Fotografía: Fractal Pictures para Adobe Stock

“DEEPFAKE” Suplantación de identidad en imágenes no estáticas, protección de datos personales y el derecho al honor

Caheri Amaya Corona
Encargada de Medición en el ITEI

Resumen

La tecnología que creíamos se encontraba solamente en manos de grandes corporaciones y entes de gobierno, se encuentra ya al alcance de cualquier persona, por lo que su utilización para fines ilícitos se ha convertido en una preocupación principal en una sociedad tecnológica y conectada constantemente a través del ciberespacio. Una de las nuevas tecnologías es la suplantación de características faciales de una persona, para implantarla en el rostro de alguien que aparece en un video, esto se le se conoce como “Deepfake” o suplantación de identidad en imágenes no estáticas, la cual representa un grave peligro para las personas en el aspecto de su privacidad, su derecho al honor y a la protección de sus datos personales. Esta nueva tecnología va más allá de la suplantación de la identidad para cometer delitos, pues se ha utilizado para crear videos que dañan la reputación y el honor de las víctimas. En el presente artículo se analizan las implicaciones y consecuencias que trae consigo el uso de la identificación facial y la recabación de datos biométricos desde el aspecto de la protección de los datos personales como derecho humano y el derecho al honor. En el auge de la tecnología, la protección de datos personales se ha vuelto fundamental para proteger los derechos humanos y conservar la paz entre las naciones, pues este tipo de suplantación de identidad ha llegado al extremo de crear declaraciones de funcionarios de gobierno. La suplantación de identidad en imágenes no estáticas representa una nueva amenaza a la intimidad y privacidad de las personas, por lo que debe de ser estudiada desde la perspectiva del derecho de protección de datos personales.

PALABRAS CLAVES:
Reconocimiento Facial, Deepfake, Identidad Digital, Datos Biométricos, Suplantación de Identidad, Derecho al Honor

Introducción

En enero del 2018, en Rasana, una villa ubicada en la India, una niña de ocho años fue secuestrada, violada y asesinada por un grupo de ocho hombres (AsiaNews.it, 2018), ante este siniestro crimen, una periodista hindú adepta a los derechos de las mujeres, se vio envuelta en controversia al criticar a los integrantes del partido de derecha Bharatiya Janata quienes defendieron a los acusados y pidieron su liberación (Safi, 2018). Días después, un amigo de la periodista le compartió un video que circulaba en redes sociales: un video pornográfico donde ella es la protagonista (Ayyub, 2018). Este es el caso de Rana Ayyub, quien fue víctima de una nueva forma de falsificación de identidad, pues la mujer del video no era ella, el cabello y el cuerpo son de otra persona aunque efectivamente es su rostro. Rana no puede creer que la difamación de la que normalmente es víctima haya llegado tan lejos, pues el video se compartió más de 40,000 veces (Desk, 2018). La periodista acudió a la policía con su abogada para levantar una denuncia por daños a su honor y la utilización inapropiada y sin permiso de su imagen, pero su denuncia fue rechazada por la policía, quien argumentó que no hay leyes ni procedimientos para hacer nada al respecto. Finalmente, tras amenazar a la policía con exponerlos en los medios de comunicación, su denuncia es levantada pero siguió transcurriendo el tiempo y aún no se tienen culpables ni se ha hecho nada para protegerla (Ayyub, 2018).

Ali Bongo, presidente de la República Gabonesa en África Central, tenía meses sin salir a la luz pública, por lo que la gente empezó a cuestionar la salud del mandatario, incluso existieron rumores sobre su muerte, pues el silencio de los demás integrantes del gobierno alimentaba este rumor, finalmente el vicepresidente anunció que el mandatario había sufrido una embolia, pero que se encontraba con buena salud y que por el momento se encontraba en reposo. Después de tanta especulación y rumores, se publicó finalmente un video del presidente pero en lugar de tranquilizar a la población, incremento la especulación y las teorías, pues dicho video era muy extraño, las actitudes y gestos del mandatario no parecían na-

turales. El opositor de Ali Bongo declaró que dicho video era producto del "deepfake"[1], realizado por el gobierno para ocultar las enfermedades del presidente y hacer creer que se encontraba en buen estado de salud, por otro lado, muchas personas pensaron que el opositor fue quien creó dicho video para generar desconfianza hacia el gobierno representándolo como un gobierno autoritario y poco honesto.

En los casos anteriores, las personas fueron víctimas de una nueva forma de falsificación, el deepfake o la suplantación de identidad en imágenes no estáticas[2] (…) "es el uso de inteligencia artificial para colocar el rostro de una persona en el cuerpo de otra" (Harris, 2019, pág. 1). Esta técnica puede ser utilizada para falsificar un video, haciendo que aparezca una persona en dicho video pero en realidad es otra persona quien aparece en el mismo, pues se ha implantado el rostro de la víctima en el video.

Esta nueva herramienta tecnológica en un principio era difícil de utilizar, pues se necesitaban códigos de codificación y programación pero en el presente cualquier persona con conocimientos básicos de computación puede realizar este tipo de falsificaciones (Ciberseguridad LATAM). Esta nueva herramienta se encuentra al alcance de cualquier persona y la proliferación de esta falsificación ha sido tan grande que la empresa Google publicó una base de datos con 3,000 deepfake creado a partir de actores y fotografías para que pueda ser utilizada en la investigación y desarrollo de tecnología que detecte estas falsificaciones (Ciberseguridad LATAM) y de esta forma intentar contener la difusión masiva de estos videos falsos. Aunque las celebridades y personas con una vida pública son más propensos a ser víctimas de esta falsificación, según el Departamento de Defensa de los Estados Unidos de América todas las personas estamos expuestas a ser víctimas de esta falsificación (Vaas, 2018) pues según la Metodología de Beneficio y Anonimidad del Atacante BAA (Instituto Nacional de Transparencia, Información Pública y Protección de Datos Personales, 2015, pág. 3 a 5) a mayor beneficio y anonimidad tiene el atacante, mayor es el riesgo, por lo tanto el deepfake al realizarse en el ciberespacio donde la anonimidad es mayor, el atacante encuentra el medio idóneo para llevar a cabo sus acciones, y siendo la pornografía el principal objetivo de llevar a cabo estas falsificaciones (Ciberseguridad LATAM) el beneficio es mayor, pues la pornografía es uno de los negocios más remunerados del mundo (elmundo.com.ve, 2013).

En la actualidad, los avances tecnológicos han sobrepasado la imaginación de las personas, la tecnología que veíamos en las películas de ciencia ficción hoy en día se ha vuelto una realidad, por lo que la innovación es rápida y constante, sin que nos detengamos a pensar en las repercusiones que podría tener o si debería de hacerse, pues la practicidad de la vida cotidiana tiene mayor valor tanto en el aspecto económico como social, en consecuencia, tiene un respaldo inmenso en las nuevas creaciones de grandes compañías de tecnología como Apple Inc. o Google LLC.

Un ejemplo de ello son los teléfonos celulares, cuya función principal fue conectar a las personas sin que sea necesario que se encuentren en el mismo lugar, pero actualmente su tecnología ha avanzado tanto que ahora se les conoce como teléfonos inteligentes, convirtiéndose en una herramienta para las actividades cotidianas. Estos avances se encuentran al alcance de las personas con acceso a internet y a estos celulares inteligentes, por lo tanto la mayor parte de la población mundial tiene conocimiento de estas nuevas tecnologías y su utilización se encuentra cada vez más a disposición de todos.

La utilización de esta tecnología esta tan permeada en la sociedad que las actividades cotidianas se pueden realizar a través de una aplicación de teléfono, facilitando las tareas del día a día, como por ejemplo aplicaciones para conectarnos rápidamente con otras personas sin importar el tiempo o la distancia, escuchar música, realizar movimientos bancarios, consultar citas con el Instituto Mexicano del Seguro

[1] Término en lengua inglesa compuesta por dos palabras: deep y fake, que significan profundo y falso, respectivamente.

[2] La traducción literal al español sería "falso profundo", la cual no refleja el significado del concepto, en consecuencia la autora hace la traducción para dar entender al lector el significado global de dicho término.

Social, pedir transporte particular, entre otras aplicaciones que rebasarían nuestra imaginación, esto ha traído como consecuencia el desarrollo masivo de aplicaciones.

Una de las nuevas tecnologías a través de aplicaciones para teléfonos inteligentes es el reconocimiento facial, el cual consiste en técnicas que permiten la identificación de las personas basándose en el reconocimiento de peculiaridades, propias e individuales (Caldera-Serrano & Zapico-Alonso, 2009). Esta nueva tecnología permite que la identificación de personas por medio de su rostro sea utilizada como medida de seguridad técnica y como una herramienta para la seguridad pública o nacional.

Los usos que se le dan a esta técnica son diversos, pero en el contexto de los teléfonos inteligentes, principalmente se utilizan para el acceso al aparato, así como para proteger el acceso a las aplicaciones sensibles, como puede ser la banca móvil, correos electrónicos fotografías, entre otras. Aunque el reconocimiento facial implique una tecnología sofisticada, los avances han permitido que podamos tenerla en nuestros teléfonos.

Esta nueva tecnología se ha simplificado a tal punto que cualquier aplicación de android[3] contiene esta función, ya sea para facilitar el acceso del usuario a sus funciones o para hacer divertidas modificaciones al rostro conocidos como “filtros”, que pueden desde cambiar el color del cabello hasta cambiar el género del usuario. Este tipo de aplicaciones utilizan los datos biométricos extraídos de un individuo en forma de patrones para crear una base de datos y poderla comparar con los datos biométricos que se le presentan (Ortega García, Alonso Fernández, & Coomonte Belmonte, 2008). Esta tecnología se encuentra disponible para cualquier persona que cuente con un teléfono celular con suficiente memoria de almacenamiento y una cámara con buena definición, contrario a lo que hace un par de décadas hubiéramos pensado que sólo las grandes corporaciones o las instancias de seguridad y defensa nacional tendrían acceso.

Lo anterior ha traído como consecuencia que los programas o aplicaciones para realizar deepfakes sean accesibles y sencillos de utilizar con los recursos adecuados. Actualmente, la mayoría de los casos de deepfakes se han hecho contra las celebridades, pues la cantidad de imágenes que hay de ellos en línea son muchas y son de fácil acceso, además de que la difusión es mayor por tratarse de una persona pública[4], cuya vida privada es de interés de muchas personas. Aunque veamos poca probabilidad de ser víctimas de esta técnica, el riesgo es real, por lo que tenemos que comenzar a ejercer ciertas prácticas para minimizar la posibilidad de encontrarnos en una situación de suplantación de identidad en imágenes no estáticas que puedan dañar nuestro honor y reputación.

Por todo lo anterior esta investigación se centra en determinar en quién recae la responsabilidad para evitar ser víctimas del deepfake, por lo anterior se ha planteado la siguiente pregunta: ¿Cuál es la mayor fuente de información para quienes realizan los deepfakes? La metodología para responder esta pregunta será a través de la investigación teórica sobre el deepfake, como funciona, qué recursos utiliza y para qué se realiza. Se efectuará un análisis de informes estadísticos para conocer donde se encuentra la mayor fuente de información necesaria para llevar a cabo el deepfake.

[3] Sistema operativo desarrollado por Google para los teléfonos inteligentes.

[4] Sistema operativo desarrollado por Google para los teléfonos inteligentes.

“Deepfake” Suplantación de identidad en imágenes no estáticas y delitos cibernéticos

La característica principal del ciberespacio es que es un entorno anónimo, donde no sabes quién está detrás del ordenador ni las intenciones reales de sus acciones, dicha anonimidad acarrea problemas que se han vuelto comunes pero que su trasfondo es peligroso para la integridad de los cibernautas. Según (Pons Gamón, 2017):

> *El delincuente aprovecha el anonimato de sus ciberacciones al ser complicado identificar al atacante; cualquier usuario que tenga un equipo informático y conexión a internet, con unos conocimientos técnicos que están al alcance de cualquiera y con una inversión económica no elevada, puede ejecutar un ciberataque (pág. 82).*

Gracias al nivel de anonimidad que existe en el ciberespacio, el internet ha traído una nueva plataforma para cometer distintos delitos, pues al no existir fronteras ni un territorio donde establecer una jurisdicción, los criminales pueden cometer los delitos de una forma fácil y práctica. Uno de los nuevos ciberdelitos, es el llamado “Phishing”[5], que se conoce como “Suplantación de Identidad”, este ciberdelito consiste en utilizar correos electrónicos o páginas web falsas para obtener información confidencial como números de tarjetas de crédito, contraseñas o cuentas bancarias (Avast Software, 2015). Sin embargo, actualmente la suplantación de identidad va más allá de obtener información confidencial para conseguir un beneficio, ya podemos encontrar diferentes formar de suplantación, como la creación de perfiles falsos en redes sociales, hacerse pasar por otra persona en redes sociales para perjudicarla publicando tweets falsos[6], modificar fotografías para humillar a la víctima o en el caso de este artículo, falsificar videos.

La suplantación de identidad en imágenes no estáticas se da cuando en un video se modifica el rostro de la persona que aparece en él, sobreponiendo el rostro de otra persona haciendo que parezca que la víctima es quien aparece en dicho video. Esta falsificación se considera “profunda” porque el cuerpo de la persona no se modifica, solo el rostro el cual refleja las expresiones de la persona detrás de la falsificación. Estos videos pueden parecer tan reales que si no se estudian con detenimiento pueden ser totalmente creíbles.

Esta falsificación comenzó con videos de contenido para adultos, donde el rostro de los participantes se remplazaba con el rostro de alguna celebridad (Harris, 2019) sin embargo esta tecnología se utiliza para difamar a las personas, sin importar quienes sean, dañando su intimidad y su honor.

El deepfake se lleva a cabo a través de un programa de inteligencia artificial como “FakeApp”[7], se recopilan cientos de fotografías de las personas las cuales se procesan y después de determinado tiempo se obtiene el rostro digital de la persona listo para implantarse en el video deseado (Harris, 2019). Primeramente se obtienen las fotografías de la víctima, para crear un conjunto de fotos, después se busca un video donde el cuerpo de quien aparece en él sea similar al de la víctima, el cual se puede obtener a través del reconocimiento facial, para finalmente colocar el rostro reproducido a través de las fotografías obtenidas y colocarlo en el video (Delp & Güera, 2018).

Se necesitan dos conjuntos de imágenes, el primero consiste en varías imágenes de la persona que originalmente sale en el video que se usará para crear la suplantación, el segundo consiste en imágenes de la persona a quien se suplantará en el video manipulado, utilizando los autoencodificadores[8], para capacitar al programa para realizar la suplantación.

---

[5] Palabra compuesta por “Fishing” que su traducción literal es “Pescar” y “Phreak” que es una palabra compuesta que hace referencia al hackeo de teléfonos para obtener llamadas gratuitas, por lo tanto “Phishing” se refiere a utilizar diferentes métodos en las telecomunicaciones para engañar y obtener información personal para entregarla a un tercero y obtener gratuitamente un beneficio.

[6] Publicación en la red social Tweeter.

[7] Programa o aplicación que se puede obtener de forma gratuita para crear deepfakes.

[8] Tipo de red neuronal artificial usado para aprender codificaciones de datos de forma no supervisada.
El objetivo de un autoencoder es aprender una representación (codificación) para un conjunto de datos, generalmente con el propósito de reducir la dimensionalidad. http://www.alegsa.com.ar/Dic/autoencoder.php

Cuando se completa el proceso de capacitación, podemos pasar una representación latente de una cara generada a partir del tema original, presente en la pantalla, en la interfaz de la persona que queremos insertar en el video (Delp & Güera, 2018).

Dentro del internet podemos encontrar trámites en línea que pueden ser hackeados para obtener la información que en ellos se vierte, por ejemplo: "facturación electrónica, visado digital, voto electrónico, firma electrónica, carné de identidad digital, formularios telemáticos, certificado digital, receta electrónica, etc." (Giones-Valls & Serrat-Brustenga, 2010, pág. 9). Por lo tanto las fuentes de las que se pueden obtener información personal son inmensas.

El obtener imágenes e información personal que nos ayuden a suplantar la identidad de una persona, es mucho más sencillo de lo que pensamos, pues existen herramientas que pueden ser utilizadas en la gestión de la identidad digital, un ejemplo es un complemento del navegador Firefox, llamado Identify (Giones-Valls & Serrat-Brustenga, 2010) el cual "busca todos los perfiles de un usuario a todos los sitios de redes sociales y los aglutina en una única interfaz" (pág.10). Este complemento puede ser utilizado para obtener toda la información regada por el ciberespacio de una persona y aglomerar la mayor cantidad de imágenes que se pueda para utilizarlas en la capacitación de nuestro programa y obtener un deepfake más real.

Otra herramienta que puede ser utilizada para recopilar imágenes de una persona en internet y alimentar nuestro programa de creación de deepfakes, es Friendfeed, la cual "es una herramienta que permite desde un mismo lugar agregar toda la actividad en línea: las fotos que subimos, los videos, los posts que se escriben, los eventos donde nos apuntamos, la música que escuchamos, (…)" (Giones-Valls & Serrat-Brustenga, 2010, pág. 11)

Al inicio, este tipo de prácticas se utilizaban para crear videos pornográficos de las celebridades para complacer las fantasías de los usuarios, sin embargo gracias a que esta tecnología se encuentra al alcance de cualquier persona, ya se utiliza con gente común con propósitos como el chantaje, la humillación, desacreditación, engaño, entre otros.

Actualmente, estos videos se utilizan para crear pornografía de venganza, es decir, se difunde el contenido sexual explícito de una persona sin su consentimiento (Security, 2017), sin embargo en el deepfake, se falsifican videos pornográficos para humillar a una persona, generalmente ex parejas, como venganza por acciones o hechos, sometiendo a la víctima al escarnio público y a las burlas por dicho contenido.

El chantaje es otro de los delitos que se comenten con el uso del deepfake, el delincuente falsifica videos y amenaza a la víctima con exponerlos sino le entrega dinero o contenido sexual real para continuar con su chantaje, la víctima en la mayoría de los casos no tiene otra opción más que entregarle al extorsionador lo que pide, pues al viralizarse el contenido muy pocas personas se detendrán a pensar si lo que ven es real o no, compartiendo indiscriminadamente afectando la privacidad y la intimidad de la víctima.

Esta tecnología también puede ser utilizada para crear declaraciones o falsificar acciones que afecten la reputación de cualquier persona, desde un ciudadano común hasta algún mandatario, poniendo en riesgo la seguridad nacional o las relaciones internacionales. Si lo vemos en el ámbito del activismo, esto puede ser utilizado para que un activista en contra del uso de armas por ejemplo, utilice un arma en un video y haga declaraciones racistas, poniendo en su contra a las personas y desacreditándolo, dañando su reputación y credibilidad para restarle peso a sus acciones dentro de las campañas anti armas.

El uso más preocupante de esta tecnología, es la creación de noticias falsas, creando un fenómeno de desinformación que en las manos equivocadas, podrían generar desconcierto o inestabilidad, pues los videos pueden falsificarse para darle credibilidad a las noticias falsas y presentarlas como verídicas.

Podemos preguntarnos entonces ¿Si este tipo de suplantación de identidad es tan fácil de realizar, es igual de fácil detectarlo?, la respuesta es sí. Aunque cada día se va sofisticando más haciendo que sea difícil de detectar, existen algunas técnicas que nos ayudan a dilucidar si el video que vemos es real o no. Para ello se utilizan programas de detección de deepfakes, los cuales usan los datos audiovisuales del video para detectar inconsistencias entre el movimiento de los labios y el audio, así como las variaciones de las imágenes que se encuentran en diferentes sistemas. Cuando el video es genuino, el movimiento de los labios y el audio están perfectamente sincronizados mientras que en las modificaciones el audio no se sincroniza perfectamente pues no son los labios originales los que emiten el sonido grabado (Korshunov & Marcel, 2018).

Aunque existan formas de detectar cuando un video es falso, sin embargo los avances continuos en las técnicas de suplantación facial provocarán que sea cada vez más difícil de detectar (Korshunov & Marcel, 2018).

Identificación facial, detección facial y rasgos biométricos

Para poder comprender como funcionan estas técnicas, es importante mencionar los elementos que convierten a un rasgo en un rasgo identificativo, (Ortega García, Alonso Fernández, & Coomonte Belmonte, 2008) establecen los siguientes elementos:

- **Universalidad:** todo el mundo debe poseer esa característica.
- **Unicidad:** dos personas cualesquiera deben ser suficientemente diferentes en términos de ese rasgo, es decir, un mismo rasgo para dos personas diferentes nunca puede ser idéntico.
- **Permanencia:** el rasgo debe permanecer suficientemente invariable en el tiempo durante un periodo de tiempo aceptable.
- **Evaluabilidad:** el rasgo debe poder ser medido cuantitativamente. Aparte de estas propiedades, desde el punto de vista práctico de un sistema de reconocimiento, hay otro conjunto de propiedades que deben satisfacerse.
- **Rendimiento:** hace referencia al error cometido en el reconocimiento de individuos, a la velocidad y recursos necesarios para llevarlo a cabo, así como a los factores externos que afecten a las capacidades de reconocimiento del sistema.
- **Aceptabilidad:** los usuarios deben estar dispuestos a emplear ese rasgo en las actividades de su vida cotidiana.
- **Fraude:** los sistemas que usen ese rasgo deben ser suficientemente seguros de forma que resulte difícil atacarlos (pág. 8 y 9).

Dentro de los rasgos, tenemos los que se vinculan con características físicas y los que se vinculan con rasgos de conducta (biometría y seguridad). Bajo esta tesitura, tenemos datos físicos como el rostro, el iris, la huella digital entre otros, y de los rasgos de conducta tenemos la escritura manuscrita, la firma, la voz, la dinámica de tecleo o la forma de andar (Ortega García, Alonso Fernández, & Coomonte Belmonte, 2008).

Si analizamos los elementos anteriores, nos damos cuenta que el rostro cumple con todos ellos, pues absolutamente todas las personas tienen una cara, la cual es única en cada persona y que solo varía de acuerdo al envejecimiento, sí es objeto de medición cuantitativa pues se pueden medir diferentes puntos del rostro; las personas prefieren ser reconocidas por su rostro pues es una característica pública que no provoca pudor y por último, es difícil de imitar o duplicar la cara de una persona.

Dentro de los rasgos identificativos, tenemos los rasgos o datos biométricos, el (Instituto Nacional de Transparencia, Información Pública y Protección de Datos Personales, 2018) refiere que son: "propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles" (pág. 5). Con esta definición podemos entonces hablar de los sistemas biométricos. Un sistema biométrico (…) "es un reconocedor de patrones que captura datos biométricos de un individuo, extrae un conjunto de características a partir de dichos datos y las compara con otros patrones previamente almacenados en el sistema" (Ortega García, Alonso Fernández, & Coomonte Belmonte, 2008, pág. 15), sobre la identificación biométrica nos enfocaremos únicamente en el reconocimiento facial, el cual se basa principalmente en puntos nodales que se encuentran en nuestro rostro, el rostro puede llegar a tener 80 puntos nodales[9], por lo que básicamente se trazan los espacios y patrones que tiene nuestro rostro, midiendo el espaciado entre ellos para poder tener un patrón que hace identificable a una persona (Caldera-Serrano & Zapico-Alonso, 2009).

Estos patrones se registran en una base de datos, la cual es comparada con la persona que accesa al identificador, comparando los patrones actuales de la persona y los patrones guardados en el sistema, obteniendo los resultados de "sí es" "no es".

Para poder comprender con mayor facilidad cómo funcionan los sistemas biométricos, debemos tener en cuenta las etapas por las que se construye el mismo:

- **Adquisición de datos:** Se recogen los datos analógicos de partida a través de un sensor y se convierten a un formato digital.
- **Pre-procesado:** Acondicionar la información capturada para tener una mayor efectividad en el reconocimiento posterior.
- **Extracción de características:** Se elimina la información que no resulte útil en el proceso de reconocimiento, se extraen únicamente aquellas características que sean discriminantes entre distintos individuos y que al mismo tiempo permanezcan invariables.
- **Generación de un modelo y comparación de patrones:** Se elabora un modelo que representa a cada individuo, dichos modelos se almacenan en la base de datos del sistema.
- **Base de datos:** Se almacenan los modelos que representan la identidad de cada usuario del sistema, la base de datos puede estar almacenada en un lugar único centralizado
- **Umbral de decisión:** La comparación entre los datos de entrada y un modelo de identidad extraído de la base de datos (Ortega García, Alonso Fernández, & Coomonte Belmonte, 2008, págs. 15, 16)

[9] Una pareja de puntos, situados en el eje óptico de un objetivo compuesto que sirven de referencia para mediciones básicas. https://www.fotonostra.com/glosario/puntonodal.htm

Este proceso se puede describir en la siguiente figura:

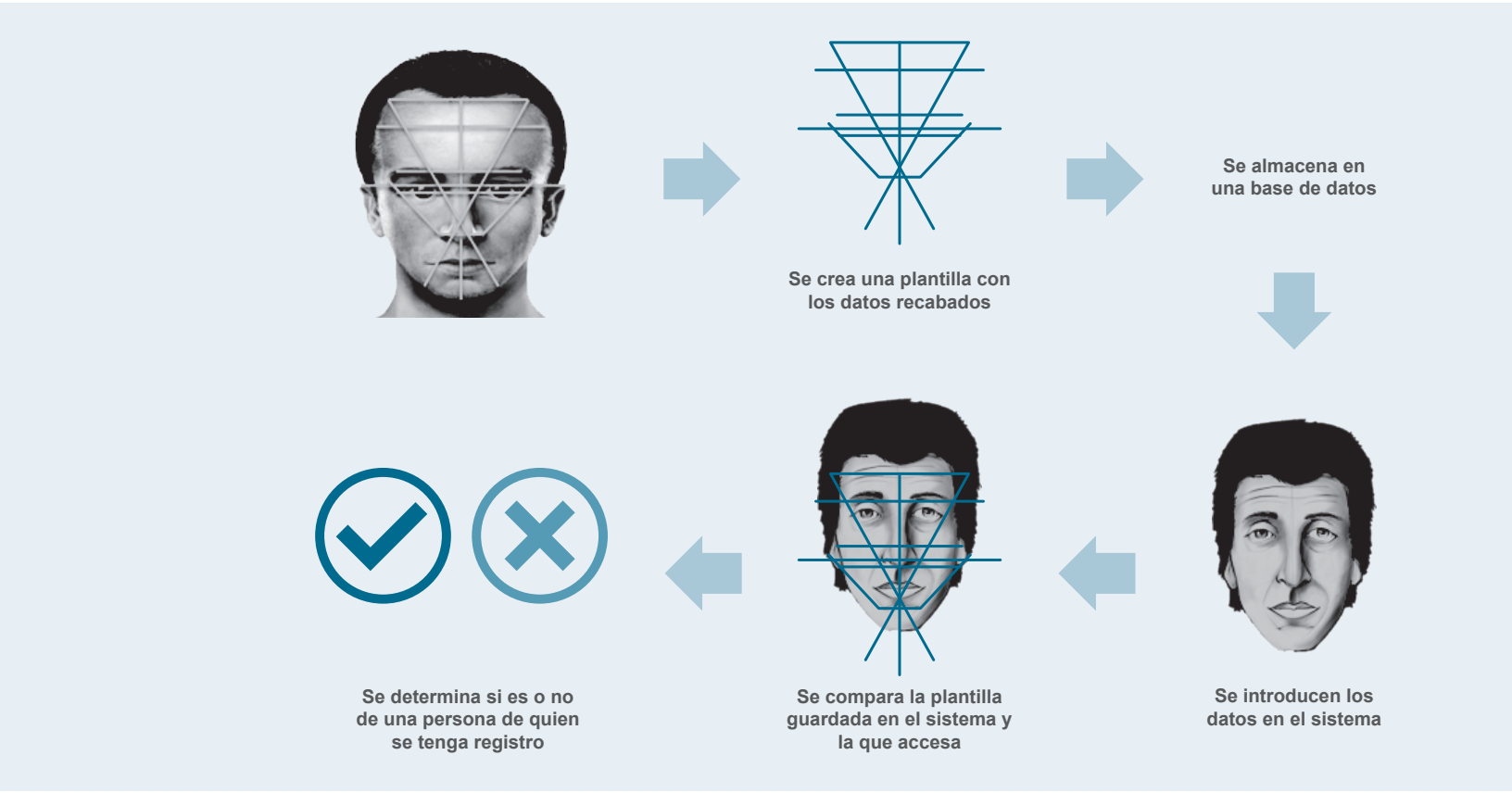

Figura 2. Proceso de identificación facial biométrica. Representación sencilla del proceso que implica la identificación facial. Autoría propia.

Cuando utilizamos las aplicaciones y herramientas que están a nuestro alcance, se nos hace fácil utilizarlas sin ponernos a pensar cómo funcionan y los recursos que utiliza. Aunque estas aplicaciones nos parezcan divertidas, detrás de ellas se encuentra una herramienta poderosa y peligrosa: los datos faciales biométricos de las personas. Este conocimiento tan exacto del rostro de una persona puede acarrear riesgos en el mundo virtual que ni siquiera podemos plantearnos.

La identificación facial tiene distintos usos, como el acceso controlado a ciertas zonas u objetos, la identificación de personas en aduanas o para seguridad pública identificando criminales. Sin embargo el uso excesivo de esta técnica genera riesgos inimaginables, pues se utiliza de forma arbitraria sin detenerse a pensar en las implicaciones éticas o morales que conlleva la utilización de datos biométricos. Por lo tanto es importante identificar el contexto social en el que se desarrollan estas tecnologías.

Identidad digital y vida cibernética

Con la creación del internet, se ha formado un nuevo mundo en el cual los horizontes y las fronteras no existen, construyendo una realidad ilimitada, lo que se conoce como ciberespacio, el cual (…) "existe solamente como espacio relacional; su realidad se construye a través del intercambio de información; es decir, es espacio y es medio. Una red sin interacción entre sus miembros deja de ser una red; la red existe porque existen relaciones entre sus integrantes" (Aguirre Romero, 2004, pág. 1).

> *La identidad digital es la representación de uno mismo, una identidad digital que se va construyendo a partir de la propia actividad en Internet y de la actividad de los demás. La oferta actual de ocio/negocio y consumo cultural en Internet, las aplicaciones para la comunicación electrónica y los sitios de redes sociales construyen una estructura en la que vive un "yo virtual". (Giones-Valls & Serrat-Brustenga, 2010, pág. 2 y 3).*

La identidad digital se forma con cada uno de los movimientos y decisiones que se toman en línea, por ejemplo, la información que publicamos en nuestras redes sociales, las búsquedas que hacemos y las descargas. Nuestra sola presencia en el mundo cibernético representa ya una parte importante de nuestras vidas, las personas que no utilizan las redes sociales pueden llegar a sentirse aisladas, pues la comunicación y el contacto entre las personas se hace a través del ciberespacio, por lo que redes sociales como Facebook se han vuelto parte de nuestra identidad digital, pues nos representan dentro del ciberespacio.

En la actualidad, la información personal que nosotros mismos compartimos en redes es inmensa, (…) este cambio de lo privado a lo público se genera por la necesidad de las personas de ser protagonistas y reconocidos, que se los tenga en cuenta. Cada persona decide qué y cuánta información personal publicar en el perfil ((Heiderscheid, 2016, pág. 59)., pues se tiene la idea de que la popularidad que tengamos en nuestras redes sociales es equivalente a nuestra valía como persona, trayendo como consecuencia la excesiva apertura de nuestra vida en internet.

Esta necesidad de aceptación y validación social ha llegado tan lejos, que los adolescentes se sienten estresados por mantener un estatus social en sus redes a través de publicaciones y likes[10] (Wallace, 2018). Incluso llegando al extremo de pagar por recibir cierta cantidad de likes en sus publicaciones[11]. Lo más inquietante de la sobre exposición en las redes, es que es voluntaria, es decir, nadie nos obliga a compartir ni publicar, es la propia necesidad de sentirse parte de la sociedad la que nos lleva a exponer nuestra vida privada ante millones de personas.

Algunas décadas atrás, las personas tenían la costumbre de llevar diarios íntimos, donde contaban las experiencias personales y los pensamientos que tenían día a día, convirtiéndose en algo tan introspectivo que normalmente se escondía del resto de las personas, incluidos los demás miembros del hogar. Hoy en día, estos diarios se han convertido en algo totalmente público y materia de entretenimiento, conocidos como "blogs" donde las personas publican cosas sobre su vida cotidiana y los pensamientos que van teniendo, incluso ya hay diarios tan públicos que podemos ver a las personas realizando sus actividades cotidianas, conocidos como "vlogs"[12]. Es por ello que podemos conocer aspectos de la vida de otras personas que nunca pensamos que conoceríamos a menos de tener una relación estrecha.

La información personal que se comparte día a día, nos puede dar una idea bastante cercana de la personalidad y el estilo de vida de alguien, creando una identidad dentro del ciberespacio con una gran cantidad de fotografías, publicaciones y datos sobre sí mismos. Una de las redes sociales más populares es Facebook, en la cual según el estudio publi-

[10] Función de Facebook cuya traducción literal sería "Gusta" pero en el contexto de redes sociales significa "Me gusta", utilizado para otorgar aprobación a una publicación de una persona.

[11] www.kickliker.com

[12] Diarios virtuales en formato de video, que generalmente se comparten en plataformas como youtube o instagram.

cado por (Smith C. , 2013), cuenta con 1.5 billones de usuarios, quienes han subido un promedio de 217 fotos cada uno, obteniendo el resultado de 250 billones de fotos subidas, con 350 millones fotos nuevas (Smith C. , 2013). Esto nos arroja luz a la cantidad de fotografías de nosotros que tenemos compartidas, convirtiendo nuestro rostro en información que se comparte masivamente a través de lo que compartimos en nuestras redes, si además de ello agregamos la demás información que compartimos como: nombre completo, fecha y lugar de nacimiento, lugar de residencia, datos académicos y laborales, datos sensibles[13] como la preferencia sexual, gustos y actividades favoritas, prácticamente estamos volcando toda nuestra identidad en la red.

La vida cibernética ya forma parte de nuestra vida cotidiana, pues en simples actitudes podemos identificar el nivel de integración que ha desarrollado el internet en nuestra vida, por ejemplo: al despertar lo primero que hacemos es revisar las notificaciones de redes sociales, todavía no nos hemos levantado de la cama y ya estamos enterados de cuestiones a nivel mundial y de asuntos personales de otras personas.

Ante esta nueva vida cibernética, es importante aprender a gestionar nuestra identidad digital en el ciberespacio, pues como Nieves González-Fernández-Villavicencio (como se citó en Sola-Martínez, 2009) menciona, la falta de conciencia en cuanto al uso de las redes sociales y su correcto empleo, es decir, formar personas consientes de los peligros de la red, que tengan el conocimiento suficiente para gestionar su propia identidad digital y evitar que nos sorprenda el uso de nuestros datos por parte de terceros.

La gestión de la identidad digital refiere a “Todas las acciones que un individuo suele realizar para adquirir, crear, organizar, almacenar, recuperar, utilizar y distribuir la información necesaria para completar las diferentes tareas y las responsabilidades que tiene asumidas a nivel personal, social y laboral” (Ferran-Ferrer & Pérez-Montoro, 2009, pág. 366).

Para poder gestionar nuestra identidad digital, es importante conocer los elementos que la conforman, pues teniendo presentes todos los alcances de la misma, es más sencillo controlar su expansión. La identidad digital se conforma de los siguientes elementos:

a) Blogs. (…) un blog ha pasado a ser un diario que, tanto puede ser personal como corporativo (…)

b) Microblogs. Es una herramienta similar al blog, con la diferencia que tienen un número limitado de caracteres y que se pueden publicar a través de diversas aplicaciones. (…)

c) Portales de noticias y sitios web. (…) Cuando se aportan comentarios y opiniones en Internet, hay que tener presente que estos mensajes se pueden encontrar a través de los buscadores y que difícilmente desaparecen de la red.

d) Sitios de redes sociales genéricas o especializadas, tales como Facebook, LinkedIn, XING o Pleiteando (esta última especializada en el mundo jurídico).

e) Textos, fotografías o vídeos en la red, con Google Docs, Picasa, Flickr, YouTube o Vimeo. Todas las actividades en la red (visitas a la web, clics en un enlace, comentarios en un blog, colgar una foto o un vídeo...) quedan registradas y difícilmente se borran. El conjunto de todos estos pasos en Internet forma parte de la identidad digital de una persona, de quien posteriormente se pueden buscar y recuperar gran parte de las acciones, comentarios y opiniones que ha dejado en la red.

f) El correo electrónico. Del mismo modo que no se borra el rastro a la red, en general, tampoco se borran los mensajes de correo electrónico, a pesar de que estén protegidos con una contraseña (…). (Giones-Valls & Serrat-Brustenga, 2010, pág. 3 y 4)

[13] Artículo 3 fracción X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Para facilitar el entendimiento respecto a los elementos que conforman la identidad digital, a continuación se presenta la siguiente figura:

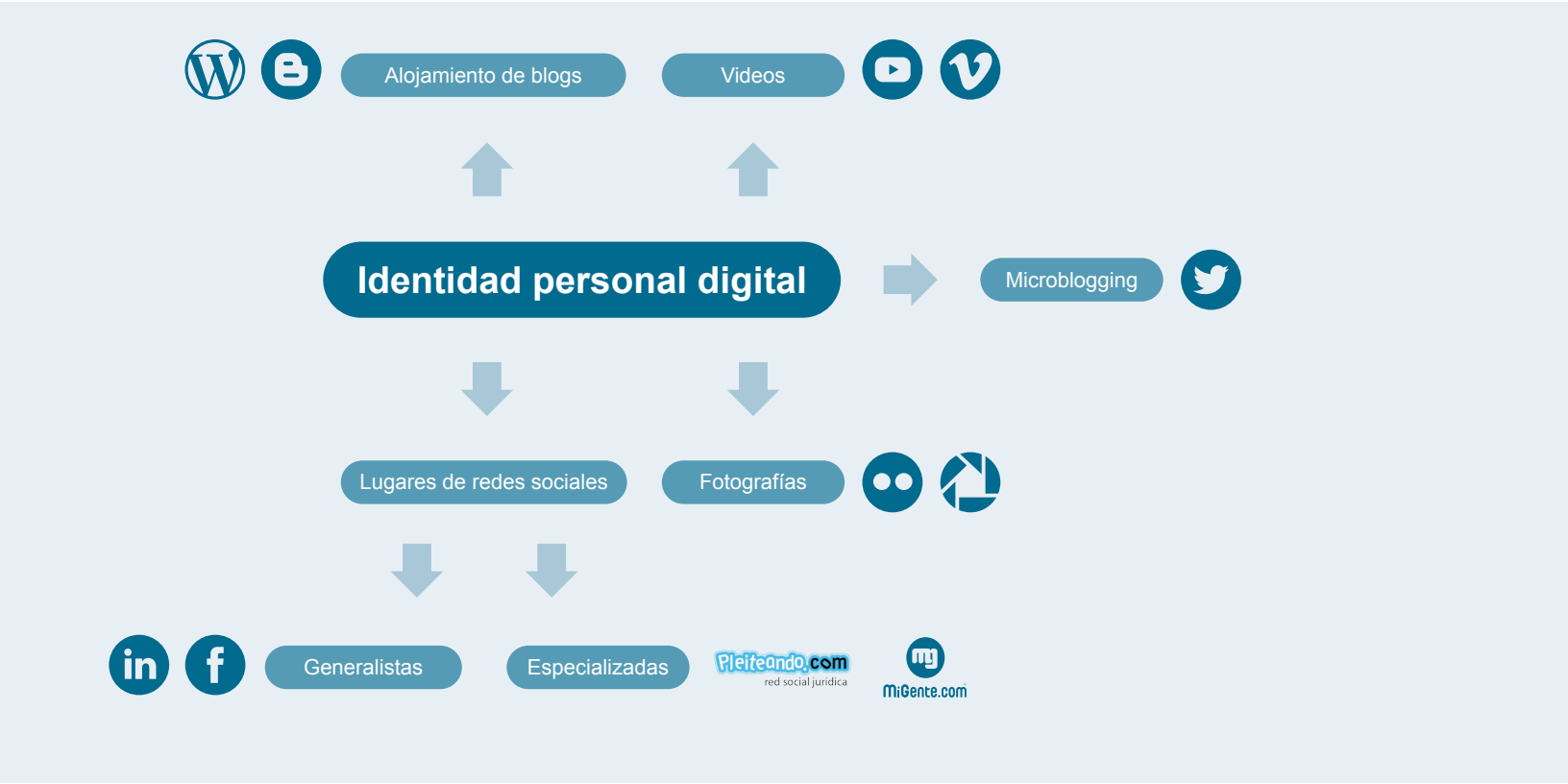

Figura 1. Ejemplo de las identidades digitales. Representación de lo que puede conformar una identidad digital, dependiendo del uso y la navegación del usuario. (Giones-Valls & Serrat-Brustenga, 2010, pág. 4)

La gestión de la identidad personal (PIM)[14] se ha convertido en un (…) "área de estudio que comprende disciplinas como la psicología cognitiva, la interacción persona-ordenador, la gestión de bases de datos, la inteligencia artificial, la gestión de información y de conocimiento, la recuperación de información, y las ciencias de la información. (Franganillo, 2009, pág. 400).

[14] Personal Information Managment cuya traducción al español sería: gestión de información personal.

En esta nueva era de una sociedad dependiente de la tecnología y con avances tan rápidos de los cuales es difícil mantenerse al tanto.

> *En una sociedad intensamente informatizada, uno de los peligros existentes es la diferencia entre los que tienen acceso a las nuevas tecnologías y los que no, así como el abismo entre los que saben utilizarlas y los que no. Estos últimos se convierten en el nuevo sector en riesgo de exclusión social, fenómeno denominado brecha digital. (Giones-Valls & Serrat-Brustenga, 2010, pág. 3)*

La brecha digital a la que se refiere el autor, podemos entenderla como las diferencias del conocimiento y manejo que tienen las personas en las tecnologías de la información y comunicación, en razón de las (…) "brechas sociales producidas por las desigualdades económicas, políticas, sociales, culturales, de género, generacionales, geográficas, etc." (Camacho, 2005, pág. 5). Es por esto, que se vuelve fundamental el capacitar a todas las personas para que aprendan a gestionar la información personal que vierten en el ciberespacio, para tener un mayor control sobre nuestra identidad digital y poder protegerla de las amenazas de las que se hablará más adelante.

Es importante conocer los elementos que conforman la gestión de la información personal, por lo que (Franganillo) establece:

- **Información personal.** Puede ser definida como la relativa a una persona, pero custodiada y controlada por otras; la experimentada por una persona, pero ajena a su control.
- **Piezas de información.** Son documentos de papel o digitales, o la referencia a cualquiera de éstos. Es información empaquetada con expectativas de persistir. Es posible crear una pieza de información, almacenarla, trasladarla, darle nombre, copiarla, distribuirla, borrarla y transformarla, y se le pueden otorgar ciertas propiedades. Cada pieza tiene asociada una forma de información, determinada por las herramientas y aplicaciones que permiten manipularla.
- **Espacio personal de información.** Es un dominio abstracto que abarca todas las piezas de información que están bajo el control de un individuo. La información personal se combina para formar este espacio que contiene libros, documentos en papel (en cualquier lugar), mensajes electrónicos (de varias cuentas) y ficheros electrónicos (en cualquier ordenador).
- **Ecosistema de información personal.** Tungare, Manas (como se citó en Franganillo, 2009, pág. 401) El entorno de información de un individuo lo forma un sistema de dispositivos y aplicaciones que interactúan estrechamente entre sí para satisfacer las necesidades de información.
- **Colecciones de información personal.** Son subconjuntos del espacio personal de información definidos por las actividades de una persona en relación con tales espacios, más que por la forma de la información.
- **Actividades de guardado.** Al encontrar una pieza de información se anticipan necesidades futuras que esa pieza podría resolver, y se determina qué podría hacerse con ella en el futuro. (pág. 401 y 402).

Teniendo en cuenta todos los elementos que conforman la gestión de información personal, podemos darnos una idea de lo complicado que puede llegar a ser mantener el control de la información personal que llega al ciberespacio, por lo que conocer lo que es nuestra identidad digital ha pasado a ser un conocimiento necesario en esta sociedad informática.

> *Hay dos perspectivas para aproximarse al tema de la identidad digital y de Internet. Una es creer que la presencia virtual significa un peligro para la seguridad personal y, por tanto, convenir en que si un individuo no construye su identidad digital, una tercera persona puede suplantarla y pueden ocurrir hechos indeseables. La otra perspectiva es entender la construcción de la identidad en la red como una oportunidad de aprendizaje tanto personal como pro-*

fesional dentro de la cultura informacional donde vivimos inmersos. Freire (como se cita en Giones-Valls & Serrat-Brustenga, 2010, pág. 8)

La identidad digital es una proyección de quienes somos en el mundo físico, por lo que conocer e informarnos acerca de la gestión de información personal es indispensable para preservar nuestros derechos cuando nos encontramos en el ciberespacio.

La suplantación de identidad en redes sociales es tan fácil como descargar algunas fotografías del perfil de la víctima, ya que la cantidad de fotografías que se comparten a diario por usuario es inmensa. Ahora imaginemos que una persona sube fotografías suyas diariamente en sus redes sociales, esta cantidad de fotografías pueden ser robadas y analizadas a través de un programa de deepfake, para obtener los patrones necesarios para recrear digitalmente el rostro de la persona y poder utilizarla en videos.

Por otro lado, aunque el conjunto de fotografías que compartamos en internet sea poca o se encuentra protegida; información como fotografías, correo electrónico, currículo profesional entre otras, es solicitada en la mayoría de los formularios para crear un perfil (Giones-Valls & Serrat-Brustenga, 2010) incluso el visitar páginas web puede ser riesgoso, en razón de que la mayoría de estas páginas recogen nuestra información con nuestro consentimiento, ya que gran parte de los usuarios acepta sin leer las políticas de privacidad y de cookies[15] para navegar dentro de la página.

Por lo tanto, la utilización del internet y de las nuevas tecnologías en la vida cotidiana debe de contemplar las implicaciones y consecuencias que se podrían tener al no utilizar estas herramientas de forma responsable y consciente de todos los peligros que implica.

Derecho al honor y a la protección de datos personales

Desde la declaración universal de los derechos humanos en 1948, se han reconocido diversos derechos que las personas tienen por el simple hecho de ser humanos, en el artículo 12 se señala el derecho a la integridad de su vida privada, el honor y la reputación (ONU, 1948). En el mismo artículo se menciona el derecho a que las leyes protejan este derecho, lo que conocemos como el derecho a la protección de datos personales.

Dentro de la legislación de nuestro país, podemos encontrar que en el artículo 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, establecen este derecho a la protección de datos personales, por lo que se crearon Organismos Constitucionales Autónomos, tanto a nivel nacional como estatal, cuya función es garantizar este derecho. Además a nivel nacional se tienen leyes generales en materia de protección de datos personales para sector privado y público. Sin embargo, este derecho se ve amenazado por los avances tecnológicos que surgen en la actualidad, teniendo como ejemplo la utilización del deepfake.

La intimidad según (Martínez de Pisón, 1997) es "La capacidad para llevar nuestras relaciones íntimas y personales, nuestra autonomía moral y nuestras acciones como ciudadanos libres según nuestro arbitrio, sin intromisiones ni interferencias, de otros" (pág. 728). Por lo tanto, el que nuestras características faciales sean utilizadas para crear videos falsos, afecta directamente nuestra intimidad, pues al compartirse este tipo de videos, expone a las victimas al escrutinio público y a la opinión pública, por lo que el daño muchas veces es irreparable.

Como señala (Villanueva-Turnes, 2016) el derecho al honor:

"Se dirige a preservar no solo el honor en sentido objetivo sino también en sentido subjetivo de dimensión individual, o dicho en otras palabras, no únicamente se va

[15] Las cookies son archivos que crean los sitios web que visitas y guardan datos de navegación para que disfrutes de una experiencia online más sencilla. Gracias a ellas, los sitios web no cierran tu sesión, recuerdan tus preferencias y te proporcionan contenido relevante según tu ubicación. https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=es

a proteger la reputación o valoración que tenga la sociedad sobre uno mismo, sino también la consideración que cada uno tenga de sí mismo" (pág. 196).

En el caso de Rana Ayyub, la periodista era conocida por defender los derechos de las mujeres en India, por lo que cuando se involucró en el caso de Rasana, criticando a los miembros del partido de derecha por defender a los acusados, los miembros de este partido decidieron crear una campaña de desprestigiación en su contra, publicando un falso video pornográfico de la periodista y humillarla públicamente. Esto vulneró su derecho al honor, pues se le exponía en una situación vergonzosa, que en un país como la India con altos índices de violencia de género (Foundation, 2018), provocó una oleada de maltratos y acosos por parte de la sociedad hindú, teniendo como resultado la publicación de su número privado de teléfono, insinuaciones sexuales en sus redes sociales y comentarios vejatorios en las calles (Ayyub, 2018). Esta vulneración dañó su derecho a la intimidad, al honor, a la protección de sus datos personales y a su reputación.

Al ser humano siempre le ha importado como es percibido y aceptado en la sociedad en la que se desenvuelve, por lo que el honor y la reputación han jugado un papel importante en el desarrollo de las personas, pues este bien lo otorgan las personas a quien lo merece, teniendo como resultado que el honor es una característica frente a los demás que nos hace distinguibles y virtuosos. En consecuencia, el deepfake amenaza el honor y la reputación de las víctimas, pues es comúnmente utilizado para humillar a las personas haciéndole creer a los demás que dicha persona efectivamente es quien aparece en el video y las expone al escarnio público.

La reputación es según Solove (como se citó en Giones-Valls & Serrat-Brustenga, 2010) "un componente clave de nuestra identidad, refleja quiénes somos y define como interactuamos con los demás" (pág. 6). Por lo tanto, podemos entender que la forma en que nos relacionamos con los demás está directamente ligada en cómo somos percibidos en la sociedad, por lo que una violación a nuestro honor o reputación tiene repercusiones directamente en la sociedad en la que nos desenvolvemos y en la forma en que nos relacionamos con los demás, generando un daño que puede ser irreparable.

Los derechos humanos deben ser garantizados por el Estado[16], por lo tanto el derecho al honor, a la intimidad y a la protección de los datos personales se encuentra contemplado en nuestra carta magna, teniendo como medio de control las leyes en materia de protección de datos personales, pues al protegerse los datos personales dicha protección alcanza al honor y a la intimidad de la persona, pues forman parte de la misma esfera de derechos.

Es por ello, que el derecho a la protección de datos personales juega un papel importante en la creación de nuevas tecnologías, en razón de que al diseñar nuestra tecnología se debe realizar con base en la ética, buscando que se preserven los principios de privacidad, seguridad, transparencia, control, explicabilidad, apego a las leyes, pruebas, calidad y reparación y mitigación (McSweeny, 2018) de esta manera garantizamos que los derechos humanos son respetados al diseñar nuevas tecnologías.

Sin embargo, el desarrollo masivo de la tecnología y el avance y mejora constante de las tecnologías de la información hace casi imposible la regularización de las mismas, ya que cuando se expide alguna norma o alguna ley sobre alguna tecnología, los avances la sobrepasaron haciendo la norma insuficiente o incluso obsoleta (Arreola, 2019). Por ello, se debe de pensar en otra forma de garantizar el derecho a la protección de datos personales de los usuarios de redes sociales.

En la Ley Federal de Protección de Datos Personales en Posesión de Particulares, se establecen los principios que rigen el tratamiento de datos personales, siendo estos licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y respon-

[16] Artículo 1 párrafo tercero Constitución Política de los Estados Unidos Mexicanos.

sabilidad[17]. Dentro del principio de consentimiento, tenemos el derecho a la autodeterminación informativa, la cual se denomina según (Riande Juárez) de la siguiente manera:

> *El Derecho a la autodeterminación informativa hace referencia a la prerrogativa que todo individuo tiene frente a cualquier ente público o privado, por la cual nadie debe introducirse, sin autorización expresa (de él mismo o por mandato de ley o judicial), en aquellos aspectos que no son públicos –sino de su vida personal, familiar, documentos, correspondencia y domicilio–, para conocerlos, conservarlos, procesarlos y/o transmitirlos, independientemente de que dicha acción le cause o no, algún daño o molestia (pág. 8).*

Podemos entender entonces que las personas tienen el derecho de decidir qué información personal comparten, ya sea en el ámbito privado o público, por lo que el deepfake atenta contra este derecho al utilizar los datos biométricos de la persona sin que pueda decidir si los comparte o no, pues son tomados de imágenes robadas de la víctima.

Por otro lado las imágenes que se utilizan para realizar la suplantación, son obtenidas de las redes sociales de las personas que voluntariamente han decidido compartir en la red, sin embargo, las personas comparten sus fotografías con la intención de compartir alguna situación en específico, como un cumpleaños o un viaje, no para que sean utilizadas en su contra.

Debemos tener en cuenta que toda la actividad que se genera al utilizar el internet, ya sean post, comentarios, fotos, videos, mensajes, es completamente visible y sujeta a referencias o comentarios de terceros (Giones-Valls & Serrat-Brustenga, 2010), sin embargo, es inevitable que toda la información que compartimos en redes sea utilizada para fines ilícitos o que no son informados a los titulares, pues como se vio anteriormente, el ciberespacio es el ámbito idóneo para cometer delitos a causa de su nivel de anonimidad, su bajo costo y sin límites de espacio o tiempo. Por lo que se vuelve esencial el mantener el control de nuestra identidad digital y conocer cuánta y qué tipo de información personal asentamos en el internet.

En esta nueva era tecnológica apareció un fenómeno que nunca antes se había visto, la viralización de contenidos, la cual se entiende como la comunicación masiva entre personas de todo el mundo de un contenido (publicación, video, mensaje, fotografía, etc.) sin control alguno (Allende de Llamas, 2016, pág. 25). Este fenómeno entonces trajo como consecuencia que contenido humillante de una persona, en este caso un video, se propague por todo el mundo sin que pueda ser detenido, pues aunque los sitios web eliminen dicho contenido, siempre habrá alguna persona que tomó captura de pantalla o grabó el video y lo guardó en algún soporte físico o electrónico privado.

Muchos son los casos de personas que son grabadas en estado inconveniente que se convierten en la burla de los demás, personas que se equivocan frente a la cámara y su error es viralizado o personas que cometen errores y que se usa la evidencia para juzgar y castigar a la persona. En todos estos casos, los titulares no tienen la oportunidad de defenderse ni dar explicaciones, pues además de la rapidez con que se comparten los videos, al sacarse del contexto en el que fueron grabados pueden ser interpretados de manera errónea y provocar algún tipo de discriminación.

En razón de lo anterior, el aprender a gestionar adecuadamente la propia visibilidad, reputación y privacidad de nuestra identidad digital en la red (Giones-Valls & Serrat-Brustenga, 2010) pues el no hacerlo genera vulnerabilidades que pueden ser utilizadas para cometer ciberdelitos como la suplantación de identidad.

[17] Artículo 6 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares

El deepfake presenta una amenaza grave para la era tecnológica en la que se encuentra la humanidad, pues la difusión masiva de información es indetenible e incontrolable, por lo que un falso video que atente a una persona o que busque mal informar de algún escenario, se vuelve una situación irreparable, pues toma más tiempo rastrear el origen del deepfake que de compartirse en todo el mundo, por ello es importante que conozcamos los alcances del internet y las repercusiones que podría tener el compartir nuestra información personal en las redes, aprendiendo a utilizar las herramientas que tenemos pero protegiendo siempre nuestra esfera de derechos.

Si bien en primera instancia los titulares deben proteger sus datos personales, es importante que los desarrolladores se detengan un poco antes de continuar y el principio de factibilidad sea parte de este proceso de creación el cual refiere a la "posibilidad moral, es decir, que cuenta con las limitaciones que le presenta a la pura factibilidad técnica la factibilidad moral" (Dussel, 2014, pág. 71). Esto refiere a que la factibilidad, en referencia a lo que puede hacerse, reproducirse o efectuarse (Dussel, 2014, pág. 72), en los aspectos económicos y técnicos (Teruel, 2017) es decir, que la posibilidad de crear algo en el aspecto de los recursos que se utilizarían y lo materialmente viable, sean la única razón para seguir adelante con las creaciones. Según (Teruel, 2017) "el criterio de factibilidad queda definido por la posibilidad empírico-tecnológica y económico histórica de poder contextualmente realizar algo: el fin puede ser realizado exclusivamente por ciertos medios, elegido mediante el cálculo y usado de determinada manera" (pág.5). La factibilidad moral refiere a que "la moral deberá situarse en la condición humana posible, real, pero no descartará el horizonte utópico como un postulado que puede iluminar la elección de las mediaciones moralmente posibles" (Dussel, 2014, pág. 73).

Esto puede resumirse a que si tenemos la posibilidad de hacer algo, no significa que debamos hacerlo o que exista una obligación de realizarlo, pues los aspectos morales deben de detener la creación de algo por el simple hecho de poder hacerlo. En este sentido, según (Teruel, 2017, pág. 6) "lo decidido a realizarse, con factibilidad técnico-económica, alcanza posibilidad ética cuando es sometido a juicio material de la razón práctico-material o ético originaria". Esto engloba la visión de los derechos humanos en las creaciones, es decir, que las nuevas tecnologías se enfoquen en respetar los derechos humanos y contemplar todos los aspectos morales que su realización acarrearía. Esto debe aplicarse a todo aquello que se desarrolle en base a los datos biométricos de las personas, pues como vimos anteriormente, el derecho al honor y a la protección de los datos personales van íntimamente ligados a la recabación de los datos biométricos, pues estos datos son los que nos identifican visiblemente en una sociedad y que nos hacen biológicamente únicos.

Es por ello que la ética por diseño, refiere a que los diseñadores deben crear productos que contemplen la perfección y si realmente deben de crearse (Ethics for Design), este manifiesto se enfoca a cualquier persona, está planteado para que todas las personas en cualquier disciplina formen parte de la discusión sobre la ética y tomen decisiones informadas sin importar el nivel de conocimiento que se tenga de los lineamientos éticos de cara área de aplicación (Mulvenna, Boger, & Bond, 2017). Al diseñar productos, se debe pensar en las implicaciones que tendrían para los usuarios de los mismos, así como los límites que podría llegar a sobrepasar, teniendo en cuenta el contexto ético antes de llevarlo a cabo, no traer el contexto ético al producto terminado y considerar el contexto ético una vez creado y en funcionamiento.

Aunque se intente llegar a una regularización del diseño y creación de tecnologías, el ritmo en el que se desarrollan dificulta la legislación, por lo que es importante que las personas tomen precauciones para proteger su identidad digital.

Recomendaciones para proteger nuestra identidad en el ciberespacio.

Es importante tener en cuenta que en primera instancia, seamos nosotros quienes cuidemos nuestros datos personales, pues si evitamos su filtración y protegemos nuestra esfera de derechos, evitamos la mayoría de las vulneraciones que podrían ocurrir. Por ello, la educación enfocada al uso responsable de las redes e internet, es fundamental para una sociedad que se desarrolla no solo en el plano físico, sino también el virtual.

Aunque no podemos evitar ataques al cien por ciento, si ponemos en práctica algunas acciones podemos reducir este riesgo. El uso responsable de las redes sociales como Facebook, Twitter, Instagram y demás redes sociales es primordial para la gestión adecuada de nuestra identidad digital, siendo el tema principal el saber qué información no debe ser publicada en redes sociales. Los datos personales son aquellos que nos hacen identificables[18], por lo tanto debemos evitar compartir información que nos identifique. Así como debemos aprender a gestionar nuestra identidad digital, debemos cuidarla, controlando la información de nosotros que se encuentra en el ciberespacio, pues en algunos casos es tan amplia que no tenemos muy claro en donde se encuentra, por lo que el llevar un control de las páginas que nos piden información y reducir al mínimo la que entregamos, hace más fácil que sepamos qué información personal está en riesgo y qué se podría hacer con ella.

Como se vio anteriormente, para crear un deepfake, es necesario un conjunto de imágenes para ser estudiadas y reproducidas digitalmente, por lo que una medida de precaución sería reducir el número de fotografías de primer plano de nuestro rostro que compartimos en las redes, o configurar la privacidad para que sólo las personas de nuestro círculo social tengan acceso a ellas.

Si reducimos la información que compartimos en redes como datos personales, actividades, lugares visitados entre otros e implementamos buenas prácticas, por ejemplo no utilizar el nombre completo en el usuario de una red social, sino de preferencia usar los apodos por los que nuestro círculo cercano nos identifica o solamente el nombre y un apellido, así no nos pueden buscar en bases de datos; reducimos el riesgo de ser suplantados en el ciberespacio, pues los criminales no tienen a la mano la información que necesitan para llevar a cabo el ciberdelito.

En referencia a los datos biométricos, podemos observar que la tendencia es que cualquier programa, aplicación, empresa, etcétera, utilizan como forma de acceso o de autenticación datos biométricos como la huella digital o la identificación facial, por un lado para hacerlo más rápido y más práctico, sin embargo, esto provoca que nuestros datos biométricos se encuentren cada vez más en riesgo, pues la probabilidad de ser robados aumenta cada vez que los entregamos. Es por ello, que como titulares de estos datos, nos neguemos a entregarlos sin solicitar el aviso de privacidad[19] y sin preguntar las finalidades, solicitando que esta identificación se haga por otros medios que no requieran datos biométricos.

En la actualidad, no existe regulación alguna sobre el uso de la identificación facial (Arreola, 2019), por lo que es importante que seamos nosotros los que en primera instancia evitemos entregar nuestros datos biométricos y exijamos que se nos fundamente el requerimiento de los mismos, pues si bien es cierto que la utilización de la identificación facial no está regulada, es obligación de los particulares cumplir con el principio de licitud[20] y recabar los datos con fundamento legal aplicable, pues el consentimiento libre e informado es la clave para que los datos biométricos se entreguen de forma responsable y que el titular tenga la certeza del fin para los que se utilizarán sus datos biométricos.

[18] Artículo 3.1 fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Jalisco y sus Municipios.

[19] Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales. Artículo 3 fracción I de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

[20] Artículo 7 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Conclusiones

El acelerado crecimiento de las tecnologías que envuelven aspectos físicos, electrónicos y biológicos, ha traído una nueva discusión a la conversación sobre la ética en la creación de tecnologías y los derechos humanos, pues la utilización de datos biométricos pone en riesgo otros derechos, riesgos que no han sido discutidos antes de la aparición de las novedades tecnológicas como lo son la identificación facial y los programas de suplantación facial. Sin embargo, el propio crecimiento rápido de las tecnologías hace casi imposible la regulación de las mismas, por lo que la prevención es la única forma con la que contamos actualmente para no ser víctimas de esta nueva práctica.

La suplantación de identidad en imágenes no estáticas representa una amenaza no solo a la intimidad y privacidad de las personas, sino que atenta directamente al derecho al honor el cual es un bien social muy preciado en esta era de transmisión masiva de información, pues la creación de videos deepfake donde se falsee las acciones de una persona puede traer repercusiones en su honor y reputación, pues la vergüenza a la que es sometida la víctima es de imposible reparación, pues el escrutinio y la burla pública no son fáciles de ignorar y borrar de la mente de las personas.

Como se vio a lo largo de este trabajo, el deepfake es posible a través de la recopilación de imágenes para recrear una máscara digital que se implanta en los videos que se quieren falsificar, de esta forma se tienen distintos ángulos y perspectivas del rostro de la persona, para implementarlas en el video y hacer que parezca real. A consecuencia de esto, si las personas suben constantemente fotografías suyas a redes sociales, estamos entregando todos los recursos necesarios para que se realicen deepfakes de nosotros, pues las fotografías que se comparten son de diferentes momentos y ángulos, haciendo más fácil el trabajo de los falsificadores.

Es por ello que los titulares de estas fotografías deben ser la primera barrera para proteger su imagen, teniendo una cultura de protección de datos personales y uso responsable de las redes sociales, reduciendo la cantidad de información que vierten en el ciberespacio y restringir el acceso que se tiene a ella, pensando en las consecuencias que puede traer la apertura masiva a nuestra privacidad y el compartimiento irresponsable y desmedido de nuestra propia imagen. Por lo tanto, la responsabilidad para evitar ser víctimas del deepfake recae en los propios titulares, compartiendo nuestra información en redes de forma responsable y consciente de todos los peligros que ello conlleva.

Aunque la tecnología siga avanzando y sea más y más sofisticada, si nosotros protegemos nuestra imagen y eliminamos a personas que no conocemos de nuestras redes sociales y evitamos lo más posible compartir fotografías nuestras en primer plano, reducimos en gran porcentaje la posibilidad de ser víctimas del deepfake, pues no importa la regularización que puedan llegar a tener estas tecnologías, el beneficio y la facilidad de utilizarlas para fines lucrativos ilegales o moralmente inaceptables, seguirá siendo atractiva y monetariamente efectiva.

A pesar de que las celebridades son potenciales víctimas de esta falsificación por la condición de persona publica y el interés que generan en la sociedad, su misma fama y apertura provoca que cuando vemos videos pornográficos o socialmente incorrectos la mayoría de las personas asumimos que son falsos, pues es ampliamente conocido que estas personas son el blanco fácil para estas prácticas, caso contrario con el resto de las personas, pues su vida no es tan pública ni tan abierta, por lo que al aparecer estos videos las personas que rodean a la víctima del deepfake podrían asumir de primera mano que son reales, sin prestar tanta atención a detalles que hacen sospechar de la falsedad de los mismos.

La cultura de la protección de nuestros datos personales es la única forma de reducir la posibilidad de ser blanco de ataques a nuestra reputación y a nuestro honor por la creación de deepfakes, pues mientras menos información nuestra vertamos en redes para ser robada, menos elementos se tendrán para usar-

los en nuestra contra. Si las personas conocen todos los peligros que conlleva la excesiva apertura al de compartir nuestros datos personales y se toman precauciones para evitar que nuestras fotografías caigan en manos equivocadas, el riesgo podría reducirse y las posibilidades de ser víctimas de esta suplantación de identidad se verán minimizadas.

Mi propuesta para resolver este problema es que se realicen contenidos educativos para que los niños y adolescentes que empiezan a utilizar las redes sociales y el internet en general, conozcan los ciberdelitos y sepan cómo evitar ser víctima de ellos, al igual que hacer campañas informativas en medios de comunicación para que las personas conozcan estas prácticas y utilicen las redes sociales de forma responsable. Me parece también importante que en las familias exista una cultura de protección de datos personales, enseñándoles a los integrantes del núcleo familiar el uso responsable de redes y los peligros y consecuencias posibles que se podrían presentar si se comparten fotografías de forma desmedida.

Caheri
Amaya Corona

Nacida en Guadalajara, Jalisco. Abogada por la Universidad de Guadalajara, Especialista en Gestión, Publicación y Protección de Información por el Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales, con Diplomado en Desarrollo Humano por la Universidad del Valle de Atemajac. Encargada de Medición de la Dirección de Protección de Datos Personales del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco desde Septiembre del 2018.

Referencias

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (24 de marzo de 2018). *FaceForensics :A Large-scale Video Data set for Forger y Detectionin Human Faces.* Munich, Alemania.

Aguirre Romero, J. (2004). *Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI*. Universidad Complutense de Madrid. Obtenido de http://www.ucm.es/info/especulo/numero27/cibercom.html

Allende de Llamas, A. (Julio de 2016). *Viralizando en la Web.* (F. Knop, Ed.) Escritos en la Facultad(118), 25.

Arreola, J. (26 de marzo de 2019). *Forbes México.* Obtenido de https://www.forbes.com.mx/ruta-a-la-regulacion-del-reconocimiento-facial/

AsiaNews.it. (13 de abril de 2018). *Jammu y Cachemira: Violación grupal de Asifa Bano, ocho años. La protesta de la sociedad.* AsiaNews.it. Obtenido de http://www.asianews.it/noticias-es/Jammu-y-Cachemira:-Violaci%C3%B3n-grupal-de-Asifa-Bano,-ocho-a%C3%B1os.-La-protesta-de-la-sociedad-43616.html

Avast Software. (2015). *Phishing.* Avast. Obtenido de https://www.avast.com/es-es/c-phishing

Ayyub, R. (21 de noviembre de 2018). *I Was The Victim Of A Deepfake Porn Plot Intended To Silence Me. Huffpost.* (Huffington Post UK). Obtenido de https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316

Caldera-Serrano, J., & Zapico-Alonso, F. (julio- agosto de 2009). *Identificación Facial Biométrica.* El profesional de la Información, 18(4), 427-431. Obtenido de https://recyt.fecyt.es/index.php/EPI/article/viewFile/epi.2009.jul.11/21552

Camacho, K. (2005). *La Brecha Digital.* En Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información. (pág. 656). C & F Éditions. Obtenido de https://vecam.org/archives/article550.html

Ciberseguridad LATAM. (s.f.). *Deepfake la veganza porno del momento.* Ciberseguridad LATAM. Recuperado el 27 de septiembre de 2019, de https://www.ciberseguridadlatam.com/2018/05/08/deepfake-la-venganza-porno-del-momento/

Ciberseguridad LATAM. (s.f.). *Facebook y Microsoft unen fuerzas para detectar videos falsos.* Ciberseguridad LATAM. Recuperado el 27 de septiembre de 2019, de https://www.ciberseguridadlatam.com/2019/09/08/facebook-y-microsoft-unen-fuerzas-para-detectar-videos-falsos/

Delp, E., & Güera, D. (Noviembre de 2018). *Deepfake Video Detection Using Recurrent Neural Networks.* Proceedings of AVSS 2018, 17, 580. Obtenido de https://ieeexplore.ieee.org/abstract/document/8639163

Desk, I. T. (21 de noviembre de 2018). *I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot.* India Today. Obtenido de https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21

Domínguez Espinosa, A., Aguilera Mijares, S., Acosta Canales, T., Navarro Contreras, G., & Ruiz Paniagua, Z. (2012). *La deseabilidad social revalorada: más que una distorsión, una necesidad de aprobación social.* Acta de investigación psicológica(2), 808-824. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-48322012000300005&lng=es&tlng=es.

Dussel, E. (2014). 14 Tesis de Ética, *El fundamento esencial del pensamiento crítico.*

elmundo.com.ve. (2013 de agosto de 2013).*Conozca las industrias que más dinero mueven a nivel global.* America Economía. Obtenido de https://www.americaeconomia.com/economia-mercados/finanzas/conozca-las-industrias-que-mas-dinero-mueven-nivel-global

Espinoza Olguín, D. E., & Jorquera Guillen, P. I. (Junio de 2015). *Reconocimiento Facial.* Pontificia Universidad Católica De Valparaíso.

Ethics for Design. (s.f.). *Ethics for Design.* Obtenido de https://ethicsfordesign.com/

Ferran-Ferrer , N., & Pérez-Montoro, M. (julio-agosto de 2009). *Gestión de la información personal en usuarios avanzados en TIC.* El profesional de la Información, 18(4), 365-373.

Foundation, T. T. (2018). *The world's most dangerous countries for women.*The Thomson Reuters Foundation Annual Poll. Obtenido de http://poll2018.trust.org/

Franganillo, J. (Julio-Agosto de 2009). Gestión de información personal: elementos, actividades e integración. *El profesional de la Información*, 18(4), 399-406. Obtenido de https://dialnet.unirioja.es/ejemplar/233068

Giones-Valls, A., & Serrat-Brustenga, M. (Junio de 2010). *La gestión de la identidad digital: una nueva habilidad informacional y digital.* Textos universitaris de biblioteconomía i documentació(24). Obtenido de http://bid.ub.edu/24/giones2.htm

Harris, D. (05 de Junio de 2019). *Deepfakes: False Pornography Is Here and the Law Cannot Protect You.* Obtenido de Duke Law and Technology Review: https://dltr.law.duke.edu/

Heiderscheid, N. (Julio de 2016). *Las redes sociales y la necesidad de mostrarse.* Escritos en la Facultad(118), 104.

Instituto Nacional de Transparencia, Información Pública y Protección de Datos Personales. (Junio de 2015). *Metodología Beneficio, Anonimidad del Atacante BAA.* INAI. Obtenido de http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m3

Instituto Nacional de Transparencia, Información Pública y Protección de Datos Personales. (Marzo de 2018). *Guía para el Tratamiento de Datos Biométricos.* Ciudad de México, Coyoacán, México. Obtenido de http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4

Korshunov, P., & Marcel, S. (2018). *Deepfakes: a new threat to face recognition? Assessment and detection.* IDIAP Research Institute. Martigny: IDIAP Research Institut. Obtenido de http://publications.idiap.ch/downloads/reports/2018/Korshunov_Idiap-RR-18-2018.pdf

K Kulp, P. (02 de Noviembre de 2017). *Facebook admits to nearly as many fake or clone accounts as the U.S. population.* Mashable. Obtenido de https://mashable.com/2017/11/02/facebook-phony-accounts-admission/#Ka8aV2qMkPq3

Martínez de Pisón, J. (1997). *Vida privada e intimidad:implicaciones y perversiones.* En U. d. Rioja, & S. E. BOE (Ed.), Anuario de la Filosofía del Derecho XIV (Vol. 14, págs. 717-738). La Rioja: Ministerio de Justicia.

McSweeny, T. (2018). *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is The FTC Keeping Pace?* Georgetown Law Technology Review, 2.2(514), 514-530.

Mulvenna, M., Boger, J., & Bond, R. (2017). *Ethical by Design, a Manifesto.* (U. University, Ed.) Coleraine, Irlanda del Norte, Reino Unido.

Nguyen, H., Yamagishi, J., & Ech, I. (26 de Octubre de 2018). *Capsule-Forensics: Using Capsule Networks to Detect Forged Images and Videos.* Kanagawa, Japón: The Graduate University for Advanced Studies.

ONU, O. d. (10 de diciembre de 1948). *Declaración Universal de los Derechos Humanos.* Naciones Unidas. Obtenido de https://www.un.org/es/universal-declaration-human-rights/

Ortega García, J., Alonso Fernández, F., & Coomonte Belmonte, R. (Mayo de 2008). *Biometría y Seguridad.* (F. R. Segovia, Ed.) Cuadernos de Cátedra ISDEFE-UPM, 3-132.

Pons Gamón, V. (2017). *Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad.* Revista Latinoamericana de Estudios de Seguridad, 20, 80-93. Obtenido de http://dx.doi.org/https://doi.org/10.17141/urvio.20.2017.2563

Riande Juárez, N. A. (s.f.). *Privacidad, autodeterminación informativa y la responsabilidad de proteger los bienes de uso común.* Orden Jurídico. Obtenido de www.ordenjuridico.gob.mx/Congreso/pdf/103.pdf

Safi, M. (15 de abril de 2018). *Extremistas hindúes en India frenan la investigación de la violación y asesinato de una niña musulmana.* eldiario.es. Obtenido de https://www.eldiario.es/theguardian/Extremistas-investigacion-violacion-asesinato-India_0_760474279.html

Security, P. (22 de febrero de 2017). *Revenge Porn: qué es y cómo evitar ser víctima.* Panda Mediacenter. Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/revenge-porn-victima/

Smith, C. (18 de Septiembre de 2013). *Facebook Users Are Uploading 350 Million New Photos Each Day.* Business Insider. Obtenido de https://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9?IR=T

Sola-Martínez, M.-J. (julio-agosto de 2009). *Redes sociales: más allá de la privacidad.* El profesional de la Información, 18(4), 470-474. Obtenido de https://dialnet.unirioja.es/ejemplar/233068

Teruel, F. (2017). Sesión 4. *Factibilidad ética: el "bien".* Seminario Permanente 2017, Filosofía de la liberación. Perspectivas y prospectivas. Ciudad de México, México: Universidad Autónoma de la Ciudad de México.

Ursua, N. (Noviembre-Diciembre de 2006). *La(s) identidades(es) en el ciberespacio. Una reflexión sobre la construcción de las identidades en la red ("online Identity").* Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación(7), 277-296. Obtenido de https://www.oei.es/historico/revistactsi/numero7/articulo03.htm

Vaas, L. (09 de agosto de 2018). *Darpa takes aim at deepfake forgeries.* Naked Security by Sophos. (Sophos Ltd) Recuperado el 27 de septiembre de 2019, de https://nakedsecurity.sophos.com/es/2018/08/09/darpa-takes-aim-at-deepfake-forgeries/

Villanueva-Turnes, A. (2016). *El derecho al honor, a la intimidad y a la propia imagen, y su choque con el derecho a la libertad de expresión y de información en el ordenamiento jurídico español.* Díkaion, 25(2), 190-215.

Wallace, J. B. (4 de Mayo de 2018). *The teenage social media trap.* The Wall Street Journal. Obtenido de https://www.wsj.com/articles/the-teenage-social-media-trap-1525444767?ns=prod/accounts-wsj