



Mi Universidad
AVANCE TESIS

CAP 2.

Nombre del Alumno: Lionel Mollinedo Noyola.

Nombre del tema: Capítulo 2.

Nombre de la Materia: Taller de elaboración de tesis.

Maestra: Rosibel Carbajal de León

Licenciatura en Derecho

Noveno Cuatrimestre.

2.1 LA CREACIÓN DEL WORD WIDE WEB

El internet, tal como lo conocemos hoy, nació en un contexto de guerra y vigilancia. A finales de los años 60, “el gobierno de Estados Unidos creó ARPANET, una red de comunicación descentralizada pensada para resistir ataques durante la Guerra Fría”¹. Este proyecto militar evolucionó rápidamente y, en la década de los 80’s, con el desarrollo de protocolos como TCP/IP, se convirtió en una red global. La llegada de la World Wide Web en 1990, creada por Tim Berners-Lee, abrió las puertas a una nueva era de comunicación, conocimiento e interacción social sin fronteras.

Sin embargo, el internet también trajo consigo problemas que, hasta hoy en día nos afectan gravemente la vida de millones de personas alrededor del mundo, como por ejemplo la exposición masiva de datos personales, la vigilancia por parte de empresas y el gobierno, la desinformación de las personas, el cibercrimen que va en aumento y la creciente brecha digital. A medida que más personas compartían su información personal en línea ya fuera por correo, redes sociales o aplicaciones, surgió una necesidad urgente para proteger la privacidad e intimidad de este nuevo mundo, entorno a la era digital.

2.2 LA INTERVENCIÓN DE LA ERA DIGITAL EN MÉXICO.

En México, esta preocupación comenzó a tomar forma a nivel legal en el siglo XXI. Aunque la Constitución de 1917 ya garantizaba derechos como la inviolabilidad del domicilio, no existía una regulación específica para proteger los datos personales en el ámbito digital.

Sin embargo, fue hasta 2007 cuando se reformó el artículo 6º constitucional, reconociendo y valorando el derecho a la protección de datos personales, y más tarde, en 2010, se promulgó la Ley Federal de Protección de Datos Personales en

¹ Hafner Kette y Liyon Matthew, (Enero 1998) “*Donde los magos se quedan despiertos hasta tarde, Los orígenes del internet*” Siomon y Schuster.

Posesión de los Particulares (LFPDPPP). Esta legislación marcó un parteaguas, en el derecho a la privacidad digital, ya que estableció obligaciones claras para empresas privadas y otorgó a los ciudadanos los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) sobre su información personal.

De esta manera el avance continuó en 2011 con la reforma constitucional en materia de derechos humanos, causando que fortaleciera la protección legal del derecho a la privacidad al elevar a rango constitucional los tratados internacionales. Además, se creó el INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales), un organismo autónomo responsable, encargado de velar por estos derechos en el país.

No obstante, mientras que los retos persisten. En 2017, México se vio envuelto en un nuevo escándalo internacional cuando se reveló que el gobierno mexicano había adquirido y manipulado el software espía Pegasus para vigilar a periodistas, activistas y opositores políticos. Este caso destacó y puso en evidencia los peligros que implican la vigilancia digital y la falta de controles efectivos sobre las tecnologías de espionaje.

Hoy en día, mientras el internet sigue expandiéndose y en un constante cambio todos los aspectos de la vida humana, el derecho a la privacidad sigue enfrentando nuevos desafíos: la minería de datos por empresas tecnológicas, el uso de inteligencia artificial, el reconocimiento facial y la creciente presión por una legislación en ciberseguridad que equilibre protección y derechos humanos adecuados.

En definitiva, el derecho a la privacidad en la era digital en México es el resultado de una evolución y un crecimiento constante, impulsada tanto por los beneficios como por los peligros del internet. A pesar de que se han logrado importantes avances legales e institucionales, el verdadero reto está en mantener este derecho vigente y eficaz frente a una tecnología que cambia cada día con más frecuencia.

2.3 ANTECEDENTES DEL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL EN MÉXICO.

El derecho a la privacidad ha sido históricamente reconocido a lo largo del tiempo como un componente esencial de la dignidad humana y del desarrollo libre de la personalidad. Sin embargo, su configuración jurídica y social ha evolucionado significativamente con el avance de las tecnologías digitales. En el caso de México, la noción de privacidad comenzó a consolidarse formalmente en el marco constitucional a partir de las reformas en materia de derechos humanos y acceso a la información pública durante las primeras décadas del siglo XXI.

En la Constitución Política de los Estados Unidos Mexicanos, el artículo 16 reconoce explícitamente el derecho de toda persona a la protección de sus datos personales, incluyendo también el acceso, rectificación, cancelación y oposición (ARCO) respecto al tratamiento de su información personal.

Este reconocimiento fue establecido y reforzado por la reforma constitucional del 2009, que dio origen a la creación de instituciones especializadas como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Este órgano autónomo ha sido una pieza fundamental en la

promoción y defensa del derecho a la privacidad, más enfocado en un contexto marcado por la digitalización de la vida común y cotidiana.

A nivel legislativo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, promulgada en 2010, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en 2017, constituyen los marcos normativos fundamentales que rigen el uso de la información personal por parte de empresas y organismos públicos. Son estas leyes establecen principios como la licitud, finalidad, consentimiento, proporcionalidad y responsabilidad en el tratamiento de datos, así buscando equilibrar el uso de la tecnología con la garantía de los derechos principales.

Los antecedentes internacionales también han sido fundamental en la configuración del derecho a la privacidad en México. Tratados como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos, ambos donde el Estado mexicano forman parte, reconocen el derecho a la privacidad y a la protección frente a injerencias arbitrarias. Asimismo, modelos normativos como el Reglamento General de Protección de Datos de la Unión Europea (GDPR) han servido como referencia para dar más fuerza a los estándares de la protección que se puede aplicar en el país.

La creciente relevancia en el entorno digital, ha planteado nuevos desafíos. La masificación del uso de redes sociales, la recolección automatizada de información a través de algoritmos, la proliferación del comercio electrónico y la expansión de la vigilancia gubernamental han generado un nuevo escenario en el que el derecho a la privacidad se ve constantemente, perjudicado y amenazado. Esto ha llevado a una revisión crítica de los marcos legales existentes, así como a la necesidad de ampliar la educación digital de las personas que lo emplean y el conocimiento respecto a los riesgos que puede haber al manejo de la información personal en línea.

Asimismo, en este contexto, los antecedentes normativos, institucionales y sociales del derecho a la privacidad en México han sido fundamentales para comprender cómo ha ido evolucionando este derecho en este entorno digital. También permiten identificar las brechas actuales que existen entre la regulación y la práctica, principalmente en lo que respecta a la aplicación efectiva de las leyes y la capacidad de las personas para hacer que valgan sus derechos frente a sectores públicos y privados.

2.4 LA LLEGADA DEL NUEVO MUNDO DIGITAL EN TIEMPOS DE PANDEMIA COVID- 19.

La pandemia de COVID-19, que se expandió por todo el mundo en 2020, marco un punto de inflexión en la historia de la sociedad, esta pandemia global aceleró los medios digitales y transformó la manera en la que vivimos y nos comunicamos, la pandemia obligó a gobiernos y la ciudadanía a tomar medidas para aislar a las personas para la propagación del virus.²

Esta cuarentena desarrolló un papel fundamental para la tecnología, aceleró los medios digitales en el mundo, implementando el teletrabajo, la educación en línea y el comercio electrónico, esto se convirtió en herramientas esenciales para mantener la economía y el funcionamiento en la sociedad, sin embargo, la llegada del nuevo mundo digital en pandemia planteó tanto nuevas oportunidades para mejorar la eficiencia, la productividad y la accesibilidad, por otro lado también plantea desafíos en términos a la hora de la privacidad y seguridad de la información personal de las personas.

² Pablo Fanelli (2021). ¿La nueva realidad es el mundo de la soberanía digital?. XIV Jornadas de Sociología. Facultad de Ciencias Sociales

Después de la cuarentena de COVID-19, el futuro de la era digital se presenta lleno de oportunidades y desafíos, se tuvo que mejorar la infraestructura pública en las plataformas digitales para la identificación, pagos e intercambio de datos para acceder a los servicios públicos y privados, igual se tuvo en un avance en la IA acelerando el crecimiento en varios sectores digitales, sin embargo se hizo una brecha digital, generando desigualdad en el acceso a internet y habilidades digitales que hace que genere un desafío importante, especialmente en los países de poco ingreso

Asimismo, la digitalización puede impulsar el crecimiento económico y el empleo en países en desarrollo mejorando la calidad de vida, la era digital en pandemia también generó inclusión a servicios para las personas con capacidades diferentes o para aquellas que viven en áreas remotas y con menor acceso a los medios digitales.

2.5 LA ADAPTABILIDAD EN MÉXICO A LA ERA DIGITAL EN PANDEMIA COVID-19.

La educación en México experimentó un cambio radical debido a la pandemia de COVID-19. ³Se adoptó y adaptó la educación a distancia en diferentes modalidades en este periodo, lo que lleva a inferir que para la Ciudad de México se repitió el patrón. Pues durante este periodo, también fue necesario recurrir a esta forma de enseñanza. *cita.

Recordemos que cuando inició la pandemia por el coronavirus, clases y trabajos de oficina sufrieron cambios drásticos, y es por ello que diferentes sectores tuvieron que arriesgarse a probar cosas nuevas, y utilizar como aliado a las tecnologías, y

³ Pablo Fanelli (2021). ¿La nueva realidad es el mundo de la soberanía digital?. XIV Jornadas de Sociología. Facultad de Ciencias Sociales

sus derivados para la óptima realización de las actividades, para que no se creara un desequilibrio.

La pandemia de COVID-19, impactó significativamente en la educación, obligando a docentes y estudiantes a adaptarse rápidamente al uso de las TIC para llevar a cabo la enseñanza y el aprendizaje de manera remota.⁴ Es por ello que fue todo un desafío realizar este nuevo cambio a un panorama complicado, ya que se realizaron diferentes estrategias de salud, inclusive por las diversas muertes que hubieron y la falta de utilización de las tecnologías y sus herramientas.

La pandemia ha dejado una huella indeleble en la humanidad, también fue un catalizador de la digitalización. Ahora que la emergencia ha sido superada, es importante analizar cómo la tecnología durante este trance ha influido en nuestras vidas, tanto positiva como negativamente.

Durante más de tres años, uno de los aspectos relevantes de la transformación digital durante la pandemia fue su capacidad para mantenernos conectados y permitir la continuidad de diversas actividades económicas y sociales. La interacción entre humanos con dispositivos electrónicos y datos se normalizó.

La tecnología fue fundamental para el sostenimiento y la recuperación económica y ha permitido a gobiernos, empresas y trabajadores adaptarse a la nueva normalidad, incluido el teletrabajo y el comercio electrónico.⁵

La tecnología se convirtió en una herramienta indispensable para mantener la comunicación con nuestros familiares y amigos, trabajar de forma remota, continuar y reactivar las actividades económicas y proporcionar soluciones innovadoras a nuevos desafíos.

⁴ ABRIL 2018 EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL

⁵ IDEM.

2.6. IMPACTO DEL COVID-19 EN LA UTILIZACIÓN DE TECNOLOGÍAS EN AMÉRICA LATINA.

La pandemia del COVID-19 ha generado una recesión económica mundial de escasos precedentes. En el año 2020, el PIB real se contrajo en un 3.1% a escala global, generando cierre de empresas y aumentos de desempleo en todo el mundo, sin desmedro de lo cual su incidencia fue muy variable dependiendo de la región.,⁶ Por lo que derivado de esta problemática, se tuvieron que buscar diversas alternativas de crecimiento y de poder mejorar las cuestiones tecnológicas, lo cual fue un reto.

La digitalización ha concebido nuevas perspectiva dentro del mercado laboral como lo es enfoque estratégico, reducción de costo, transformación digital, realidad laboral, visión digital y aprendizaje y adaptación, además, estos elementos se han convertido en necesario e imprescindibles dentro de los espacios empresariales.*

Es importante señalar esto, porque desde que inicio la pandemia se causaron muchos estragos, además de ello se tuvieron que implementar estrategias importantes para buscar la solución alternativas necesarias para crear una digitalización correcta y adecuada para los mercados laborales y estudiantiles.

2.7 LA NUEVA REALIDAD DIGITAL POS-PANDEMIA.

El mundo post-pandemia es una oportunidad para las y los jóvenes debido a que están más habituados con el uso y apropiación de la tecnología de la información y

⁶ Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Transformación Digital e Inteligencia Artificial

la comunicación en el siglo XXI. Por lo tanto, desarrollar perfiles profesionales les permite adquirir habilidades y competencias digitales para buscar empleo vinculado a los sectores sobre la base de la innovación tecnológica. El desafío para las generaciones juveniles es crear emprendimientos digitales para canalizar la comercialización de productos de valor o la posibilidad de brindar servicios profesionales mediante los canales que ofrece la virtualidad.

El proceso de mediación tecnológica en la juventud genera la construcción de la identidad digital para ofrecer un perfil que brinde la posibilidad de satisfacer las necesidades del mercado laboral.

El perfil digital de las y los jóvenes permite interactuar sin la presencialidad mediante la incorporación de la tecnología a las actividades de la cotidianeidad.

La pandemia de COVID-19 ha tenido un impacto profundo en la forma en que las organizaciones operan y se relacionan con la tecnología. La crisis sanitaria global obligó a las empresas a reevaluar sus estrategias y adoptar rápidamente soluciones digitales para sobrevivir en un entorno altamente disruptivo.

Lo que antes se consideraba una opción estratégica se ha convertido en una necesidad urgente. En este artículo, exploramos cómo la transformación digital ha evolucionado en la era post-pandemia y cómo las empresas pueden aprovechar esta evolución para obtener una ventaja competitiva.

Antes de la pandemia, muchas empresas veían la transformación digital como una opción estratégica. Sin embargo, la crisis sanitaria global cambió esta percepción. Ahora, la digitalización se considera una necesidad urgente para sobrevivir y prosperar.

Las organizaciones han comprendido que la adopción de tecnologías digitales no solo mejora la eficiencia operativa, sino que también permite la innovación y la

resiliencia. Lo que antes se consideraba una opción estratégica se ha convertido en una necesidad urgente.

La pandemia ha acelerado la adopción de herramientas digitales en todas las áreas de negocio. Las empresas han implementado soluciones para el trabajo remoto, la automatización de procesos y la mejora de la experiencia del cliente. La colaboración en línea y las plataformas de comunicación se han convertido en la norma, y las organizaciones han aprendido a adaptarse rápidamente a los cambios tecnológicos.

El teletrabajo, que antes era una opción limitada a ciertos sectores, se ha convertido en una práctica común, y las herramientas de videoconferencia y gestión de proyectos han visto un aumento exponencial en su uso.

En la era post-pandemia, los datos se han convertido en un activo estratégico fundamental. Las organizaciones están recopilando y analizando datos para tomar decisiones informadas.

La inteligencia artificial y el aprendizaje automático se utilizan para predecir tendencias, personalizar ofertas y optimizar operaciones. Además, la gestión eficiente de datos es esencial para garantizar la privacidad y la seguridad. Las empresas que invierten en capacidades analíticas avanzadas están en una mejor posición para anticipar las necesidades del mercado y adaptarse rápidamente a los cambios.

La digitalización también ha aumentado los riesgos de ciberseguridad. Las empresas deben proteger sus datos y sistemas contra amenazas cada vez más sofisticadas. Las organizaciones deben invertir en medidas de seguridad robustas y capacitar a su personal para enfrentar estos desafíos. La ciberseguridad debe ser

una prioridad en la estrategia de transformación digital, con un enfoque en la implementación de tecnologías de protección avanzadas, como el cifrado de datos, la autenticación multifactor y la detección de intrusiones.

La era post-pandemia exige una mentalidad ágil y una adaptación constante. Las organizaciones que abrazan la transformación digital estarán mejor preparadas para enfrentar los desafíos futuros. La colaboración entre equipos, la inversión en habilidades digitales y la comprensión profunda de los datos serán clave para el éxito en esta nueva era.

La digitalización no solo ofrece una respuesta a las crisis actuales, sino que también abre un abanico de oportunidades para la innovación y el crecimiento sostenible. Las empresas que adoptan un enfoque proactivo y estratégico hacia la transformación digital no solo sobrevivirán, sino que prosperarán en el futuro digital.

2.8 ETAPA CONTEMPORANEA DE LA DIGITALIZACIÓN.

El derecho a la privacidad en México ha atravesado un proceso evolutivo profundo, que ha ido adaptándose a los cambios tecnológicos, sociales y políticos del país.⁷ Es importante destacar que los contextos sociales y el avance de las tecnologías digitales han crecido y con ello las necesidades, pero también delitos que tienen que ver con la tecnología.

El uso de herramientas tecnológicas por parte del Estado para fines de seguridad pública y control social no es nuevo, ya que existen diversas herramientas

⁷ Niño, G. D. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico.

novedosas, como el reconocimiento facial o inclusive el lector de huellas dactilares que buscan un registro de las personas para fines de recaudación de datos personales.

Históricamente, el uso de tecnologías para vigilar a la ciudadanía se ha justificado en nombre de la seguridad nacional, pero los casos recientes evidencian un abuso potencial, Ya que conforme van avanzando las nuevas tecnologías, van naciendo nuevos conflictos en cuestiones de virus que dañan software Y hardware, que día con día van alentando a nuevas amenazas que podrían y pueden dañar la privacidad de las personas a que se den a conocer sus datos.

2.9 EL CONTEXTO VIRTUAL.

Con el surgimiento de la informática, la capacidad de almacenamiento de información creció de manera descomunal, los sistemas contenían y contienen información relativa a datos personales.⁸

Con este tipo de avances en mayor escala de información, se busca que todo proceso digital se tenga que almacenar en diversos formatos para almacenamiento, ya que se busca un crecimiento constante en materia virtual de almacenaje de información, por lo que a través De los años ha ido avanzando la estructura del almacenamiento desde memorias, hasta la novedosa nube donde se pueden almacenar archivos, fotos y videos.

⁸ Mendoza, E. O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. RIUs, 12(41), 267-291

El área de la privacidad se ha convertido así en un lugar de confinamiento, y el propietario de un espacio privado es sentenciado, condenado y abandonado a su suerte: entregado a una situación caracterizada por la ausencia de oyentes ávidos por conseguir información y descubrir los secretos escondidos tras las murallas de su privacidad, para exponerlos al público y convertirlos en propiedad compartida, una propiedad que todos quieren compartir.

Las videoconferencias se institucionalizaron para reuniones de trabajo, sesiones educativas y consultas médicas, brindando una solución efectiva para superar las restricciones impuestas por el distanciamiento social. Emergió Zoom no sólo como plataforma para videoconectarnos, sino que la marca se integró a nuestro lenguaje habitual.⁹

En educación, el aprendizaje en línea se convirtió en la norma para estudiantes y profesores. El detalle fue que las tecnologías son herramientas complementarias de la enseñanza-aprendizaje, pero durante el confinamiento se convirtieron en sustitutas del aula, la interacción y la participación en clase. Conozco a muchos estudiantes que aborrecen y son alérgicos a las clases en línea después de haber estado cientos de horas y días frente a la luz azul-violeta de las pantallas.

La digitalización impulsó el comercio electrónico y la economía en línea. Empresas de todos los tamaños y sectores se vieron obligadas a adaptarse rápidamente, lo que llevó a un aumento significativo de las transacciones en línea.

2.10 CIBERSEGURIDAD

La privacidad y seguridad como derechos, son parte del relacionamiento diario de los seres humanos, en sus diferentes entornos, dígame entonces que son parte inherente y esencial a la vida y al desarrollo de la misma, estos derechos básicos,

⁹ Mayorga, T. C., Miguel, G., Duret, J., Joe, C., & Yarad, P. (2019). Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos. *Revista Científica Dominio de la ciencia*, 5(1), 518

no son iguales, aunque están estrechamente relacionados para hacer del entorno digital un espacio sólido en la protección del mismo, y de la protección de los datos de los usuarios de este espacio.

La ciberseguridad es esencial para salvaguardar nuestra identidad digital, así como para hacer transacciones electrónicas o uso de servicios digitales, entre los que se encuentran las redes sociales. Sin ciberseguridad los derechos a la protección de datos personales, a su privacidad y al secreto de las comunicaciones no serían posibles. Es decir, la ciberseguridad protege también estos derechos y permite hacerlos efectivos.

La ciberseguridad forma parte de la agenda mundial. En la actualidad, nadie se salva de ser víctima de un ciberataque; empresas, gobierno, hospitales, instituciones financieras, pymes y usuario final están expuestos a las amenazas que hay en la red. Entender la importancia de la seguridad informática nos da una perspectiva más amplia sobre las estrategias, planes y buenas prácticas que se deben implementar en las organizaciones.

Por ejemplo, si una persona se conecta a una red abierta sobre la que no tiene control, por ejemplo en un hotel, durante una conferencia o en el transporte público, se podría dar el caso de que sus comunicaciones y sus datos sean interceptados por un tercero malicioso ya que la información, al no haber sido cifrada, viaja sin protección.

Utilizar el cifrado puede ayudar a evitar este tipo de ciberataques, donde personas no autorizadas interceptan la comunicación de terceros y roban sus datos personales. “Según el Banco Interamericano de Desarrollo en 2020, en comparación con 2016, se produjeron avances en cuestiones tales como la confianza y seguridad en internet o la comprensión de la persona usuaria en la protección de la información personal”.¹⁰ Derivado de esto es necesario que

¹⁰ Mendoza, E. O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. RIUs, 12(41), 267-291.

implementemos el cifrado en cada oportunidad que tengamos, para con ello causar más seguridad en plataformas digitales.

2.12 GROOMING.

El grooming es una acción ilícita que consiste en que una persona adulta, ocultando su identidad o aparentando ser alguien de una edad parecida a la de su víctima busca ganarse la confianza de una niña, niño o adolescente con la finalidad de obtener fotografías o videos de contenido sexual de carácter sexual.¹¹

Con este material, El adulto solicita más fotografías, videos o encuentros con fines sexuales, amenazando a la niña, niño o adolescente con publicar sus fotografías y videos o contar sus conversaciones. En caso de que una niña, un niño o adolescente sea víctima de grooming, se debe denunciar ante las autoridades competentes ya que se trata de una acción ilícita.

Por tanto, sus padres o tutores, así como otras personas que puedan tener conocimiento de este tipo de acciones, deben ofrecer ayuda a los menores para evitar que puedan sufrir daños. Las redes sociales y otros servicios digitales son utilizados por actores maliciosos con la finalidad de llevar a cabo este tipo de acciones y causar daños a sus víctimas.

2.13 SEXTING

El sexting es una acción que puede causar daños a una niña, un niño o adolescente e incluso ser utilizada posteriormente con fines ilícitos.¹² El riesgo es hacer que las víctimas se sientan avergonzadas para que el delincuente las amenace con hacer público el material sexual, causando un grave daño a la persona. Las fotografías,

¹¹ Posada, M. R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Revista Nuevo Foro Penal, 13(88), 72-112.

¹² IDEM

videos o audios pueden ser utilizados posteriormente para amenazar o coaccionar a la víctima. Si un menor recibe una fotografía, video o audio de este tipo, la recomendación es que nunca la envíe o comparta de alguna manera en redes sociales u otros servicios digitales, por ejemplo, en páginas web, blogs o redes sociales

2.14 FAKE NEWS.

Las noticias falsas o fake news no son algo nuevo, pero últimamente, gracias al auge de las redes sociales, se han convertido en un gran riesgo para las personas poco informadas que no hacen un uso seguro de los servicios digitales disponibles en internet.¹³ Durante la pandemia por Covid-19 las fake news fueron usadas por personas maliciosas con la finalidad de engañar a una multitud de víctimas.

Relacionado con este tipo de manipulación masiva también existen las deep fakes, que son videos manipulados para hacer creer a los usuarios que ven a una determinada persona, tanto si es anónima como si es personaje público, realizando declaraciones o acciones que nunca ocurrieron.

2.15 PROTECCIÓN DE DATOS PERSONALES.

La protección de los datos personales se considera un derecho “moderno” y activo, que establece un sistema de control mediante mecanismos que protegen a los ciudadanos cuando sus datos personales sean objeto manipulación indebida. El derecho a la protección de los datos personales es más amplio que el derecho al respeto de la vida privada, ya que entra en juego siempre que se traten datos personales

¹³ IDEM.

Debe de tenerse presente que tanto el adelanto tecnológico aunado a la economía y socialización digital, han traído entre muchas otras consecuencias que requieren la protección de los datos desde el entorno jurídico, estas normativas nacen con un objetivo de proteger información.

2.15.1 PROTECCIÓN PARA NIÑAS, NIÑOS Y ADOLESCENTES.

Según la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2022, el 92.4 por ciento de las personas entre 12 a 17 años son personas usuarias de internet (Instituto Nacional de Estadística y Geografía, 2022), representando un aumento significativo desde la pandemia.¹⁴ La privacidad y protección de datos de niños, niñas y adolescentes en el entorno digital se ha convertido en un tema de creciente preocupación debido a la masificación de la tecnología y el incremento que tuvo a partir de 2020.

Los niños, niñas y adolescentes están inmersos en un entorno digital desde una edad, cada vez más temprana, lo que los expone a múltiples riesgos relacionados con la privacidad de sus datos personales. La recopilación de datos comienza muchas veces con el consentimiento de los padres, pero a menudo éstos no comprenden completamente las implicaciones a largo plazo.

El mal uso de los datos personales de niños, niñas y adolescentes puede acarrear graves consecuencias. Entre los riesgos más preocupantes se encuentran las diferentes formas de ciberacoso, el grooming y el robo de identidad. La protección de datos y la privacidad de niños, niñas y adolescentes es un desafío multifacético que requiere la colaboración de padres, educadores, legisladores y empresas tecnológicas. En un entorno digital cada vez más complejo, es primordial adoptar un enfoque proactivo para educar y proteger a los jóvenes.

¹⁴ Zuazo, N. (2018). Los dueños de Internet como nos dominan los gigantes de la tecnología y que hacer para cambiarlo. Editor digital: Un_Tal_Lucas.

2.16 VIOLENCIA DIGITAL.

La violencia digital ha sido uno de los fenómenos que también se ha acrecentado con la intensificación del uso de tecnologías. La Era Digital ha traído consigo múltiples beneficios, indudablemente, pero también problemas y riesgos, entre los que destacan la necesidad de fortalecer la protección de los datos personales y la privacidad de las personas.

A su vez, a través del caso emblemático de la activista Olimpia Corral Melo, quien después de ser víctima de la difusión de un video íntimo sin su consentimiento, se logró que se expidiera la ley que se conoce como Ley Olimpia.

2.17 PRIVACIDAD EN LAS REDES SOCIALES.

Una de las consecuencias de la evolución de la tecnología y los servicios digitales es el cambio constante en la privacidad de las personas. Las redes sociales son un claro ejemplo de esta situación. A principios de este siglo aparecieron las primeras redes sociales. El significado y alcance de los derechos a la protección de datos personales y a la privacidad también evolucionó de manera constante y rápida a la par de estas tecnologías.¹⁵

Para evitar sufrir la vulneración de los derechos a la protección de datos y a la privacidad es importante conocer qué redes sociales y servicios digitales se utilizan a diario y quién las proporciona. Es indispensable usar responsablemente las redes sociales y otros servicios digitales, evitar proporcionar más datos personales de los que son necesarios y mantenernos atentos para evitar daños u otras consecuencias que pudiera tener un uso ilícito o malicioso de nuestra información personas.

2.18 TRATAMIENTO DE DATOS PERSONALES

Cuando las redes sociales tratan datos personales, se producen también tratamientos que son invisibles para estas. Las redes sociales pueden obtener datos personales a partir de otros datos personales, lo que se conoce también como inferir datos personales. Cuando se infieren datos personales lo que ocurre es que el

¹⁵ Zuboff, S. (2021). La era del capitalismo de la vigilancia. (A. Santos, Trad.) Paidós.

responsable del tratamiento, a partir de otros datos personales que han sido proporcionados o ha obtenido de la persona usuaria de la red social, genera nuevos datos personales.

Los algoritmos utilizan datos personales para generar un modelo de algún aspecto del mundo y aplican este modelo a nuevos datos para hacer predicciones. ¹⁶Estos algoritmos se utilizan, por ejemplo, en el caso de la inteligencia artificial para la toma de decisiones relativas a determinar qué contenido o información se muestra a unas personas usuarias de una red social y a otras.

En el ámbito de las redes sociales otro riesgo posible, derivado de un tratamiento de datos personales que sería ilícito por vulnerar los principios de la protección de datos, en particular la finalidad del tratamiento sería “la posible manipulación de los usuarios”.

Los usuarios de redes sociales tienen derechos cuando se tratan sus datos personales, pero es necesario ver a qué legislación está sujeta la red social o el servicio digital, porque los derechos y su alcance pueden variar dependiendo de cada caso, incluso, si la red social o el servicio digital se proporcionan desde otro país.

En muchas ocasiones los derechos básicos en materia de protección de datos son atendidos a través de procedimientos tales como la solicitud de borrado o eliminación de una fotografía o de un video.

2.20. CIBERACOSO.

Esta práctica se da de manera continua, cuando una niña, niño o adolescente es molestado, amenazado, humillado, acosado, avergonzado o abusado por otro niño, niña o adolescente a través de medios digitales como correo electrónico, mensajes

¹⁶ IDEM

de texto y/o audiovisuales, chats, interacción en redes sociales, videollamadas, entre otros.

Es importante distinguir que para que exista el ciberacoso en menores, se debe dar entre dos iguales, es decir, el niño, niña o adolescente y el acosador son de edades similares, pues de lo contrario sería grooming.¹⁷

Los efectos del ciberacoso sobre la salud mental pueden ser diferentes según el medio que se utilice. Por ejemplo, el acoso a través de mensajes de texto o de imágenes o vídeos en las plataformas de las redes sociales ha demostrado ser muy perjudicial para los adolescentes. La mayoría de las escuelas consideran el acoso como un problema grave y toman medidas para combatirlo.

Las víctimas de cualquier forma de violencia, entre ellas la intimidación y el ciberacoso, tienen derecho a que se haga justicia.

Las leyes contra el acoso, sobre todo el ciberacoso, son relativamente nuevas y todavía no existen en todas partes. Por este motivo, muchos países se basan en leyes relacionadas con el acoso, como las que se refieren al hostigamiento, para castigar las formas más graves de ciberacoso.

En los países que tienen leyes específicas sobre el ciberacoso, el comportamiento en línea que intencionalmente causa trastornos emocionales graves se considera una actividad delictiva. En algunos de esos países, las víctimas de ciberacoso pueden buscar protección, prohibir las comunicaciones de una persona en particular y restringir, temporal o permanentemente, el uso de los dispositivos electrónicos que esa persona utiliza para el ciberacoso.

¹⁷ Véliz, C. (2021). Privacidad es poder Datos, vigilancia y libertad en la era digital. Barcelona: penguin Random House Grupo Editorias S.A.S.

Sin embargo, es importante recordar que la criminalización no siempre es la respuesta más adecuada al ciberacoso. En algunos casos, cuando es seguro hacerlo, puede ser mejor centrarse en reparar el daño y arreglar la relación.

Las empresas de redes sociales también ofrecen herramientas educativas y orientación para que los niños, los padres y los maestros conozcan los riesgos y las maneras de permanecer seguros en línea