso de las infancias, más que enseñar a cómo usar los dispositivos y herramientas, se debe fomentar el buen uso de las plataformas para mitigar riesgos importantes.

Referencias

- Corte IDH, Caso Cantos vs. Argentina, (Fondo, Reparaciones y Costas), Sentencia de 28 de noviembre de 2002, Serie C No. 7, párr. 49. https://www.corteidh.or.cr/docs/casos/articulos/seriec_97_esp.pdf
- Corte IDH, Caso Claude Reyes y otros vs. Chile, (Fondo, Reparaciones y Costas), Sentencia de 19 de septiembre de 2006, Serie C No. 151, párr. 92 https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf
- INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares de 2022. https://www.inegi.org.mx/programas/dutih/2022/

Explicación de la importancia de desarrollar habilidades de alfabetización mediática y digital.

Julio César Bonilla Gutiérrez

La era contemporánea, caracterizada por su acelerado avance tecnológico, ha transformado drásticamente la manera en que comprendemos, consumimos y diseminamos la información. La omnipresencia de los dispositivos digitales y la revolución de las comunicaciones han generado un vasto mar de información. En este panorama, las habilidades de alfabetización mediática y digital emergen como fundamentales para el ciudadano del siglo XXI (Lee, 2019). Veamos por qué es esencial adentrarse en este tema.

1. Navegación Segura en el Entorno Digital, Fake News y fomento del pensamiento crítico

Con el Internet y los dispositivos inteligentes, en casi todos los rincones del mundo, nuestra exposición a la información y las interacciones digitales es constante. Sin embargo, este acceso sin restricciones también viene acompañado de muy diversos riesgos.

El ciberacoso, por ejemplo, ha emergido como una amenaza real en espacios digitales, afectando especialmente a mujeres, jóvenes y adolescentes. Las personas que no están familiarizadas con la etiqueta digital y las normas de seguridad pueden fácilmente ser víctimas de acoso o incluso convertirse en acosadores sin darse cuenta (Johnson & Turner, 2020). El ***phishing***, otro problema en auge, es una técnica de fraude en línea que engaña a las personas para que proporcionen información personal, como contraseñas o números de tarjeta de crédito. Contra este tipo de problemáticas originadas desde lo digital, pero, con claras y probadas consecuencias

en el mundo material, una adecuada alfabetización digital nos enseña a reconocer y evitar estas trampas (Johnson & Turner, 2020). La era de la información también ha sido apodada, lamentablemente, como la era de la desinformación. Las noticias falsas, o *fake news*, se han convertido en una herramienta propagandística y en ocasiones lucrativa. Estas noticias se diseñan para parecer creíbles, aprovechando formatos y estilos de medios legítimos para engañar al lector.

Una robusta alfabetización mediática capacita a las personas para identificar estas noticias. Nos enseña a verificar las fuentes, contrastar la información y reconocer los signos de contenido engañoso. Esta habilidad no sólo previene la propagación de falsedades, sino que también fomenta un público más informado y crítico (Smith, 2021).

La alfabetización mediática y digital va más allá de simplemente entender cómo funcionan los medios y las herramientas digitales. Se trata de desarrollar un pensamiento crítico sobre la información que consumimos. No todo contenido es neutral, y es esencial reconocer las agendas, los sesgos y las intenciones detrás de la información a la cual accedemos.

Las habilidades de análisis crítico permiten a los individuos examinar la validez, relevancia y confiabilidad de la información. Esto no sólo nos protege de la desinformación, sino que también fomenta una comprensión más profunda y matizada de los temas (Lee, 2019).

2. Participación Activa en la Sociedad Digital y Educación digital

El mundo digital ha traído consigo nuevas formas de participación cívica, social y política. Desde movimientos sociales que se organizan en línea hasta el acceso a servicios gubernamentales digitales, estar alfabetizado digitalmente significa tener una voz y poder en la sociedad actual.

Por ejemplo, muchas decisiones políticas y campañas de concienciación ahora tienen una fuerte presencia en línea. Aquellos que entienden cómo funcionan estos medios pueden participar más activamente, ya sea compartiendo información, votando en encuestas en línea o simplemente estando más informados sobre los temas actuales (González-Pérez & Hernández, 2022). El aprendizaje ya no está confinado a las aulas. Plataformas educativas en línea, MOOCs (cursos en línea masivos y abiertos) y tutoriales en línea han democratizado el acceso a la educación, quienes poseen habilidades digitales tienen a su alcance una variedad de recursos de aprendizaje, desde cursos de universidades prestigiosas hasta habilidades prácticas enseñadas por expertos.

La educación digital ofrece flexibilidad, permitiendo a las personas aprender a su propio ritmo y según sus propias necesidades. Sin embargo, es crucial tener las habilidades para discernir entre fuentes educativas de calidad y contenido menos confiable o engañoso (Martínez, 2020).

Conclusión

En un mundo interconectado, las habilidades de alfabetización mediática y digital ya no son opcionales, sino esenciales. Desde protegernos en el entorno digital hasta

participar activamente en nuestra sociedad y aprovechar oportunidades educativas, estas habilidades nos equipan para ser ciudadanas y ciudadanos informados, críticos y activos en el siglo XXI.

Referencias

- González-Pérez, A., & Hernández, B. (2022). *Sociedad digital: Un nuevo paradigma de aprendizaje y comunicación*. Ediciones Universidad de Barcelona.
- Johnson, R., & Turner, L. (2020). *Seguridad digital: Protección en la era cibernética*. Editorial Moderna.
- Lee, J. (2019). *Habilidades para la era digital: Alfabetización mediática en el siglo XXI*. Oxford University Press.
- Martínez, L. (2020). *Educación en línea: Oportunidades y retos del aprendizaje digita*l. Editorial Educativa.
- Smith, R. (2021). *Desinformación en la era digital: Identificar y combatir las fake news*. Cambridge Press.

Concienciación sobre la importancia de ser ciudadanos digitales responsables a nivel global

Julio César Bonilla Gutiérrez

En el marco de las "Jornadas Regionales de Transparencia Municipal, Ciudadanía Digital y Rendición de Cuentas", se abordaron temas fundamentales relacionados con la transformación digital y su impacto en la sociedad actual.

La importancia de la ciudadanía digital en la era de la inteligencia artificial fue resaltada destacando su papel en la construcción de entornos digitales seguros y en

la promoción de ventajas sociales susceptibles de compartirse en sus frutos, utilidad y beneficios.

En un mundo interconectado, es esencial entender los aspectos cruciales de la ciudadanía digital en la actualidad, donde la omnipresencia de diversas inteligencias artificiales exige la construcción de una ciudadanía digital responsable. Esta ciudadanía implica la adopción de derechos, responsabilidades y comportamientos apropiados en el entorno digital.

En este sentido, se plantean algunas de las ventajas significativas de construir una ciudadanía digital responsable:

Acceso a Información y Educación: La ciudadanía digital facilita el acceso a información en línea, fomentando la educación, investigación y aprendizaje continuo. Las tecnologías digitales permiten el acceso a conocimientos especializados y enriquecen la capacidad de tomar decisiones informadas.

Comunicación Global y Colaboración: La tecnología digital posibilita la comunicación y colaboración instantánea a nivel global, rompiendo barreras geográficas y fomentando la diversidad y la cooperación.

Oportunidades Educativas y Laborales: La ciudadanía digital amplía las oportunidades educativas y laborales al brindar acceso a programas educativos en línea y oportunidades de trabajo remoto.

Participación Ciudadana y Activismo: Las plataformas digitales permiten el activismo y la participación ciudadana, empoderando a las personas para expresar opiniones y promover causas sociales y políticas.

Construcción de Entornos Digitales Seguros: es de medular importancia garantizar entornos digitales seguros. Al respecto, algunos aspectos clave, son:

A) Protección de Privacidad y Datos Personales: Necesidad de regulaciones sólidas en materia de protección de datos y prácticas transparentes por parte de las empresas para proteger la privacidad de los usuarios.

B) Ciberseguridad y Prevención del Ciberacoso: Una ciudadanía digital responsable requiere medidas de seguridad en línea para prevenir amenazas como el ciberacoso y el robo de identidad. Las políticas públicas y la concientización son esenciales en esta área.

C) Alfabetización Digital y Pensamiento Crítico: La promoción de la alfabetización digital y el pensamiento crítico es fundamental para evaluar la información en línea y protegerse contra la manipulación y la desinformación.

D) Responsabilidad y Ética Digital: Fomentar una cultura digital ética es esencial para crear entornos digitales seguros. Los usuarios deben asumir la responsabilidad de sus acciones en línea y respetar los derechos de los demás.

Una ciudadanía digital responsable ofrece ventajas significativas y es esencial para construir entornos digitales seguros. La protección de la privacidad, la ciberseguridad, la alfabetización digital y la ética en línea son elementos fundamentales. Políticas públicas sólidas, educación y colaboración entre diversos actores son cruciales para lograr una ciudadanía digital responsable y entornos digitales seguros. En última instancia, la tecnología digital puede ser un espacio seguro y beneficioso para todos, impulsando el desarrollo y el bienestar de la sociedad.

IV. DERECHOS DIGITALES

Derechos fundamentales de las personas en el entorno digital

Joel A. Gómez Treviño

Lo que más define a la Web 2.0 es la explosión de contenido generado por el usuario (un proceso fundamental de abajo hacia arriba).

Desde el surgimiento de la Web 2.0, la convivencia humana se ha volcado en las redes sociales más populares. Según el popular sitio "Statista", a nivel mundial, Facebook tiene 2,958 millones de usuarios activos mensuales, YouTube 2,514 millones, WhatsApp 2,000 millones, Instagram 2,000 millones, TikTok 1,051 millones y Telegram 700 millones.

De acuerdo con la Organización de las Naciones Unidas (ONU), los derechos humanos deben respetarse tanto en línea como fuera de Internet. Las tecnologías digitales proporcionan nuevos medios para ejercer los derechos humanos, pero, con demasiada frecuencia, también se utilizan para violarlos. La protección de los datos y la privacidad, la identidad digital, el uso de tecnologías de vigilancia y la violencia y el acoso en línea son cuestiones que despiertan especial preocupación.

La hoja de ruta del secretario general de la ONU para la cooperación digital que garantiza la protección de los derechos humanos ha señalado el camino a seguir:

- ✓ Colocar los derechos humanos en el centro de los marcos normativos y la legislación sobre tecnologías digitales.
- ✓ Mayor orientación sobre la aplicación de estándares de derechos humanos en la era digital.
- ✓ Abordar las brechas de protección creadas por las tecnologías digitales en evolución.

- ✓ Desanimar los apagados generales de internet y el bloqueo y filtrado genérico de servicios.
- ✓ Leyes nacionales basadas en los derechos humanos y prácticas para la protección de la privacidad de los datos.
- ✓ Acciones claras y específicas de la empresa para proteger los derechos de privacidad y otros derechos humanos.
- ✓ Adoptar y mejorar salvaguardas relacionadas con la identidad digital.
- ✓ Proteger a las personas de vigilancia ilegal o innecesaria.
- ✓ Leyes y enfoques basados en los derechos humanos para abordar el contenido en línea ilegal y dañina.
- ✓ Garantizar espacios seguros en línea, marcos de gobernanza de contenido transparente y responsable que protejan la libertad de expresión, eviten prácticas excesivamente restrictivas y protejan a los más vulnerables.
- ✓ Orientación para todo el sistema de las Naciones Unidas sobre derechos humanos, debida diligencia y evaluaciones de impacto en el uso de nuevas tecnologías.

Los derechos humanos que estarán en mayor riesgo en Internet son los siguientes:

1. Derecho a la libertad de expresión.
2. Derecho a la igualdad y prohibición de la discriminación.
3. Libertad de trabajo o profesión.
4. Libertad de imprenta.
5. Libertad de asociación, reunión y manifestación.
6. Derecho a la inviolabilidad de las comunicaciones privadas.
7. Derecho a la protección de los datos personales.

8. Derecho a la identidad y al libre desarrollo de la personalidad.
9. Derecho al trabajo.
10. Derechos de los niños, niñas y adolescentes.

Dado que las redes sociales representan espacios de naturaleza privada, bajo el mando y control de una sola entidad privada, es fácil limitar o incluso anular los derechos de los usuarios. Será necesario un arduo trabajo conjunto entre los funcionarios de redes sociales, el sector de tecnologías de información, la academia, las ONG y el gobierno, para analizar desde una óptica de "múltiples partes interesadas" cuál será la mejor forma de regular o autorregular los espacios digitales de convivencia social, buscando siempre el respeto de los derechos humanos y derechos digitales de los usuarios.

Referencias

- Biggest social media platforms 2023 | Statista. (2023, 29 agosto). Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
- Gómez, J.A. (2022). Los Retos de los Derechos Humanos en el Metaverso. En A. Delgadillo (Coord.), *Tecnologías de Información* (1a ed., pp. 55 a 68). Editorial Comisión de Derechos Humanos del Estado de México. Obtenido de:https://www.codhem.org.mx/wpcontent/uploads/2023/01/Dialogos_DH_11_int_03_digital.pdf
- Tsekeris, C., & Katerelos, I. (2012). Web 2.0, complex networks and social dynamics. Contemporary Social Science, 7, 233 - 246. https://doi.org/10.1080/21582041.2012.721896

Derechos fundamentales de las personas en el entorno digital

Adrián Alcalá Méndez

En las recientes "Jornadas Regionales de Transparencia Municipal, de Ciudadanía Digital y Rendición de Cuentas" realizadas desde el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en colaboración con la Comisión de Vinculación, Promoción, Difusión y Comunicación Social del SNT, tuve el honor de participar en la Región Centro; Oaxaca, en el panel titulado "Ciudadanía Digital, entornos seguros, privacidad y protección de datos personales".

En primer lugar, es importante mencionar que, para entender las implicaciones de la Transparencia, la Ciudadanía Digital y la Rendición de Cuentas, debemos reconocer que, a través del tiempo, ha incrementado la comunicación entre personas en medios electrónicos, de ahí que, entre las actividades diarias, es innegable que el Gobierno y la sociedad requieran evolucionar y adaptarse a una nueva realidad.

Uno de los ejemplos más recientes, es la utilización de plataformas electrónicas en materia de educación, durante la emergencia sanitaria provocada por el COVID-19, estrategia implementada por el Gobierno Federal para dar continuidad a los ciclos escolares de educación básica.

Es por ello que el reconocimiento del derecho a la protección de los datos personales, en virtud de las interacciones en el entorno digital y, especialmente, aquellas relacionadas con las políticas públicas entre el Gobierno y ciudadanía a través de medios electrónicos, implican necesariamente el tratamiento de datos personales.

En este contexto, resulta importante destacar que, durante la sesión celebrada en octubre de 2022, la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, aprobó la "Carta de derechos de la persona en el entorno digital", la cual desde una perspectiva no vinculante, menciona los derechos con que cuenta una persona usuaria de las tecnologías de la información y las comunicaciones, las autoridades que te protegerían ante alguna vulneración derechos, así como la forma de mantener la titularidad y entera disponibilidad de sus datos personales.

También, establece los derechos de acceso universal a la Internet, a la identidad, a la no discriminación, a la privacidad, a la protección de datos personales y al uso de las redes sociales. Contiene interesantes innovaciones en la materia; como el derecho a la herencia digital, a la democracia y al buen gobierno digital. Entre los más relevantes destaca; el derecho a recibir información veraz, como la posibilidad de dar seguimiento libre y sin limitación alguna a las redes sociales de las y los servidores públicos, y de los derechos digitales frente a la Administración Pública, el cual garantiza a toda persona el acceso a los servicios públicos y a las relaciones digitales con las administraciones públicas.

Desde el INAI, realizamos herramientas que promueven una cultura de la protección de datos personales para el cumplimiento de la normativa en la materia. Ejemplo de ello, son las "Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital", documento que contiene una serie de consejos prácticos sobre configuraciones de seguridad, aplicaciones móviles y

software en general, útiles para que las personas usuarias mantengan segura su privacidad y sus datos personales en el entorno digital.

Finalmente, es importante referir que, con el incremento del uso de las nuevas tecnologías, es necesario replantearse los retos y desafíos que significa la protección de los datos personales, por lo que ampliar el marco normativo para garantizar mayor seguridad a las y los usuarios es una prioridad.

Enumeración de los derechos fundamentales de las personas en el entorno digital, como la libertad de expresión y la privacidad

Héctor Gúzman Rodríguez

La enumeración de los derechos fundamentales de las personales en el entorno digital presupone la aceptación de un concepto genérico relativo al ENTORNO DIGITAL.

Se propone retomar la definición prevista en el Reglamento de la de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares:

Es el ámbito conformado por la conjunción de hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permiten el intercambio o procesamiento informatizado o digitalizado de datos.

Lo anterior, sin perjuicio de efectuar una revisión o ampliación a la vista de la injerencia e importancia de la inteligencia artificial.

Se propone un segundo presupuesto general, relativo a la posición de los derechos en el entorno digital, frente a sus correlativos derechos en el entorno físico, a partir del cual debe quedar establecido que salvo modulación o adaptación al entorno

correspondiente (digital o físico) no existen bases objetivas para definir que existen mejores derechos o derechos de mayor importancia en uno u otro entorno.

Propuesta de enumeración de derechos:

Esta lista enunciativa tiene por objeto establecer los derechos que, en el marco del derecho digital, deben ser regulados para definir sus características particulares:

Derecho a la privacidad: uno de los derechos más cuestionados en los últimos tiempos, debido a la erosión e intrusión que diversas tecnologías y plataformas digitales han tenido sobre este derecho; es indispensable plantear que el derecho a la privacidad en el entorno digital sí existe, pero que debe ser protegido y construido en consideración de las características específicas de ese entorno, precisamente.

Derecho a la privacidad en entornos laborales: frente a la expansión de los modelos híbridos de trabajo, es necesario regular el equilibrio que debe existir entre el derecho del empleador a la supervisión de los empleados y el derecho de los empleados a no ser objeto de monitoreos desproporcionales.

Derecho a la protección de datos personales: ampliación de su protección mediante la actualización del marco jurídico vigente, para hacer frente al avance los últimos 15-20 años en el ámbito de la tecnología.

Acceso universal a Internet: reconocer y regular que, de cara a la década de 2030, no es concebible que toda la población de México no tenga acceso a un mínimo nivel

de servicio para acceder a Internet desde su casa o, al menos, desde un centro público existente en todas las poblaciones del país.

Derecho a la educación digital: reconocimiento del derecho a obtener educación para evitar en toda la población la "analfabetización digital" y la obligación del estado para brindar capacitación a los profesores encargados de las materias que se diseñen para garantizar este derecho; obligación de dotar a las instituciones públicas de los recursos necesarias para garantizar este derecho.

Derecho a la desconexión digital en entornos laborales: es necesario regular la forma en que los empleadores se comunican o supervisan a los empleados fuera del tiempo de trabajo que han acordado de forma legal o convencional, de forma que exista un respeto efectivo a su tiempo de descanso, permisos, vacaciones, así como de su intimidad personal y familiar; es necesario prohibir el despido por causas relacionadas con la desconexión digital a la que tienen derecho los trabajadores.

Derecho a la protección de los niños y niñas en Internet: regulación específica para la protección de menores de 14 años en el entorno digital.

Derecho a la protección de los adolescentes en Internet: regulación específica para la protección de mayores de 14 y menores de 18 años en el entorno digital; reconocimiento de la "emancipación digital" para personas de 14 a 17 años, reconociendo la madurez emocional e intelectual que les permite tomar decisiones informadas en el entorno digital, sin necesidad de la participación directa e inmediata de sus padres y tutores.

Información y privacidad frente a sistemas de videovigilancia, con particular relevancia en los sistemas públicos: cuyo objeto debe ser asegurar la proporcionalidad de la tecnología empleada para videovigilar espacios públicos y privados, así como el respeto de la expectativa razonable de privacidad en cada caso.

Derecho al olvido en búsquedas de Internet: derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Derecho a la información: equivalente al mismo derecho existente en el entorno físico.

Derecho a la libertad de expresión: equivalente al mismo derecho existente en el entorno físico.

Derecho al testamento digital o transmisión de última voluntad digital: posibilidad de acudir a los prestadores de servicios digitales para acceder a contenidos del fallecido e impartir las instrucciones que estimen oportunas sobre su utilización, destino o supresión (reconocido a las mismas personas que tendrían derechos equivalentes en el entorno físico).

Se propone definir las competencias de la Federación y de los Estados en cada caso, con el objeto de definir si el Congreso de la Unión (en primera instancia) tiene la facultad exclusiva para legislar sobre los derechos digitales de los ciudadanos.

Deberán definirse competencias existentes a favor de autoridades existentes y, en su caso, la necesidad de legislar sobre nuevas competencias y/o autoridades encargadas de la aplicación de una posible Ley Federal en Materia de Derechos Digitales.

Definición de una partida presupuestal para la protección y defensa de los derechos digitales de los ciudadanos.

Referencias

- Boletín Oficial del Estado (2018) *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* Disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
- Gobierno de España (2021) *Carta de Derechos Digitales.* Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Descripción de las responsabilidades de las personas en el entorno digital, como el respeto a los demás y la protección de la seguridad en línea

Salvador Romero Espinosa

El entorno digital, es un espacio público en el que las personas tenemos responsabilidades, ya que, si bien nos encontramos con un universo de oportunidades para ejercer una serie de derechos, también existe una gran cantidad de vulneraciones a las que nos exponemos en todo momento.

Pero, ¿qué entendemos por responsabilidad? Según la Real Academia Española, se entiende como la capacidad existente en todo sujeto activo de derecho para reconocer y aceptar las consecuencias de un hecho realizado libremente.

Así, para disfrutar de cualquier derecho es necesario que nuestros gobernantes y las instituciones cumplan con la responsabilidad de establecer todos los medios necesarios para garantizar su ejercicio, así como la educación adecuada para acceder fácilmente a él, con todas las implicaciones y repercusiones que ello puede tener.

Asimismo, tienen la responsabilidad de exigir el cumplimiento de estas garantías a los involucrados y deben de rendir cuentas ante los gobernados respecto a su actuar para garantizar los derechos**.**

Y es ahí, donde todos nos convertimos en corresponsables: la ciudadanía, las personas mayores de edad, niñas, niños y adolescencias, el sector privado, las instituciones, y, por supuesto, las autoridades, teniendo siempre presente que debemos velar especialmente por los derechos de las personas y sectores más vulnerables.

En ese sentido, todas las personas tenemos el derecho y la responsabilidad de educarnos y educar sobre y a través del entorno digital y de los nuevos derechos y las nuevas estructuras sociales, económicas y culturales que conlleva su utilización permanente.

Cabe señalar, que las reglas de convivencia en los entornos digitales, de origen, debieran ser las mismas que las que existen previstas en las normas legales y sociales de una comunidad, sin embargo, con el paso de los años y el aumento de la utilización de estos entornos, es importante que sí se establezcan algunas reglas enfocadas particularmente en la convivencia en dichas plataformas.

Para ello, me permito referir algunas de las que considero deben ser reconocidas como las responsabilidades más básicas que tenemos como usuarios de los entornos digitales:

- Respetar a otros usuarios, sin denigrar, ridiculizar o violentar las ideas o los derechos de las otras personas de ninguna manera al utilizar los medios digitales.
- Utilizar un lenguaje apropiado y conducta adecuada al interactuar.
- Hacer uso responsable de la información.
- Utilizar sanamente la tecnología para que no interfiera con nuestro bienestar físico y emocional.
- Denunciar cualquier mal uso de la tecnología a las autoridades.

Al tomar estas medidas estaremos colaborando a tener a una ciudanía digital comprometida, responsable y conscientes de sus derechos y obligaciones en el entorno digital.

Referencias

- Carta catalana por los derechos y las responsabilidades digitales (2019). Generalidad de Cataluña. Disponible en: https://politiquesdigitals.gencat.cat/web/.content/00-arbre/ciutadania/drets-responsabilitats-digitals/versio-es/Carta_v2_ES_.pdf

Desinformación y ciberseguridad

Anahiby Anyel Becerril Gil

En esta era de la digitalización[9] y la datificación, todo es dato (Simon, 2013), o lo será. Como individuos nos hemos despersonificado y cuantificado, evolucionado en datos; somos ceros y unos[10], dispersos en bases de datos nacionales e internacionales, y es a través del perfilamiento (*profiling*) y las predicciones que se realizan basadas en nuestra información, lo que nos define e identifica en el mundo digital. Nos hemos transformado de átomos a bits. Tenemos un legado de datos e información, del cual se conforma nuestro "yo" digital.

Nuestros datos personales no son estáticos, son dinámicos, se encuentran bajo constante revisión y análisis, además de constituir el recurso reutilizable del

[9] La digitalización, y la tecnología que lo hizo posible, ha hecho que las invasiones de la privacidad sean más penetrantes, generalizadas y prevalecientes, más frecuentes porque podemos obtener mucha más información sobre cualquier persona que antes, más generalizada porque la tecnología para las invasiones se encuentra disponible para casi todos y más prevalente porque todos somos una persona de interés para alguien que ahora puede saber fácilmente algo que era inaccesible antes de la era digital.

[10] Haciendo alusión al sistema binario, conformado por "1" y "0", el cual es empleado por las computadoras para almacenar información.

mercado digital. Son activos de información que no se deprecian, su riqueza y variedad permite su reutilización múltiple, generando más valor. Para un uso efectivo, deben llevar a la acción. El modelo DIKW (*Data*, *Information*, *Knowledge*, *Wisdom*), marca la pauta para su aprovechamiento. De esta forma, una vez recolectados los datos nos deben brindar información, la información que nos permita obtener conocimiento para finalmente, generar sabiduría que apoye la toma de decisiones. Los sujetos del ecosistema de datos[11] se encuentran en la búsqueda de esta sabiduría, porque, en el mejor de los casos, es la forma de entendernos y así ofrecernos servicios, desarrollar aplicaciones y enviarnos "sugerencias" para la toma de decisiones. En otros casos, esa información permite la manipulación[12] de individuos con múltiples finalidades (maliciosas o no).

1. Ciudadanía digital

La ciudadanía digital no sólo nos brinda derechos, sino que atribuye responsabilidades en el medio digital. Como ciudadanos digitales tenemos el compromiso de actuar de manera ética y segura en el entorno digital. Necesitamos el desarrollo de habilidades y capacidades en ciberseguridad, para lo cual, esta debe constituirse como un derecho accesible y asequible. Es nuestro deber involucrarnos en la protección de nuestra privacidad y datos personales, a la vez que hacemos uso de forma responsable de los medios y servicios digitales. También tenemos una corresponsabilidad en la cocreación de contenidos digitales, su consumo y acceso,

[11] Los individuos o grupos de individuos a quienes le conciernen los datos, aquellos que recolectan los datos, aquellos legalmente responsables de los datos, y varias partes potenciales que pueden emplearlos o desean usar estos.

[12] Un ejemplo sobre la preocupación sobre las capacidades manipuladoras en el comportamiento social y político de los individuos lo encontramos en la declaración del Comité de Ministros del Consejo de Europa adoptada el 13 de febrero de 2019. https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

así como de la comunicación y el discurso digital. Por ello se propone la construcción de un decálogo de la ciudadanía digital.

2. La ciberseguridad para proteger la ciudadanía digital

Internet y la diversidad de tecnologías digitales que se han desarrollado a partir de este nos han brindado nuevas oportunidades para desarrollar un sinfín de tareas en la esfera digital. No obstante, como cualquier otra tecnología, también han sido acompañadas de diversas amenazas, que parecieran ser cada vez más sofisticadas.

No cabe duda de que la tecnología tiene la capacidad de influenciar la opinión y comportamiento de las personas usuarias. En esto se han basado una diversidad de actores maliciosos para manipular e influir sus decisiones. En la actualidad vivimos en un "régimen de la información" (Han, 2022), en el cual su procesamiento mediante algoritmos y herramientas de Inteligencia Artificial (IA), determinan de modo decisivo los procesos sociales, económicos y políticos. La combinación de automatización, perfilamiento, targeting o micro-targeting y marketing ha tenido un impacto significativo en la opinión pública durante (Becerril, 2021), etapas fundamentales en las sociedades y democracias, además de facilitar el control sobre las personas y la vigilancia masiva, brindando información que no siempre es cierta. La IA altera fundamentalmente la forma en que los actores malintencionados la generan y difunden. Las redes automatizadas de cuentas falsas pueden enviar mensajes de forma más fácil, a mayor velocidad y escala, que las personas reales. Así, la desinformación se constituye como una de las principales amenazas que existe para socavar nuestra ciudadanía digital. Constituye una amenaza disruptiva de ciberseguridad, en donde los actores maliciosos hackean humanos en vez de sistemas.

Por ello la importancia en el desarrollo de capacidades para fomentar una ciudadanía digital racional que combata la desinformación. Es fundamental que la ciudadanía digital esté informada y adopte buenas prácticas de ciberseguridad, como:

- Educación y concientización: identificar las técnicas de ingeniería social y las tácticas de engaño como los bots, cyber-troops y cyborgs, así como su contenido falso o malicioso;
- Verificación de fuentes: antes de compartir o actuar sobre la información recibida. Además de utilizar fuentes confiables y contrastar la información, proporcionar información verificable y respaldada, fomentando la transparencia;
- Tecnología: desarrollar y utilizar herramientas de detección de contenido falso o engañoso, como sistemas de análisis de contenido y filtros antispam; etiquetas de verificación de la información que indiquen sí esta ha sido verificada; alertas de seguridad ante contenido falso o potencialmente malicioso;
- Colaboración: la colaboración entre diversos actores puede reducir la propagación de desinformación;
- Promoción de pensamiento crítico: como ciudadanos digitales tenemos el deber de cuestionar y analizar de forma crítica la información que circula en línea; entre otros.

Nosotros como ciudadanos digitales somos la primera línea de acción. En nosotros está el generar la conciencia sobre los riesgos y amenazas que existen en el entorno digital, así como la importancia de mantenernos protegidos en él.

Referencias

- Declaración del Comité de Ministros sobre las capacidades manipulativas de los procesos algorítmicos (2019). Consejo Europeo. Disponible en:

https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

- Becerril, A. (2021). Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. Revista IUS, pp. 9-34.
- Han, B.-C. (2022). Infocracia. La digitalización y la crisis de la democracia. Ciudad de México: Taurus.
- Simon, P. (2013). Too big to ignore: the business case for Big Data. Carolina del Norte: SAS Institute.

Descripción de cómo contribuir positivamente a la sociedad en línea y promover la igualdad y la inclusión.

Xóchitl Elizabeth Méndez Sánchez

La evolución de las Tecnologías de la Información y las Comunicaciones (TIC) ha favorecido la presencia de nuevas herramientas en Internet, representadas principalmente por la existencia de espacios abiertos de comunicación e interacción.

Uno de los principales elementos para garantizar el disfrute efectivo del derecho a la libertad de expresión en los entornos digitales, es el acceso a internet en igualdad de condiciones, que implica no sólo la posibilidad de contar con la infraestructura para acceder a dicho entorno, sino también la implementación de políticas públicas orientadas a erradicar la brecha digital, la enseñanza digital y la eliminación de barreras para su uso y acceso; de tal forma que se garantice el acceso y difusión de información en igualdad de condiciones, especialmente mediante acciones positivas dirigidas a las personas en situación de vulnerabilidad, sin que haya un trato discriminatorio a favor de ciertos contenidos en internet, en detrimento de aquellos difundidos por determinados sectores. (Maqueo, 2019)

Es así que el Internet se ha vuelto una poderosa herramienta para el ejercicio de los derechos humanos, se trata de un instrumento que modifica el rol que desempeñan los demás medios tradicionales de comunicación social, tales como la radio, la televisión e, incluso, los periódicos. (Maqueo, 2019)

El rápido avance de los medios electrónicos como el Internet constituye en los últimos años un sistema mundial de difusión y obtención de información en diversos ámbitos, incluso, del gobierno, ya que en la actualidad diversas autoridades han institucionalizado la posibilidad legal de que algunas gestiones los ciudadanos las puedan realizar a través de ese medio, en pro de la eficiencia de la prestación de servicios y el valor del tiempo.

Por lo que, una de las aplicaciones más importantes que han ofrecido las Tecnologías de la Información y Comunicación (TIC) es la posibilidad de modernizar la gestión pública a través de su uso para la prestación de servicios, el mejoramiento de la operación interna y el fortalecimiento de sus relaciones con ciudadanos, empresas y otros grupos sociales, lo que se ha denominado gobierno electrónico. (Coronado, 2021)

La evolución de las Tecnologías de la Información y las Comunicaciones, también ha favorecido la presencia de nuevas herramientas en Internet, como mecanismos que dan a conocer información, representadas principalmente por la existencia de espacios abiertos de comunicación e interacción; de manera que, se han vuelto uno de los principales elementos para garantizar la transparencia, el acceso a la información y el disfrute efectivo del derecho a la libertad de expresión en los

entornos digitales, además ha conseguido disminuir sustancialmente los costos de producción, distribución y uso de la información y los contenidos resultantes.

Actualmente, la participación activa y el creciente número de los usuarios de las redes sociales han producido importantes consecuencias en el ejercicio de algunos derechos fundamentales, tales como la libertad de expresión y el acceso a la información. Expresar las ideas en tiempo real se ha vuelto algo cotidiano; somos ciudadanas y ciudadanos inmersos en un mundo global donde constantemente nos relacionamos por medio de las distintas redes sociales, sobre todo cuando se difunden actividades personales derivadas del quehacer cotidiano: laboral, profesional, opiniones, reflexiones o alguna información de interés público.

De esta manera, poder tener acceso a la información, resulta un pilar esencial de la democracia que, además, de ser un derecho humano, puede servir como un instrumento esencial para el ejercicio de otros derechos fundamentales.

Referencias

- Coronado, J. (2021). Gobierno Electrónico. Hacia una tecnología humana, democrática y transparente. Universidad Continental. Obtenido de: https://repositorio.continental.edu.pe/bitstream/20.500.12394/10499/2/UC_Li_Gobierno_electronico_2021.pdf
- Maqueo,M(2019)https://www.sitios.scjn.gob.mx/cec/sites/default/files/publication/documents/201903/08_MAQUEO_La%20constitucion%20en%20la%20sociedad%20y%20economia%20digitales.pdf

¿Cómo considera que debe ser este engranaje de comunicación entre autoridades y sociedad civil para que la información llegue a la ciudadanía digital?

Amelia Lucia Martínez Portillo

La protección de datos personales y la privacidad de las personas se han convertido en dos derechos clave para el desarrollo de una sociedad que tiende aceleradamente a la digitalización en prácticamente todos los aspectos de la vida cotidiana, siendo así que, derivado de la pandemia por COVID, gran parte de nuestras actividades tuvieron que ser modificadas y adecuadas al impulso de las nuevas tecnologías que si bien ya estaban, se volvieron en algunos casos imprescindibles, desde cuestiones laborales, académicas, tramites gubernamentales, compras en línea y cuestiones recreativas.

El entorno digital puede implicar riesgos sin precedentes para la privacidad, dada la transferencia masiva de datos personales y la difusión, por parte de los titulares, de un volumen cada vez mayor de información a escala global en diversas plataformas, debilitando así el control sobre sus datos personales, lo cual amenaza las libertades civiles, económicas, la seguridad, salud, e incluso la integridad de las personas.

En ese sentido, las autoridades garantes del derecho a la protección de datos personales tenemos una ardua labor de concientizar a la ciudadanía de como ejercer sus derechos de manera adecuada, por lo que una tarea fundamental es la de sensibilizar a la ciudadanía acerca de su importancia, principalmente, en el mundo digital, además de conocer los mecanismos a través de los cuales los Organismos Garantes, integrantes del Sistema Nacional de Transparencia busca promover, difundir y promover este derecho humano de protección de datos personales, que

se encuentra legislados en nuestra Constitución y en diversos instrumentos internacionales.

Con este nuevo entorno digital en el que supone se abre un abanico de oportunidades, en temas económicos, nuevas formas de trabajo, formas de creación e innovación, se debe de tomar en cuenta que estos desarrollos tecnológicos y sociales también implican nuevos retos ya que no se cuenta con la tipicidad y marco legal actualizado a la nueva realidad. Por ello la importancia de generar las reformas necesarias para adecuar la normatividad.

En este contexto debemos recordar que el ser humano debe estar en el centro de la evolución tecnológica y no podemos perder el sentido de los derechos humanos por dar pasos a los avances tecnológicos. Los Organismos Garantes tenemos dentro de nuestras atribuciones la Protección de los Datos Personales, pero ante estos nuevos avances debemos sensibilizar a la ciudadanía sobre sus derechos digitales, pues tenemos la labor fundamental de concientizar a toda persona de como ejercerlos de manera adecuada.

Es por ello que promover la Carta de los derechos digitales de los usuarios y consumidores debe ser una de las acciones primordiales para potenciar y mejorar la calidad de vida de todo individuo, además de sensibilizar a la población sobre los riesgos y amenazas al momento de navegar en el mundo digital. “Hoy en día, la protección de datos personales cobra gran relevancia porque estamos trasladando toda la vida que teníamos en el mundo físico, al mundo digital, por el bien de todos y todas hagamos de la tecnología nuestra aliada y cuidemos nuestros datos personales en entornos digitales.”