Caja de Cristal

Publicación Semestral de Transparencia y Acceso a la Información

Año 7 - No. 13
Enero - Julio 2021

itei

INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE JALISCO

Contenido

Portada
Gestión, Publicación y Protección de Información
Fotografía: Metamorworks for Adobe Stock
Montaje: Juan Francisco García Gallegos

Revista CAJA DE CRISTAL, Año 7, No. 13, enero - julio 2021, es una publicación semestral editada por el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. Avenida Ignacio L. Vallarta No. 1312, Col. Americana, Guadalajara, Jalisco, México, C.P. 44160, Tel. (33) 3630-5745, www.itei.org.mx. Editor responsable: Salvador Romero Espinosa Reserva de Derechos al Uso Exclusivo: 04-2016-051812313300-102 e ISSN: 2448-5098, ambos otorgados por el Instituto Nacional del Derechos de Autor.

Introducción

Me es muy grato el presentarles este número, toda vez que constituye para mi uno de mucha relevancia, pues por primera vez se publicará un artículo de mi autoría en la Revista Caja de Cristal, aunque debo aclarar que cuando lo escribí, no tenía previsto que algún día culminaría en las páginas de una publicación tan importante como esta.

Es considerable recordar que esta publicación, es el producto de un incesante esfuerzo del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) por acercar a toda la sociedad en general, y particularmente a toda aquella interesada en temas sobre transparencia, derecho a la información, privacidad, derecho a la protección de datos personales, rendición de cuentas y democracia, la mayor cantidad de insumos posibles para entender estos derechos, ejercerlos y, eventualmente, defenderlos.

En ese contexto, es un hecho que mucha de la investigación, análisis y disertación sobre estos temas se realiza en las aulas, especialmente de aquellos programas especializados en dichas materias, tales como cursos, talleres, diplomados, especialidades y maestrías, es por ello que desde hace 4 años que asumí la responsabilidad de dirigir esta revista, he volteado siempre a ver a la comunidad estudiantil como una de las fuentes de artículos más importantes para las materias que aquí se difunden.

Por ello es que el número 13 de la Revista Caja de Cristal que tienes en tus manos, se encuentra nutrido del segundo bloque de los 16 trabajos académicos mejor calificados y de mayor relevancia -de acuerdo con el Comité Dictaminador- producidos por las y los alumnos graduados de la Especialidad en Gestión, Publicación y Protección de Información, impartida durante el año 2019 por el Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales (CESIP) de este Instituto.

Aunque lo comenté en el número anterior, me parece relevante reiterar que todos los artículos que se publican en esta edición, además de cumplir con los requisitos de forma aprobados por los Lineamientos correspondientes (mismos que han sido publicados en esta Revista para mayor referencia de sus lectores) se apegaron de origen a los temas revisados en el programa de la referida especialidad, y fueron posteriormente calificados, revisados y dictaminados por especialistas en dichos temas, mediante el sistema “Doble Ciego” (Double-blind peer review), con el objeto de garantizar una calidad óptima.

Finalmente quiero reiterar, como en el número anterior, el agradecimiento a mis compañeros Cynthia y Pedro por su apoyo y confianza para seguir encabezando los esfuerzos de impulsar nuestra Revista Caja de Cristal, así como a los maestros Manuel Rojas Munguía y Víctor Saavedra, a las licenciadas Jaqueline Alonso, Arani Hernández y Jessica Mejía, por haber organizado y desarrollado con absoluto éxito

la primera Especialidad de esta naturaleza en México, sin olvidar por supuesto a todas las profesoras y profesores que sin ninguna remuneración de por medio, compartieron a lo largo de todo un año sus conocimientos con los y las alumnas de dicha especialidad, que hoy veo recompensado nuevamente con la publicación de mi trabajo de titulación.

Salvador Romero Espinosa
Director de Caja de Cristal

Presentación

Esta es la segunda de dos ediciones de la revista Caja de Cristal, dedicadas a la producción de conocimiento que surge de la comunidad académica del Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales (CESIP), en específico de quienes egresaron de la Especialidad en Gestión, Publicación y Protección de Información, posgrado del cual surgen reflexiones y propuestas orientadas a profundizar en el estudio de los temas inherentes a los derechos tutelados por el organismo garante de Jalisco.

En esta ocasión se analizan temas como gestión documental, acceso a la información y derechos de autor, pero se pone el acento en la protección de datos personales ante los retos que van más allá de lo estrictamente jurídico, por lo que el análisis académico es necesario para lograr una mejor comprensión de los fenómenos aquí estudiados y presentados.

Así, inicia esta edición con el trabajo de Caheri Amaya Corona en el cual nos presenta la que es una de las grandes amenazas para el honor, la reputación de las personas y desde luego, la protección de datos personales: la tecnología existente que permite suplantar la identidad de las personas en imágenes no estáticas con todas las implicaciones que ello conlleva y que puede incluso, tener alcances internacionales por potenciales conflictos diplomáticos.

Sigue el análisis de Geronimo Anguiano Ruiz, en el cual advierte que la autonomía constitucional de la que gozan los organismos garantes es en realidad una utopía y pone, como caso de estudio al ITEI, que históricamente ha sufrido la intromisión desde el Poder Ejecutivo para asignarle techos presupuestales al momento de diseñar el Anteproyecto de Presupuesto, lo que en la práctica pone en riesgo los derechos humanos de los jaliscienses: el de acceso a la información pública y a la protección de sus datos personales.

En el ámbito de la gestión documental, Karen Michelle Martínez Ramírez analiza los alcances que tienen la Ley General de Archivos y los Lineamientos para la Organización y Conservación de Archivos, emitidos por el Sistema Nacional de Transparencia, respecto al resguardo (o custodia) de los documentos de archivo que generan, reciben y administran las entidades públicas.

Y precisamente en torno a los retos que conlleva la gestión de información en instituciones públicas, María del Rosario Navarro Zamora nos muestra la vulnerabilidad que puede existir en el contexto actual en que todo es digital y pone como ejemplo al propio INAI y en específico a la Plataforma Nacional de Transparencia, que en un lapso de 10 meses sufrió casi 78 mil ataques cibernéticos.

En este mismo sentido, Luis Abraham Rincón Prieto subraya la vulnerabilidad que prevalece al hacer uso de redes sociales, aplicaciones, plataformas digitales, y/o dispositivos con sensores de monitoreo que, sumado a la falta de capacitación dificulta la prevención de ciberdelitos y con ello el probable robo de datos personales.

La realidad es compleja y multifactorial y por ello destaca el análisis que hace Rafael Ríos Nuño acerca de la colisión de derechos que se presenta cuando se enfrentan derechos de autor, de acceso a la información, a la privacidad y a la protección de datos personales, como sucede cuando en libros y/o archivos encontramos prohibiciones expresas a la reproducción o difusión de obras artísticas o literarias y por ello el autor propone una solución mediante una interpretación de las doctrinas del fair use y transformative use.

Por supuesto, la convergencia de derechos y constantes conflictos entre ellos en las redes sociales digitales, son materia de análisis por parte de Salvador Romero Espinosa, ya que los derechos a la información, a la protección de datos personales y a la libre expresión, adquieren especial relevancia para la discusión pública en toda sociedad que aspira a tener una democracia de calidad.

Y cierra esta edición con una reflexión de María del Carmen Silva Ramírez en torno a lo que ella identifica como la necesidad de que en la gestión documental dentro de una institución, haya un mejor marco jurídico pero también personas calificadas para realizar la debida recepción y derivación de la documentación que se ingresa a las dependencias.

Sin lugar a dudas, esta segunda edición de Caja de Cristal dedicada a enriquecer la discusión pública con pensamiento generado en el posgrado del ITEI, contribuirá a problematizar situaciones que se viven en el día a día dentro de quienes nos dedicamos a la defensa de dos derechos humanos tan importantes e íntimamente ligados con la democracia, tan ávida hoy en día de ser pulida en el crisol del pensamiento crítico.

Seguro estoy que la lectura de los trabajos aquí publicados serán referente para quienes en el mundo de la vida trabajamos en aras del acceso a la información y la protección de datos personales, pero también para quienes desde la academia estudian, analizan y cuestionan para proponer nuevas formas de entender y vivir los derechos consagrados en los artículos 6 y 16 de la Constitución.

Finalmente, pero no por ello menos importante, esta edición refrenda el liderazgo y compromiso del ITEI que, pese a los escasos recursos, persevera para desde distintos ámbitos defender, promover y garantizar los derechos humanos en México y en nuestro estado.

Pedro Antonio Rosas Hernández
Comisionado del ITEI

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:

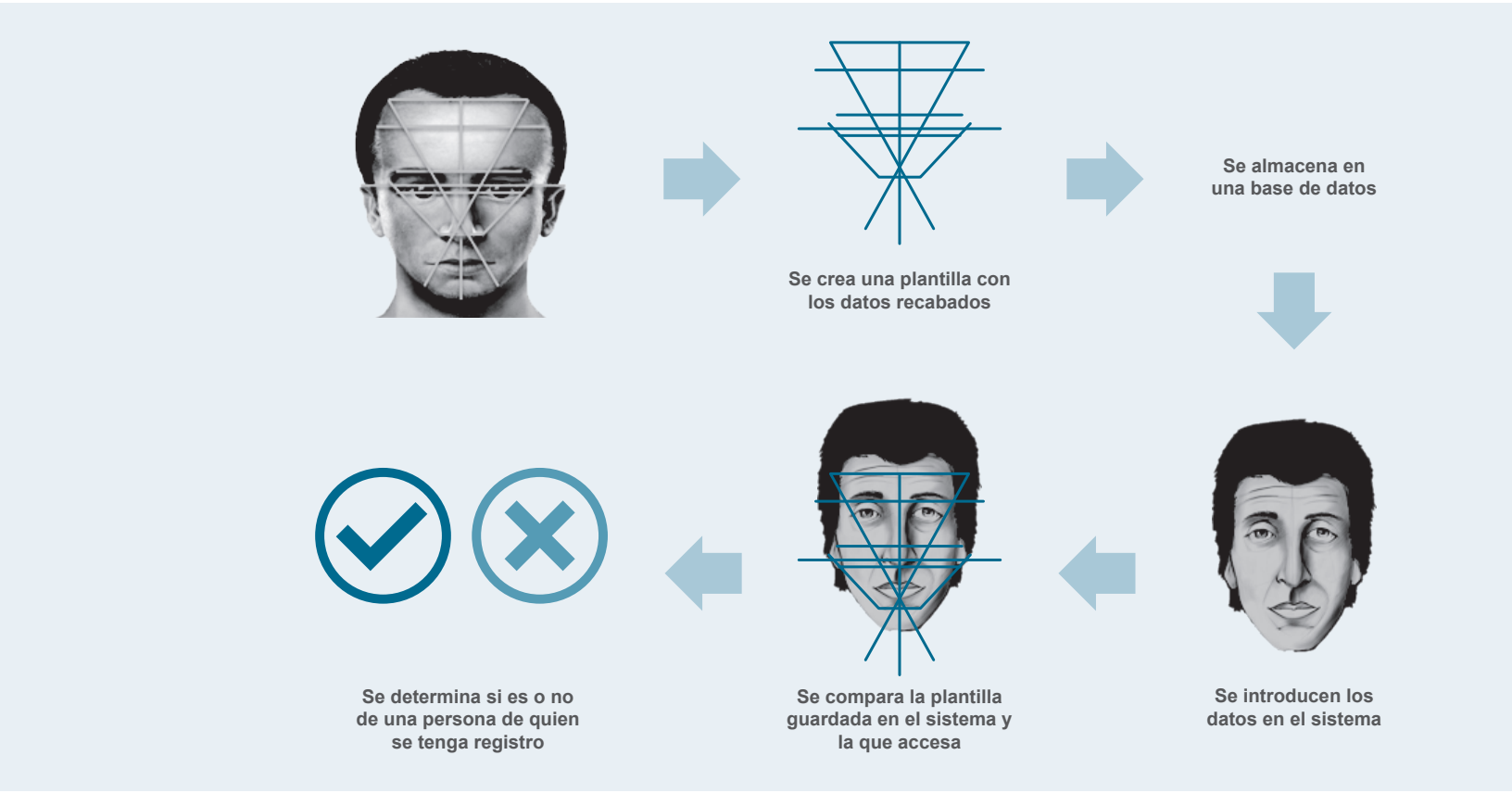


Figura 2. Proceso de identificación facial biométrica. Representación sencilla del proceso que implica la identificación facial. Autoría propia.

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:

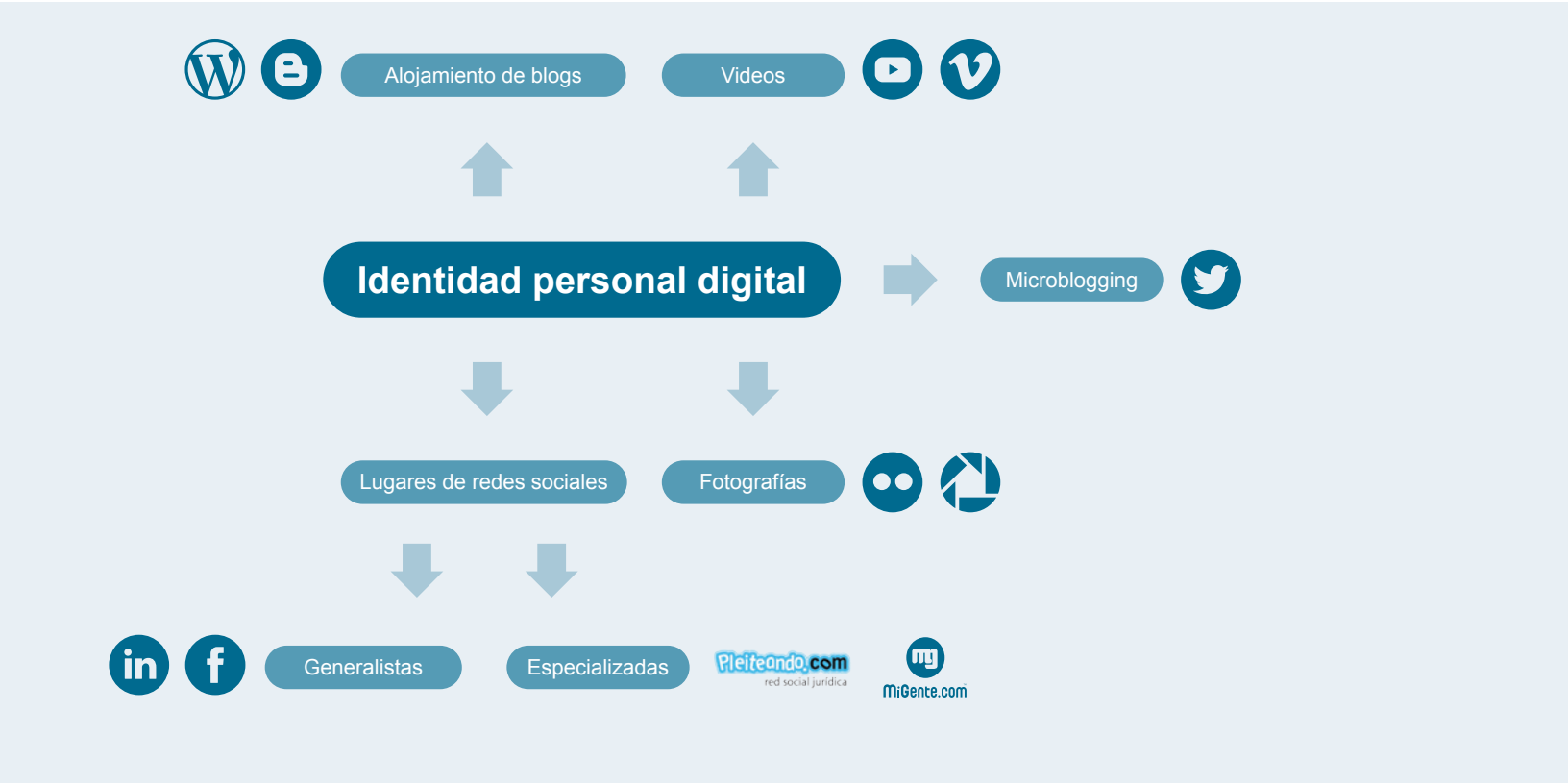


Figura 1. Ejemplo de las identidades digitales. Representación de lo que puede conformar una identidad digital, dependiendo del uso y la navegación del usuario. (Giones-Valls & Serrat-Brustenga, 2010, pág. 4)

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

TRANSPARENCIA PILAR DE LA DEMOCRACIA

itei | INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE JALISCO

www.itei.org.mx

Fotografía: Cottonbro para Pexels.com

Autonomía presupuestaria, una utopía de los organismos constitucionales; caso de estudio Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI)

Geronimo Anguiano Ruiz

Coordinador de Planeación en el ITEI

Resumen

En el presente artículo se realiza un análisis sobre si existe o no, autonomía presupuestaria de los Organismos Constitucionales Autónomos, con caso de estudio del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI); para lo cual se presenta al lector una breve introducción sobre el proceso de planeación, programación y presupuestación, que dan origen al presente artículo.

Para facilitar la comprensión, se expone el marco jurídico que sustenta dicho proceso, concebido a nivel federal desde la Constitución Política de los Estados Unidos Mexicanos, y los Planes Nacionales de Desarrollo 2007-2012 y 2019-2024 respectivamente, mientras que, a nivel local, la Constitución Política del Estado de Jalisco prevé dicho proceso, que ya fue incorporado al recién aprobado Plan Estatal de Gobernanza y Desarrollo 2018-2024. Visión 2030, teniendo a las leyes de Planeación Participativa para el Estado de Jalisco y sus Municipios y Ley de Presupuesto, Contabilidad y Gasto Público del Estado de Jalisco, como las normas que describen el procedimiento que deben realizar los organismos constitucionales autónomos para la obtención de los recursos públicos.

PALABRAS CLAVES:
Autonomía, Presupuestaria, Organismos, Constitucionales, Autónomos, Jalisco

Toda vez que, a concepto del autor, existe una utopía en relación a la autonomía presupuestaria del ITEI, esto es, que se ven inmersos en un sistema deseable difícil de realizar, por la serie de procesos internos que sobre-regulan esta supuesta autonomía.

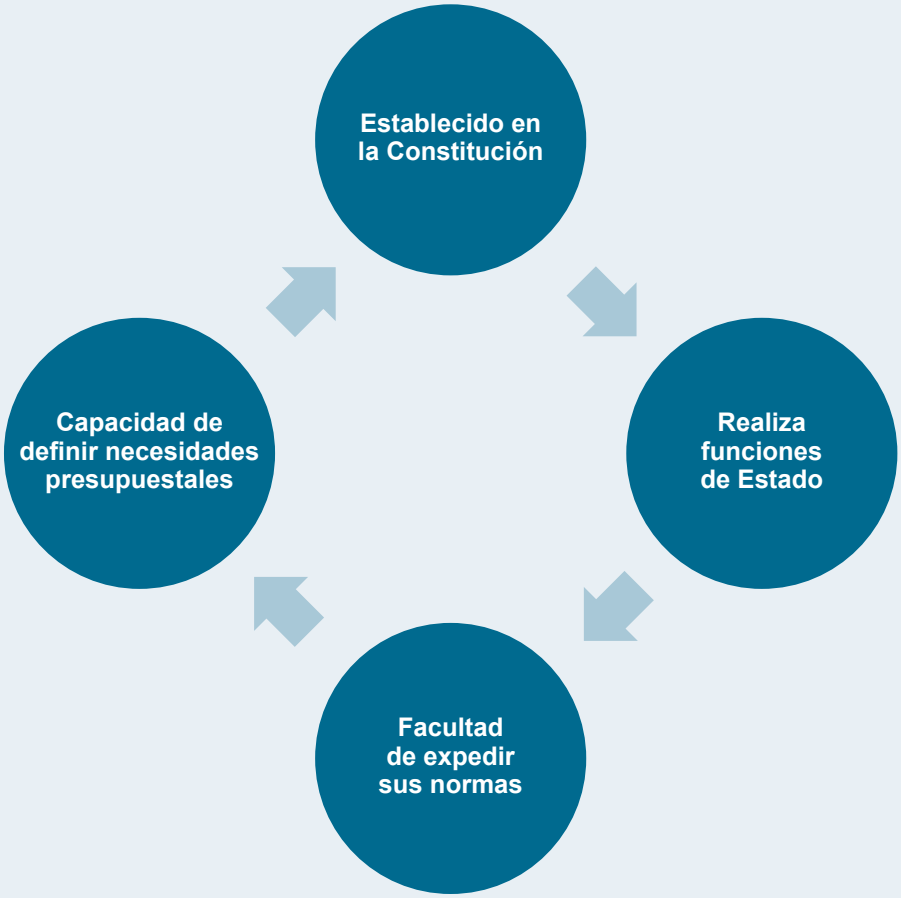
Por lo cual, una vez analizados los hallazgos obtenidos a lo largo de la investigación, se incorpora un apartado de conclusiones, que sirven de sustento para generar propuestas para modificar el estado actual de las cosas.

Introducción

El Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), según lo establece el artículo 33, punto 1, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, es un organismo público autónomo, es decir, no depende de ningún poder (Ejecutivo, Legislativo o Judicial), ya que señala lo siguiente:

> *Artículo 33. Instituto - Naturaleza*
> *1. El Instituto es un organismo público autónomo con personalidad jurídica y patrimonio propios, con autonomía en sus funciones e independencia en sus decisiones y tiene como funciones, promover la transparencia, garantizar el acceso a la información pública de libre acceso y proteger la información pública reservada y confidencial.*

En ese contexto, es importante reflexionar respecto al concepto de autonomía, ya que es: “la facultad que las organizaciones políticas tienen de darse a sí mismas sus leyes y de actuar de acuerdo con ellas (García, 1993, p.104), “También tiene la acepción de ´libre albedrío´ y ´mando propio´” (García, 1977, p. 23), bajo esas premisas, es importante señalar que dichos organismos constitucionales autónomos, cuentan con diversas características, mismas que a continuación se describen:



Fuente: elaboración propia con base a Ugalde (2009, p. 255).

Para efectos de análisis del presente estudio, la autonomía financiera-presupuestal y administrativa con la que cuentan los organismos constitucionales autónomos, esto es, "la capacidad para definir sus necesidades presupuestales y para administrar y emplear sus recursos económicos que les sean asignados" (Ugalde, 2009, p. 256), es lo que se pone en tela de juicio, ya que a concepto del autor, esto resulta ser una utopía, entendiendo esta como un: "Plan, proyecto, doctrina o sistema deseables que parecen de muy difícil realización" (RAE, 23 a ed.), toda vez que en el ciclo presupuestario que da como resultado la elaboración del anteproyecto de presupuesto, este último facultad exclusiva del Ejecutivo del Estado, se transgrede dicho principio, por la serie de procesos que sobre-regulan esta facultad, por lo que para efectos de una mejor comprensión se presenta el marco jurídico que aplica al caso.

Marco jurídico

En nuestro país, la Constitución Política de los Estados Unidos Mexicanos, establece en su artículo 26, inciso A, que la nación organizará un sistema de planeación democrática reflejado a través de un Plan Nacional de Desarrollo al cual se sujetarán los programas de la Administración Pública, ya que textualmente señala lo siguiente:

> *Artículo 26.*
> *A. El Estado organizará un sistema de planeación democrática del desarrollo nacional que imprima solidez, dinamismo, competitividad, permanencia y equidad al crecimiento de la economía para la independencia y la democratización política, social y cultural de la nación (sic)".*

En ese tenor, el Plan Nacional de Desarrollo (PND) 2007-2012, establecía como uno de sus objetivos en materia de política hacendaria para la competitividad: "contar con una hacienda pública responsable, eficiente y equitativa que promueva el desarrollo en un entorno de estabilidad económica" (PND 2007-2012, p.92), situación que fue adoptada en el Plan Nacional de Desarrollo 2019-2024, al señalar lo siguiente: "La Constitución ordena al Estado mexicano velar por la estabilidad de las finanzas públicas y del sistema financiero" (PND 2019-2024, p.6), por lo que el estado mexicano, adoptó la metodología de Presupuesto Basado en Resultados, para hacer frente a esta responsabilidad, entendiendo esta como un modelo que tiene por objeto: "mejorar la eficiencia y eficacia del gasto público estableciendo un vínculo entre el financiamiento de las entidades del sector público, y su desempeño" (Robinson y Duncan, 2009, p. 1).

Bajo esa lógica la Constitución Política del Estado de Jalisco establece en el artículo 50, fracción X, la facultad y obligación del Gobernador del Estado, sobre la conducción de la planeación del desarrollo, al señalar lo siguiente:

> *Artículo 50.- Son facultades y obligaciones del Gobernador del Estado:*
>
> *X. Organizar y conducir la planeación del desarrollo del Estado, velando por la sostenibilidad de las finanzas públicas y establecer los medios para la consulta ciudadana y la participación social (sic)*

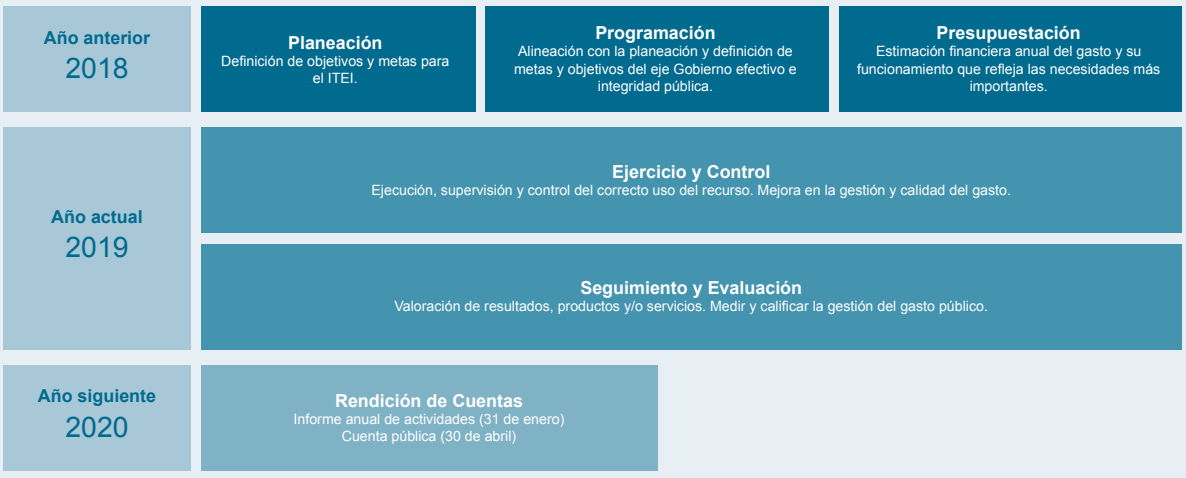
Es por ello, que el recién aprobado Plan Estatal de Gobernanza y Desarrollo de Jalisco 2018 -2024. Visión 2030, documenta que, en nuestra entidad, se implementó un: "Sistema estatal de planeación participativa, monitoreo y evaluación" (PEGD 2018-2024, p.23) que vincula a todos los niveles y poderes del Estado, incluyendo al caso de estudio de este artículo; atendiendo a lo previsto en el artículo 34 de la Ley de Planeación Participativa para el Estado de Jalisco y sus Municipios, que señala lo siguiente:

> *Artículo 34. El Ejecutivo deberá observar el Plan Estatal y los programas que de él se deriven como base para realizar los proyectos de la Ley de Ingresos y del Presupuesto de Egresos del Estado, y precisar los objetivos de los Programas derivados del Plan que deberán cumplirse a través de la aplicación del gasto público durante el ejercicio siguiente.*

Esto es, el Ejecutivo del Estado, al elaborar el proyecto de Presupuesto de Egresos, debe observar el Plan Estatal y los programas que de él deriven, en ese tenor; se presenta a continuación la ruta crítica de integración del proyecto de presupuesto:

Fuente: elaboración propia con base SHP (2019, p. 5)

Para realizar este proceso, la entonces Secretaría de Planeación, Administración y Finanzas del Gobierno del Estado de Jalisco, hoy Secretaría de la Hacienda Pública, "integra el Anteproyecto de Presupuesto de cada anualidad, a través de plataforma denominada: Sistema Estatal de Presupuesto Basado en Resultados 2020 (SEPbR)" (SHP, 2019, p. 6), en dicha plataforma se realiza el proceso de Planeación, Programación y Presupuestación, basado en el siguiente esquema:

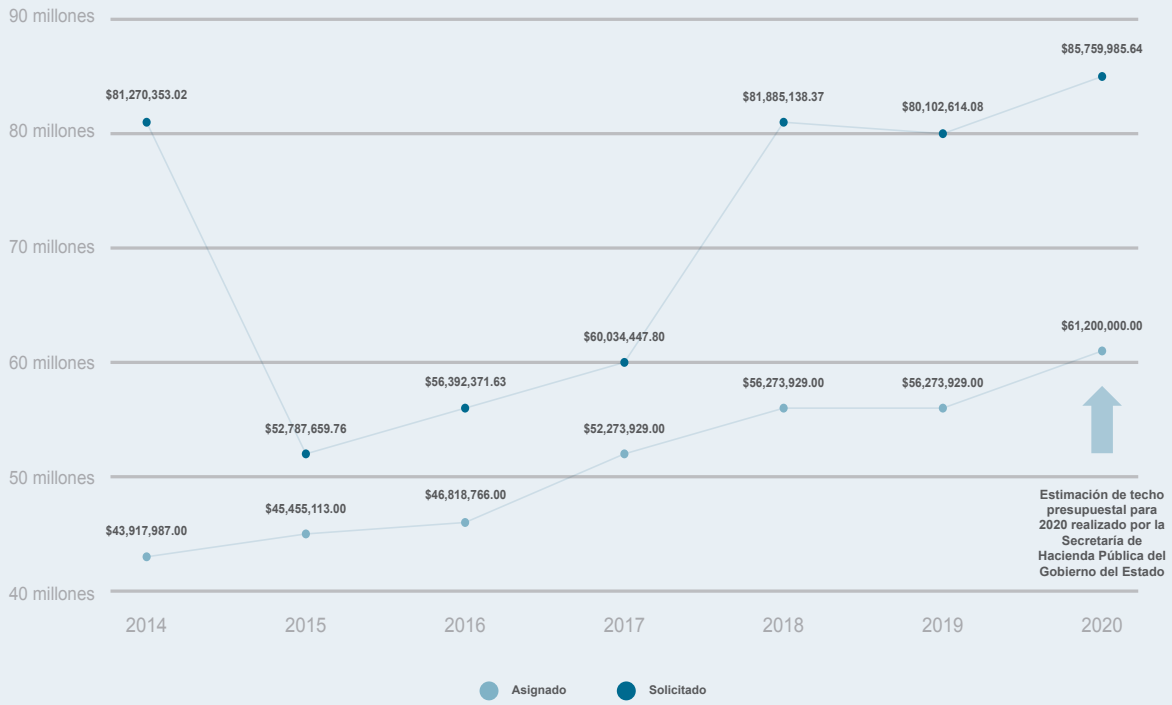


Fuente: elaboración propia con base SHP (2019, p. 6)

Una vez, que se presentó la ruta crítica para la integración del anteproyecto de presupuesto y el esquema de Planeación, Programación, Presupuestación, Ejercicio y Control, Seguimiento y Evaluación y Rendición de Cuentas, como el escenario general del proceso; se presentan los puntos que dan origen a la presente investigación, toda vez que la Ley de Presupuesto, Contabilidad y Gasto Público del Estado de Jalisco, establece en su artículo número 29, los términos y plazos en los que se deberá de integrar y presentar el anteproyecto de presupuesto de las dependencias y entidades (incluyendo a los Organismos Constitucionales Autónomos), ya que señala expresamente lo siguiente:

> *Artículo 29. Para la formulación del proyecto de presupuesto de egresos del Gobierno del Estado, las dependencias y entidades elaborarán sus anteproyectos con base en los programas respectivos, ajustándose a los criterios generales de responsabilidad hacendaria y financiera establecidos en la Ley de Disciplina Financiera de las Entidades Federativas y los Municipios, así como a los principios de racionalidad, austeridad, disciplina presupuestal, motivación, certeza, equidad, proporcionalidad y perspectiva de género, a la ley y a los montos que establezca el titular del Poder Ejecutivo, por conducto de la Secretaría, remitiéndolos, en el caso de las Dependencias, directamente a la Secretaría, a más tardar el 15 de agosto de cada año. Por lo que respecta a las entidades sectorizadas, éstas lo harán por conducto y con la validación de la dependencia coordinadora del sector correspondiente, en el mismo plazo. (sic)*

De lo anterior resulta importante recapitular que el anteproyecto de presupuesto del ITEI, se debe capturar en el sistema que para tal efecto diseñó la Secretaría de la Hacienda Pública del Gobierno del Estado de Jalisco, quien impone como requisito *sine qua non*, para continuar con la captura en el sistema que el Instituto, “acepte” el techo presupuestario que le fue impuesto, argumentando una serie de “Lineamientos Generales de Presupuestación” (SHP, 2019, p. 44 y 45), cifra que termina siendo la que aprueba el Congreso en el Presupuesto de Egresos del Estado de Jalisco, la cual siempre dista a la baja de lo peticionada por el Instituto para cumplir con las atribuciones y obligaciones que se le encomiendan, tal y como se muestra a continuación:



Fuente: Presupuesto de Egresos del ITEI. Información fundamental. URL: https://www.itei.org.mx/v4/index.php/transparencia/fraccion/art8-5c
Periodico Oficial "El Estado de Jalisco", Presupuesto de Egresos del Estado de Jalisco. URL: https://periodicooficial.jalisco.gob.mx/peri%C3%B3dicos/presupuesto-de-egresos

Lo anterior, resulta ser el primer indicio de agravio a la autonomía presupuestaria del Instituto, toda vez que el presupuesto asignado ha estado por debajo de lo solicitado y aprobado por el Pleno del Organismo Garante, y remitido al Ejecutivo para su integración en el Proyecto de Presupuesto de Egresos respectivo, en un 29.9% del año 2015 a la fecha; lo cual se traduce en la imposición de un recurso que no resulta ser suficiente para atender las obligaciones que marcan las normas.

Aunado a lo anterior, se identifica que en el ejercicio fiscal 2019, el presupuesto asignado al Instituto, lo posiciona en el lugar número 23 (veintitrés) a nivel Nacional en cuanto a presupuesto asignado por persona, con $7.10 (siete pesos 10/100 M.N.) (per cápita); siendo el Estado de Quintana Roo (primer lugar) toda vez que asigna $29.99 (veintinueve pesos 99/100 M.N.) por persona, y el Estado de Chiapas se ubicaba en el último lugar, ya que destina tan solo

$1.80 (un peso 80/100 M.N.) por persona, tal y como se muestra a continuación:

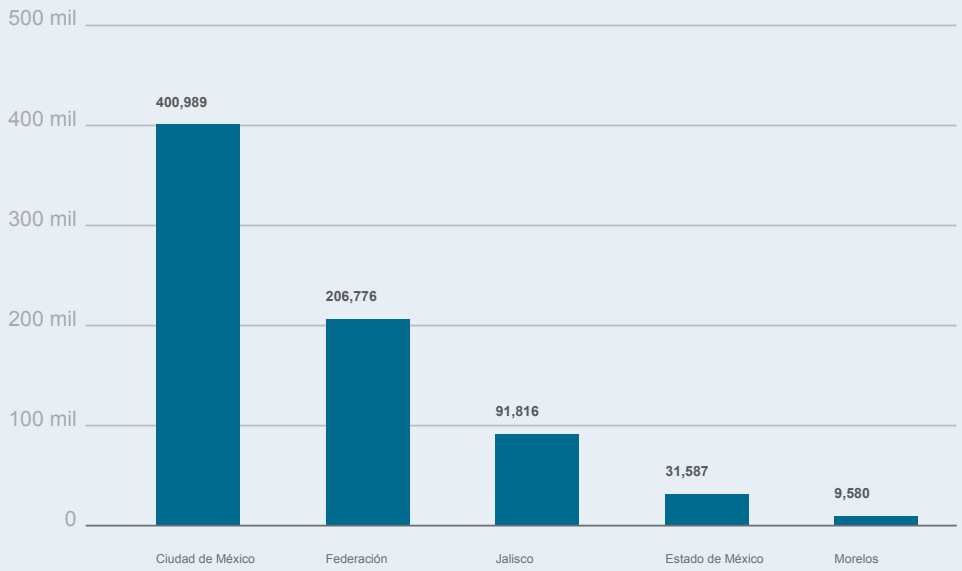
No.	Entidad Federativa	Presupuesto asignado 2019	Cantidad de Población	Per cápita
1	Quintana Roo	45,040,000	1,501,562	29.99
2	Campeche	21,620,000	899,931	24.02
3	Aguascalientes	22,260,000	1,312,544	16.95
4	Ciudad de México	143,440,000	8,918,653	16.08
5	Coahuila	45,640,000	2,954,915	15.44
6	Nuevo León	76,650,000	5,119,504	14.97
7	Zacatecas	23,270,000	1,579,209	14.73
8	Yucatán	30,700,000	2,097,175	14.63
9	Chihuahua	48,520,000	3,556,574	13.64
10	Baja California Sur	7,900,000	712,029	11.09
11	Durango	19,170,000	1,754,754	10.92
12	Sonora	30,480,000	2,850,330	10.69
13	Colima	7,500,000	711,235	10.54
14	Tlaxcala	13,240,000	1,272,847	10.40
15	San Luis Potosí	27,300,000	2,717,820	10.04
16	Estado de México	159,650,000	16,187,608	9.86
17	Morelos	18,700,000	1,903,811	9.82
18	Querétaro	19,040,000	2,038,372	9.34
19	Sinaloa	25,230,000	2,966,321	8.50
20	Tabasco	20,000,000	2,395,272	8.34

21	Nayarit	9,790,000	1,181,050	8.28
22	Guanajuato	47,770,000	5,853,677	8.16
23	Jalisco	56,000,000	7,844,830	7.13
24	Oaxaca	28,210,000	3,967,889	7.10
25	Hidalgo	18,980,000	2,858,359	6.64
26	Michoacán	30,100,000	4,584,471	6.56
27	Veracruz	46,180,000	8,112,505	5.69
28	Baja California	15,430,000	3,315,766	4.65
29	Tamaulipas	15,860,000	3,441,698	4.60
30	Guerrero	14,820,000	3,533,251	4.19
31	Puebla	16,650,000	6,168,883	2.69
32	Chiapas	9,520,000	5,217,908	1.82

Fuente: elaboración propia con base a información publicada por el SNT[1] y la Encuesta Intercensal 2015 del INEGI.

[1] SNT, Sistema Nacional de Transparencia

De lo que se aduce que se atenta en contra de la autonomía presupuestaria del Instituto, ya que al "limitar el recurso que se asigna anualmente", no resulta suficiente para atender las necesidades de los habitantes de la entidad; toda vez que existen Estados que asignan mayor cantidad de recursos por habitante como lo es el caso de Quintana Roo, no obstante de que el Estado de Jalisco ha sido referente a nivel nacional en materia de acceso a la información pública, como lo es el caso que en el año 2018, Jalisco ocupó el tercer lugar a nivel nacional en cuanto a solicitudes de acceso a la información tramitadas vía Infomex y Plataforma Nacional de Transparencia, sólo por debajo de la Federación y la Ciudad de México, tal y como se muestra a continuación:



Fuente: elaboración propia en base a Informe Anual de Actividades del ITEI 2018, p. 9 disponible en: http://www.itei.org.mx/v3/documentos/art8-6l/XIII_informe_2018_ITEI.doc

Otro de los elementos que atentan en contra de la autonomía presupuestaria, consiste en que una vez que el Congreso del Estado asigna el presupuesto anual a todas y cada una de las dependencias, entidades y/o para el caso de estudio, Organismos Constitucionales Autónomos, vía el presupuesto de egresos, según lo establece el artículo 45 de la Ley de Presupuesto, Contabilidad y Gasto Público del Estado de Jalisco, la Secretaría de la Hacienda Pública del Gobierno

del Estado de Jalisco, ministra mensualmente dichos recursos, esto es, realiza una calendarización para entregar de forma mensual los recursos al Instituto, lo que implica un trámite burocrático para "solicitar" mensualmente un recurso que ya había sido otorgado por el Congreso.

Un tema por demás interesante, es el de los "intereses o rendimientos" generados por la administración del recurso de forma anual, lo cual también atenta en contra de la autonomía presupuestaria del Instituto, ya que los mismos no son entregados al "Organismo Constitucional Autónomo", ya que como se describió en líneas anteriores, dichos recursos son administrados por la Secretaría de la Hacienda Pública del Gobierno del Estado de Jalisco, lo que pudiera representar un ingreso adicional que pudiera servir para ofrecer mejores servicios a la ciudadanía; el autor del presente artículo, realizó una estimación del monto al que ascenderían los intereses o rendimientos de los recursos en el año 2019, si los mismos fueran administrados por el Instituto, utilizando el Sistema de Información Económica del Banco de México, mediante la tasa de interés interbancaria de equilibrio por sus siglas (TIIE), en inversiones gubernamentales, mismas que equivalen hasta al 8.2% anual, lo que se traduce en obtener un ingreso adicional por la cantidad de $4,614,462 (cuatro millones seiscientos catorce mil cuatrocientos sesenta y dos pesos 00/100 M.N.), tal y como se advierte a continuación:

Año (Rendimiento)	Presupuesto asignado por el Congreso al ITEI	Tasa de interés interbancario de equilibrio (Gubernamental	Cantidad anual
2019	$56,273,929.00	8.2%	$4,614,462

Fuente: elaboración propia en base al Sistema de Información Financiera del Banco de México y Presupuesto de Egresos del ITEI 2019.

Asimismo, otro de los elementos que sirven de sustento para la presente investigación, consiste en que anualmente la Secretaría de la Hacienda Pública del Gobierno del Estado de Jalisco, retiene al Instituto,

una cantidad del presupuesto asignado por el Congreso, por concepto de “Responsabilidad patrimonial”, que en el año 2019 ascendió a la cantidad de: $1,060,900.00 (un millón sesenta mil novecientos pesos 00/100 M.N), según el presupuesto de egresos para el ejercicio fiscal 2019, publicado en el periódico oficial El Estado de Jalisco, el día 25 de diciembre del año 2018, número 33, sección V, volumen II; mismo que según el Clasificador por objeto y tipo de gasto para la administración pública del Estado de Jalisco 2019, consiste en lo siguiente:

3943 Responsabilidad Patrimonial

Asignaciones destinadas al cumplimiento de la Ley de Responsabilidad Patrimonial del Estado de Jalisco, para indemnizar a quienes sin obligación jurídica de soportarlo, sufran daños en cualquiera de sus bienes o derechos como consecuencia de la actividad administrativa irregular de los Poderes del Estado, sus Entidades y Dependencias, organismos públicos, fideicomisos públicos estatales y de las empresas de participación mayoritaria estatal.

De lo anterior, se advierte que si bien es cierto existe una normatividad que obliga a las Instituciones del Estado, incluyendo a los Organismos Constitucionales Autónomos, a la contratación de un seguro para atender posibles contingencias, pero si existiera una autonomía presupuestal como constitucionalmente se describe, el ITEI tendría la libertad de contratar el seguro con la Institución financiera que deseara y no que de forma “arbitraria” le fuera retenida dicha cantidad, que es importante señalar no es devuelta al Instituto al finalizar el ejercicio fiscal; no obstante de que no se haya hecho efectivo el seguro contratado.

Lo anterior, puede ser evidenciado, en la conclusión de la auditoría del ejercicio fiscal 2016, realizada por la Auditoría Superior del Estado de Jalisco, al Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, observación número 28, a fojas 309 a 325, la cual consistía en lo siguiente:

Observación 28.

Monto observado: $1,030,00.00

Por la partida presupuestal ejercida denominada “3943 Responsabilidad Patrimonial”, la cual muestra un saldo ejercido al cierre por la cantidad de $1,030,00.00 (un millón treinta mil pesos 00/100 m.n.) de dicha partida se requiere: la documentación que compruebe y justifique, como son los estados de cuenta, copias de las pólizas, facturas, órdenes de compra, cotizaciones, contratos, pólizas de seguros, etc., así como la copia del acta de Consejo donde demuestre la autorización y destino de dicho recurso.(sic)

Observación que fue solventada por el Instituto con la evidencia documental aportada, pero se emitió una recomendación donde se acredita que dicha cantidad nunca fue recibida por el ITEI y recomiendan a los funcionarios públicos responsables, de asegurarse que la información y documentación que entregan en la cuenta pública sea correcta y en su caso, se realicen las aclaraciones pertinentes sobre el contenido de dicha cuenta pública.

Lo anterior, forma parte de la información fundamental que publica el Instituto en su portal de Internet y puede ser consultado en la siguiente liga:

https://www.itei.org.mx/v3/documentos/art8-5i/decretos_aprobacion/conclusion_auditoria_ejercicio_2016.pdf

Por todo lo anterior, al análisis de las evidencias documentadas en el presente artículo se arriba a las siguientes conclusiones.

Conclusiones

El Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, fue creado para desempeñar una función de Estado, esto es, garantizar el acceso a la información pública y la protección de datos personales, sus funciones y atribuciones se encuentran previstas en la Constitución Política del Estado de Jalisco y efectivamente cuenta la atribución de generar su normatividad interna. Por lo que, a concepto del autor, se cumple "parcialmente" el principio de autonomía que establece la constitución local, ya que existen evidencias documentadas en el presente artículo de las que se advierte que existe una clara irrupción del Poder Ejecutivo Local y del Congreso del Estado de Jalisco, en su autonomía financiera-presupuestal, toda vez, que desde la elaboración del Anteproyecto de Presupuesto y posteriormente en la administración del recurso otorgado por el Congreso del Estado al Instituto, vía el Presupuesto de Egresos correspondiente, existen una serie de procesos que no permiten administrar y emplear sus recursos económicos asignados de una forma eficiente y en beneficio de la ciudadanía.

Evidencia de lo anterior, resulta el hecho de que el Ejecutivo Estatal, al momento de diseñar el Anteproyecto de Presupuesto, históricamente determina un techo presupuestal (que generalmente) resulta ser el presupuesto que ejercerá el Instituto en el siguiente ejercicio fiscal, inferior al presupuesto solicitado y necesario para hacer frente a las obligaciones que establecen las normas aplicables al Instituto, lo que pone en riesgo un derecho humano de los jaliscienses como es el de acceso a la información pública y la protección de sus datos personales.

En ese orden de ideas, el recurso asignado al Órgano Garante per cápita, esto es, una vez que se analizó el recurso asignado por el Congreso del Estado para el ejercicio fiscal 2019, en comparación con el número de habitantes en el Estado de Jalisco, resulta ser claramente "insuficiente", ya que lo ubica en la posición número 23 a nivel nacional, con una asignación de tan solo $7.13 (siete pesos 13/100 M.N.) por habitante, en comparación con los demás órganos garantes del país, donde el Estado que más presupuesto asigna per cápita resulta ser Quintana Roo con $29.99 (veintinueve pesos 99/100 M.N.) no obstante, los buenos resultados en materia de acceso a la información pública del ITEI, por lo que se debe "reconsiderar" la cantidad asignada por el Congreso del Estado de Jalisco, para que los ciudadanos de la entidad, tengan un órgano garante que continúe siendo un referente a nivel nacional en materia de acceso a la información pública y protección de datos personales.

Se debe permitir por parte del Ejecutivo del Estado de Jalisco, "una administración y empleo total (en una sola exhibición)" de los recursos públicos asignados por el Congreso, para que el ITEI realice lo siguiente:

a) Disponga del recurso y no sea necesario solicitar mensualmente una cantidad para hacer frente a las necesidades Institucionales, lo que se traduce en la reducción de trabajo burocrático para la entrega de un recurso que ya había sido otorgado;

b) Una vez hecho lo anterior, el Instituto estaría en condiciones de obtener "intereses o rendimientos adicionales" por la administración del recurso, hasta por la cantidad de $4,614,462 (cuatro millones seiscientos catorce mil cuatrocientos sesenta y dos pesos 00/100 M.N.), según cifras del Banco de México mediante la tasa de interés interbancaria de equilibrio por sus siglas (TIIE), en inversiones gubernamentales, mismas que equivalen hasta el 8.2% anual; y

c) Contratar con la Institución financiera que mejor servicio ofrezca (buscando un menor costo) en relación a los $1,060,900.00 (un millón sesenta mil novecientos pesos 00/100 M.N), que son retenidos de forma anual para adquirir un seguro por "Responsabilidad patrimonial", y de esta forma cumplir con las normas en la materia.

Con lo anterior, el Instituto ejercería una "plena" autonomía financiera, tal y como lo previó el Congreso del Estado de Jalisco, en el artículo 9, fracción VI, segundo párrafo que señala lo siguiente:

> *Art. 9º. El derecho a la información pública tendrá los siguientes fundamentos:*
>
> *VI. La promoción de la cultura de transparencia, la garantía del derecho a la información y la resolución de las controversias que se susciten por el ejercicio de este derecho a través del Instituto de Transparencia e Información Pública de Jalisco.*
>
> *El Instituto es un órgano público autónomo, con personalidad jurídica y patrimonio propio.*

El objetivo del presente artículo es contribuir a la ampliación de conocimientos, además de permitir la generación de propuestas que modifiquen el estado actual de las cosas, en beneficio de la Autonomía presupuestaria del ITEI, y claro está de los ciudadanos del Estado de Jalisco, que serán los que finalmente reciban un servicio más eficiente, por lo que se realizan las siguientes

Propuestas

Primera. Realizar las gestiones necesarias por conducto del Pleno del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, con el aval del Consejo Consultivo de dicho Instituto, para solicitar al Titular del Ejecutivo del Estado, que en el *proceso de elaboración del Anteproyecto de Presupuesto, se considere la cantidad solicitada por el Instituto*, toda vez que en caso de no aprobar lo requerido, se *pone en riesgo un derecho humano establecido constitucionalmente* como lo es derecho de "Acceso a la Información Pública y la Protección de Datos Personales en el Estado de Jalisco".

Segunda. Se realicen las gestiones necesarias por conducto del Pleno del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, con el aval del Consejo Consultivo de dicho Instituto, para solicitar al Ejecutivo del Estado, la entrega en una sola exhibición del total del presupuesto asignado por el Congreso del Estado de Jalisco, para que así se realice una eficiente administración de los recursos públicos, en beneficio de la ciudadanía.

Tercera. Se realicen las gestiones necesarias por conducto del Pleno del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, con el aval del Consejo Consultivo de dicho Instituto, para solicitar al Congreso del Estado de Jalisco, un presupuesto *irreductible*, como el caso del Poder Judicial estatal, y *mayor*; para que de esta forma, no se violente el principio de Autonomía Presupuestaria del Instituto, y la asignación de recursos, no quede al arbitrio de ningún factor político, social, etc.

Cuarta. Se elabore un estudio por parte de la Dirección General de Innovación y Mejora Gubernamental del Gobierno del Estado de Jalisco, que tenga por objeto analizar las atribuciones, requerimientos y recursos (humanos, materiales, financieros, tecnológicos, etc.) con los que cuenta el Instituto, así como la eficiencia del Órgano Garante en los temas de su competencia, realizando un *benchmarking* a nivel

nacional que arroje como resultado, una *estimación de cuanto porcentaje del total del presupuesto de egresos se debe destinar al Instituto de forma anual*, para que haga frente a sus obligaciones para con la sociedad y sea entregado al Congreso del Estado de Jalisco a su consideración y en la medida de lo posible se establezca a nivel constitucional un porcentaje anual que se deberá otorgar al Instituto del total de presupuesto de egresos.

Geronimo Anguiano Ruiz

Especialista en Gestión, Publicación y Protección de Información por CESIP, maestría en Política y Gestión Pública por el ITESO. Se desempeña como Coordinador de Planeación del ITEI, líneas de trabajo: planeación, programación, evaluación de políticas y programas públicos, presupuesto basado en resultados, transparencia, acceso a la información y protección de datos.

Formación:

- Especialista en Gestión, Publicación y Protección de Información, CESIP.
- Maestría en Política y Gestión Pública, ITESO.
- Abogado por la U. de G.

Referencias y/o fuentes de consulta

PND 2007-2012, Plan Nacional de Desarrollo 2007-2012, Poder Ejecutivo Federal, pág. 92, disponible en: http://www.paot.org.mx/centro/programas/federal/07/pnd07-12.pdf, recuperado el 23 de septiembre de 2019.

PND 2019-2024, Plan Nacional de Desarrollo 2019-2024, pág. 6, disponible en: http://gaceta.diputados.gob.mx/PDF/64/2019/abr/20190430-XVIII-1.pdf, recuperado el 23 de septiembre de 2019.

PEGD 2018-2024, Plan Estatal de Gobernanza y Desarrollo de Jalisco 2018-2024. Visión 2030, pág. 23, disponible en: https://plan.jalisco.gob.mx/sites/default/files/2019-09/PEGyD.pdf, recuperado el 23 de septiembre de 2019.

Ugalde, F. (2009). Filiberto Valentín Ugalde Calderón, Órganos constitucionales autónomos. Revista del Instituto de la Judicatura Federal, número 29, pág. 253 a 257, disponible en: https://www.ijf.cjf.gob.mx/publicaciones/revista/29/Filiberto%20Valent%C3%ADn%20Ugalde%20Calder%C3%B3n.pdf, recuperado el 24 de septiembre de 2019.

RAE (23 A ed), Real Academia Española: Diccionario de la lengua Española, 23. A ed.- [versión 23.2 en línea], disponible en: https://dle.rae.es, recuperado el 24 de septiembre de 2019.

SHP (2019), Manual de Programación y Presupuesto 2020, pág. 5-6. Secretaría de la Hacienda Pública del Gobierno del estado de Jalisco, Dirección General de Programación, Presupuesto y Evaluación del Gasto Público, disponible en: https://presupuestociudadano.jalisco.gob.mx/material/apoyo, recuperado el 23 de septiembre de 2019.

Pedroza (2002), Susana Thalía Pedroza de la Llave, Los Órganos Constitucionales Autónomos en México, Capítulo V, Libro: Estado de Derecho y Transición Jurídica", 2002, p. 175, editores Serna, José y Caballero.

Robinson y Duncan (2009), Marc Robinson y Duncan Last. Un modelo básico de presupuestación por resultados. Fondo Monetario Internacional. Notas técnicas y manuales sobre gestión financiera pública. Pág. 1, 2009, disponible en: https://blog-pfm.imf.org/files/fad-technical-manual-4_spanish-translation.pdf, recuperado 23 de septiembre de 2019.

Robbins, S., & Coulter, M. (2010). Administración (Décima Edición ed.). México: Pearson Educación. Pág. 182.

García (1993) García Máynez, Eduardo. Introducción al estudio del Derecho, 45 a edición, Porrua, México. p.104.

García (1977) García Laguardia, José Mario, La autonomía universitaria en América Latina, mito y realidad, México, UNAM, 1977, p. 35.

SISTEMA NACIONAL DE TRANSPARENCIA
ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

La Coordinación de Organismos Garantes de las Entidades Federativas es el representante electo de los Organismos Garantes que los representa a nivel nacional.

El Sistema Nacional de Transparencia cuenta con 11 comisiones, conformadas por integrantes del mismo para coordinar, analizar y dictaminar asuntos y temas de interés en las materias de Transparencia, Acceso a la Información y Protección de Datos Personales:

- Comisión Jurídica, de Criterios y Resoluciones
- Comisión de Protección de Datos Personales
- Comisión de Capacitación, Educación y Cultura
- Comisión de Vinculación, Promoción, Difusión y Comunicación Social
- Comisión de Tecnologías de la Información y Plataforma Nacional de Transparencia
- Comisión de Archivos y Gestión Documental
- Comisión de Gobierno Abierto y de Transparencia Proactiva
- Comisión de Asuntos de Entidades Federativas y Municipios
- Comisión de Indicadores, Evaluación e Investigación;
- Comisión de Derechos Humanos, Equidad de Género e Inclusión Social
- Comisión de Rendición de Cuentas

conoce más en

www.snt.org.mx

Fotografía: Ro Ma para Pixabay

Documentos de archivo y procedimientos judiciales y administrativos

Karen Michelle Martínez Ramírez
Secretario de Acuerdos de Ponencia en el ITEI

Resumen

En este artículo se analizan los alcances que tienen la Ley General de Archivos (LGA) y los Lineamientos para la Organización y Conservación de Archivos (LOCA), emitidos por el Sistema Nacional de Transparencia, respecto al resguardo (o custodia) de los documentos de archivo que generan, reciben y administran las entidades públicas.

Lo anterior, con el objetivo de valorar la armonización de dichos instrumentos jurídicos con la facultad potestativa que tienen las entidades públicas a fin de remitir a las autoridades administrativas y jurisdiccionales, aquellos documentos originales que consideran pertinentes para la tramitación de los procedimientos en los que fungen como parte.

Ello, debido a la heterogeneidad que existe respecto a las providencias que se han tomado sobre aquellos documentos originales que se remiten a otras autoridades para los fines en mención; los efectos que producen las declaraciones de inexistencia previstas en las leyes generales y locales que en materia de acceso a la información pública y protección de datos personales se encuentran vigentes en México; y la importancia que tienen los documentos para la impartición de justicia y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO), así como para el ejercicio del derecho de acceso a la información pública (DAI).

Concluyendo así que en materia de archivos resulta pertinente contar con un marco normativo que contemple la facultad potestativa en mención, esto, con la finalidad de estandarizar procedimientos que garanticen el debido resguardo de documentos para así estar en posibilidades de garantizar a las personas, los multicitados derechos humanos universales, sin generar afectaciones en el trámite de los procedimientos judiciales y administrativos en los que las entidades públicas funjan como parte.

PALABRAS CLAVES:
Derecho de Acceso a la Información Pública, Derechos ARCO, Declaraciones de Inexistencia, Documentos de Archivo, Medios de Prueba, Procedimientos

Introducción

En los últimos tres sexenios y el inicio de esta cuarta transformación, se ha visto como es que la transparencia, el acceso a la información pública, los datos personales, e incluso la rendición de cuentas y la lucha contra la corrupción han ido tomando un lugar importante en la agenda pública del país; cada tema en un momento diferente que ha atendido a los acontecimientos que se han suscitado durante el desarrollo del país y que invariablemente se han señalado bajo un contexto de garantía a los derechos humanos, la consolidación democrática y credibilidad institucional.

En este sentido, es que vale la pena señalar que en los tres sexenios anteriores se aprobaron diversas reformas constitucionales que nos han colocado en la realidad normativa que en el país se encuentra vigente en materia de acceso a la información pública, archivos y datos personales; siendo el caso que la reforma más relevante, resulta ser la publicada el día 7 de febrero de 2014, en el Diario Oficial de la Federación (DOF), toda vez que con dicha reforma se estableció la obligación de documentar todo acto de autoridad y a su vez, se dotó de atribuciones al Congreso de la Unión para emitir las leyes generales que en materia de archivos, acceso a la información pública y protección de datos personales se encuentran vigentes en el país. (Cámara de Diputados, 2014).

Así pues, es que bajo esa tónica, vale la pena señalar que dicha reforma se propuso argumentando la necesidad de homologar términos, procedimientos y sanciones, así como de estandarizar la información pública fundamental y a su vez, establecer bases y principios en las materias de referencia. Debiendo precisar a este respecto, que los archivos se colocaron como los cimientos para el ejercicio del DAI y los derechos ARCO (Senado, 2012), pues a decir, se expuso la necesidad de contar con criterios de custodia de archivo que cancelen la posibilidad para que los servidores y funcionarios públicos hagan uso discrecional de los mismos y así entreguen, al final de su encargo, la totalidad de la documentación que generaron[1]. (Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos; de Gobernación y Anticorrupción et al., 2012).

Bajo esa perspectiva, es que el Congreso de la Unión aprobó de manera progresiva, las leyes generales que le fueron encomendadas, esto es, la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[2] y la LGA (Congreso de la Unión, 2017 y 2018), dando así inicio a los procesos de armonización legislativa en las entidades federativas del país.

Establecido lo anterior, y habida cuenta de la reciente entrada en vigor de la LGA, la aplicabilidad de los LOCA y término que corre a las legislaturas locales para efectuar la armonización correspondiente, vale la pena cuestionarnos si la LGA y los LOCA garantizan normativamente que los servidores y funcionarios públicos entregaran, al terminar su encargo, la totalidad de los documentos que recibieron y generaron, tal y como se planteó en la iniciativa de reforma que formularon las Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos; de Gobernación y Anticorrupción y Participación Ciudadana en Materia de Transparencia, en 2012.

Ello debido a que los documentos son necesarios para el ejercicio de los derechos ARCO y del DAI, siendo importante recordar que es a través del ejercicio de éstos derechos que podemos obtener documentos para ejercer otros más, entre ellos, el derecho de acceso a la justicia, pues los documentos son fiel testimonio de las decisiones y actuaciones de las entidades públicas (UNESCO, 2012) por lo que en ese sentido es que éstos revelan por un lado, como es que las autoridades cumplen o incumplen con sus funciones, atribuciones y obligaciones; y por otro

[1] Dicha obligación se encuentra prevista en el artículo 12.3 de la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía, España.

[2] Las disposiciones vigentes en la LGTAIP se armonizaron con la LTAIPEJM, mientras que lo previsto en la LGPDPPSO se tomó como base mínima para que Jalisco aprobará su ley local, lo último conforme a lo previsto por el artículo séptimo transitorio de la LGPDPPSO; de tal suerte que las disposiciones que se refieren en el presente artículo respecto a la normatividad local, no contravienen lo dispuesto en las Leyes Generales de referencia.

lado, los derechos y obligaciones de las personas. (INFOEM, 2017)

Evidenciando así que los archivos son la materia prima para el ejercicio de los derechos humanos fundamentales en mención (Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos; de Gobernación y Anticorrupción et al., 2012) y a su vez, para acreditar los hechos que se señalen ante alguna autoridad judicial o administrativa dentro de algún procedimiento. (Congreso de la Unión, 2012); por lo que en ese sentido es que resulta importante destacar lo siguiente:

Que a las entidades públicas les asiste la facultad potestativa de remitir a las autoridades jurisdiccionales y administrativas, los documentos originales que obran en su poder para ser ofertados como medios de prueba dentro de aquellos procedimientos en los que fungen como parte;

Que es la autoridad judicial y administrativa quien determina el valor probatorio de los documentos que se ofertan dentro de los procedimientos que sustancian dentro de su competencia, esto, en función de la legislación adjetiva que al respecto resulte ser aplicable; y

Que los documentos que obran en resguardo de las entidades públicas pueden obtenerse por los particulares para los fines que estimen pertinentes, esto, mediante el ejercicio de los derechos ARCO y del DAI.

Bajo esa lógica de ideas, es que ahora vale la pena formular las siguientes preguntas: ¿Las autoridades remiten documentos originales a las autoridades administrativas y jurisdiccionales para los fines señalados? y de ser así, ¿Conservan copia certificada de los mismos para garantizar el DAI y los derechos ARCO de aquellas personas que los soliciten, o declaran su inexistencia conforme a lo previsto por las LGTAIP y la LGPDPPSO, según el caso?

Dichas interrogantes resultan ser de suma importancia pues las tres leyes generales en mención se emitieron a fin de contar con un marco legal homologado que permitiera tutelar sin distinción alguna, los derechos aquí mencionados, creando “derecho igual para todos y un deber igual para cualquier instancia” (Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos; de Gobernación y Anticorrupción et al., 2012); situación que normativamente aún no se puede asegurar pues del análisis literal y sistemático de la misma se advierte que la lógica de administración de documentos consiste en que éstos pasen únicamente de un archivo a otro, ello, sin contemplar en su texto o el de los LOCA, que los documentos salgan del dominio de los sujetos obligados, o en su defecto, alguna prohibición o condición expresa al respecto. Dejando así obsoleto uno de los argumentos con los que se impulsó la iniciativa de fecha 19 de diciembre de 2012, citada en párrafos anteriores:

> *“Mediante la integración de una Ley General de Archivos, se facilitará el uso de la información, y se contribuirá al ejercicio eficaz del derecho de acceso a la información, desembocando en una mejor rendición de cuentas” (Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos; de Gobernación y Anticorrupción et al., 2012)*

Metodología

La investigación para este artículo se realizó bajo el siguiente diseño:

En cuanto al enfoque: multimodal (o de triangulación) con análisis lógico racional, ya que se recolectaron y analizaron datos para contestar las preguntas planteadas con antelación, para así estar en condiciones de construir una realidad operativa respecto la administración de documentos en las entidades públicas que integran el universo de estudio, la cual se contrastó con las disposiciones normativas vertidas en la LGA y los LOCA.

En cuanto al tiempo de ocurrencia y secuencia: retrospectivo y longitudinal.

Retrospectivo ya que por un lado se analizó la importancia que han tenido los documentos públicos en casos jurisdiccionales resueltos por la Corte Interamericana de los Derechos Humanos (CIDH) en los años 2010 y 2014; por otro lado, se analizó la normativa aplicable en Colombia, España, México y la República de Chile, respecto a la administración de documentos públicos, y finalmente, se analizaron y registraron datos atinentes a la remisión de documentos que han tenido lugar en el Estado de Jalisco durante el periodo comprendido de 2013 a 2019.

Longitudinal ya que se estudiaron las variables que se han presentado en los casos acontecidos, denotando una relación de causa-efecto.

En cuanto al control sobre las variables: por instrumento jurídico en relación con la información pública proporcionada por el universo de sujetos obligados, ya que se analizan los alcances que tienen diversos ordenamientos respecto a la gestión documental;

En cuanto al análisis y alcance de los resultados: descriptivo y analítico ya que por un lado se estudió la ausencia de un efectivo resguardo de documentos, y por otro lado, se analizó la viabilidad de propuestas que atendieran el déficit normativo que aquí se plantea, esto, tomando en consideración los datos numéricos obtenidos, en relación con el ejercicio de los derechos ARCO y del DAI; y

En cuanto al método de recolección de información, se llevó a cabo el análisis documental y la observación de campo no experimental.

Respecto al análisis documental, se atendió lo vertido en resoluciones emitidas por organismos internacionales en materia de derechos humanos y diversa legislación en materia procesal, de archivos, acceso a la información pública y ejercicio de derechos arco, así como de publicaciones electrónicas y artículos.

Respecto a la observación de campo no experimental, se analizó información pública que permitió detectar la existencia de un patrón en cuanto a las providencias que se toman antes de que los documentos originales se remitan a las autoridades administrativas y jurisdiccionales en mención.

El universo de estudio se constituye por sujetos obligados del gobierno federal con competencia en rubros como salud, educación, e investigación de delitos, por señalar algunos ejemplos.

Desarrollo

I. Archivos, expedientes, documentos de archivo y gestión documental

A fin de tener un mejor entendimiento respecto a un tema de cualquier rama del conocimiento, es importante siempre tener claros los conceptos que rodean al mismo.

En ese sentido, es que se inicia señalando algunas definiciones que se han establecido respecto a los archivos, expedientes y documentos de archivo, ya que estos conceptos son fundamentales en el presente artículo.

Así pues, es menester señalar que en los años ochenta los archivos se definían como aquella parte de la estructura orgánica que tenía la autoridad a fin de resguardar sus documentos (Universidad Autónoma de México, 1982 e Instituto Nacional de la Administración Pública, 1985) para posteriormente contemplarse en la Ley Federal de Archivos (LFA) como todos aquellos documentos que se recibían o generaban por las autoridades o particulares en razón de sus funciones, atribuciones o actividades (Congreso de la Unión, 2012), para finalmente, definirse en la LGA de la siguiente manera:

> *"(…) conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden" (Cámara de Diputados, 2018).*

Con lo anterior, se observa como es que ha evolucionado el concepto de archivo y principalmente que con pocas palabras, se generan cambios sustanciales, ya que al contrastar las definiciones previstas en la LFA y la LGA, se logra advertir la sustancialidad del cambio que se ha generado, ya que mientras la LFA contempla como archivo a todo documento recibido o generado, la LGA modifica dicha concepción al agregar "conjunto organizado de documentos", lo cual implica que dicha concepción se ciñe ahora a los expedientes no así a los documentos en particular.

Dicha aseveración se sostiene ya que la LGA define expediente como "la unidad documental compuesta por documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite" (Cámara de Diputados, 2018), por lo que en ese sentido, resulta pertinente señalar a su vez que los documentos de archivo son aquellos en los que básicamente, se hacen constar los hechos y actos que realizan los sujetos obligados (Congreso de la Unión, 2018).

Figura 1. Representación gráfica de conceptos básicos contenidos en la LGA.

Siendo que, a la serie de acciones que las entidades públicas realizan con los documentos de archivo, expedientes y archivos, se le llama gestión documental, pues LGA define tal término como el "tratamiento integral de la documentación a lo largo de su ciclo vital, a través de la ejecución de procesos de producción, organización, acceso, consulta, valoración documental y conservación" (Congreso de la Unión, 2018).

Ahora bien, planteado lo anterior, resulta oportuno señalar que la importancia de los documentos en general se elevó con la reforma constitucional que se efectúo en febrero de 2014 respecto al artículo 6° de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), pues con ello se estableció la obligación de documentar todo acto de autoridad, lo que propició que en la LGTAIP y la LGPDPPSO se contemplaran disposiciones específicas respecto a la inexistencia de información.

Siendo el caso que aunado a lo anterior, a los documentos se les han atribuido funciones administrativas, históricas y sociales, ya que por un lado coadyuvan en la toma de decisiones y fungen como testigos respecto al cumplimiento de las atribuciones, funciones y obligaciones de las entidades públicas; y por otro lado permiten "descubrir la verdad y contrastar diferentes versiones sobre los acontecimientos"; y finalmente, permiten acreditar los derechos y obligaciones de las personas[3] (INFOEM, 2017).

Por lo que en ese sentido es que resulta ser prioritario, garantizar el debido resguardo de los documentos que administran, generan y reciben las entidades públicas, o dicho de otro modo, garantizar el debido resguardo de cada documento de archivo que integra cada expediente.

Ello, debido a que son precisamente los documentos de archivo los que fungen como materia prima para el ejercicio del DAI y de los derechos ARCO (Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos; de Gobernación y Anticorrupción et al., 2012).

II. Los documentos de archivo como medios de prueba y su conservación conforme a la LGA y los LOCA

Habida cuenta de las funciones que tienen los documentos es que resulta importante señalar que en los procedimientos, éstos juegan un papel fundamental ya que pueden cumplir, incluso de manera simultánea, con las tres funciones que se les han atribuido, esto, en razón del uso que se dé a los mismos, ya que por ejemplo, a través de un mismo documento de archivo se puede constatar si una entidad pública ejerció ciertas atribuciones, así como la existencia de derechos y obligaciones de quien los firma para con ello verificar lo que aconteció en una fecha o periodo determinado, cumpliendo así su función administrativa, social e histórica, respectivamente.

Establecido lo anterior, es que vale la pena señalar que los documentos de archivo se ofertan como medios de prueba en procedimientos locales, federales e internacionales a fin de acreditar los hechos que en ellos se narran y en consecuencia obtener las pretensiones deseadas. Siendo el caso que al respecto, dichos documentos de archivo han fungido como agentes determinantes en la impartición de justicia.

Bajo esa perspectiva es que vale la pena recordar que el artículo 298 fracción II del Código de Procedimientos Civiles del Estado de Jalisco (CPCEJ) reconoce medios de prueba a los documentos públicos, señalando además, en su numeral 329 aquellos documentos que cuentan con dicha naturaleza; entre los cuales destacan aquellos que son emitidos y autorizados por servidores públicos, en el ejercicio de sus funciones o con motivo de ellas (CPCEJ, 2018).

Debiendo precisar a ese respecto que dichos documentos pueden ser ofertados tanto por particulares como por entidades públicas, ya que como bien sabemos, éstas últimas son susceptibles de formar parte de procedimientos judiciales y administrativos.

No obstante a lo anterior, en la LGA y los LOCA se omitió contemplar la facultad potestativa que tienen las entidades públicas para ofertar tales documentos, pues no se señalan disposiciones que regulen la remisión de documentos públicos originales a otras autoridades para los fines señalados, con lo que se deja a las entidades públicas decidir arbitrariamente respecto a las medidas que se tomarán sobre los documentos que salgan de su dominio para ser exhibidos como medios de prueba, lo que genera heterogeneidad en los procedimientos para el reguardo de documentos de archivo.

Ello, debido a que de un análisis literal y sistemático de la LGA, se advierte que se contempla la remisión de documentos de archivo de una unidad administrativa a otra, es decir, de un tipo de archivo a otro, excluyendo en ese sentido la remisión éstos a otras entidades públicas y garantizando en términos legales su localización y disponibilidad conforme a la vigencia documental establecida. Obviando que

[3] Dichas funciones se han atribuido de manera expresa a los documentos, en Colombia, esto, en el artículo 4 de la Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

a consecuencia de dicha gestión documental, se garantizará a su vez, el efectivo ejercicio del DAI y de los derechos ARCO.

Partiendo de lo anterior, es que en dicha LGA se aprobaron las siguientes obligaciones respecto a la conservación de documentos:

1. La obligación de conservar los documentos de archivo que versen respecto al ejercicio de las facultades, competencias o funciones de las entidades catalogadas como sujetos obligados;

2. La obligación de “mantener los documentos contenidos en sus archivos en el orden original”, de modo que los documentos de archivo originales no se deben sustituir por certificaciones, copias simples o soportes documentales como discos compactos o dispositivos universal serial bus (USB) que contengan la digitalización de los mismos;

3. La obligación de dar acceso a los documentos de archivo conforme a lo previsto en la LGTAIP y la LGPDPPSO;

4. La obligación de “conservar de manera homogénea los documentos de archivo que produzcan, reciban, obtengan, adquieran, transformen o posean”, lo que implica que de manera indistinta se deben implementar las mismas medidas en todos los expedientes, para la conservación de los documentos de archivo que en ellos se encuentran; y

5. La obligación que tienen los servidores públicos de entregar los documentos que tienen bajo su resguardo, esto, al concluir su encargo; lo que hace presumir que la totalidad de los documentos que recibió, generó y administró una unidad administrativa, se encontrarán durante su plazo de conservación o de manera permanente, en resguardo de la entidad pública a la que pertenecen las unidades administrativas que recibieron, generaron y administraron dichos documentos, ya sea en su archivo de trámite, de concentración o histórico.

Debiendo precisar respecto al punto número cinco que, en caso de optar por la eliminación de documentos, se presupone también la obligación de aprobar actas y dictámenes de baja documental, así como de emitir un inventario de baja documental, esto, de conformidad a lo establecido en los artículos 13 fracción III, en relación con el similar 4 fracciones XII y XXXIX, y 31 fracción IX, todos de la LGA.

Lo cual, es importante referir, permite brindar plena certeza jurídica a las personas respecto a las declaraciones de inexistencia que, en términos de lo dispuesto por el artículo 87, fracción III de la LPDPPSOEJM, confirma el Comité de Transparencia; así como respecto al procedimiento de declaración de inexistencia previsto por el artículo 86 bis de la LTAIPEJM; ya que en dicha acta, dictamen e inventario de baja documental se constataría fehacientemente la inexistencia de los documentos que ahí se refieren y son solicitados mediante el ejercicio del DAI y los derechos ARCO.

Así pues, es que de manera general, la secuencia de ideas prevista en la LGA respecto a la gestión documental, resulta ser la siguiente:

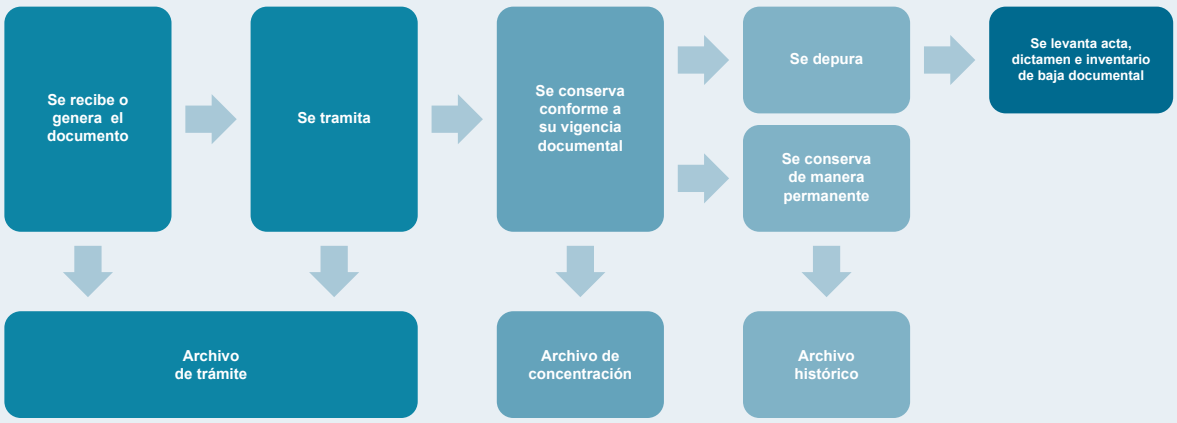


Figura 2. Flujo general de gestión documental, conforme a lo previsto en la LGA.

Ahora bien, planteado lo anterior, y a fin de agotar las opciones legales vigentes a nivel nacional, es que al remitirnos a los LOCA, se constata que en ellos también se excluye la remisión de documentos que se

refiere, ya que si bien, en sus artículos décimo primero, fracción II inciso b) y décimo noveno, se establece la obligación que tienen los responsables del archivo de trámite respecto al resguardo de expedientes y el deber que tienen los sujetos obligados a fin de garantizar la integridad y debida conservación de los expedientes, en dichos Lineamientos se omite considerar la multicitada facultad potestativa que tienen las entidades públicas a fin de ofertar ante otras autoridades, aquellos documentos de archivo que consideren pertinentes para resolver los procedimientos en los cuales funjan como parte (LOCA, 2016).

III. Declaraciones de inexistencia y sus efectos

Respecto a este tema, es importante señalar que la CIDH, como órgano jurisdiccional encargado de resolver las controversias que se suscitan respecto a la presunta violación de los derechos conferidos en la Convención Americana de Derechos Humanos (también llamado Pacto de San José), resolvió en noviembre de 2014, que las declaraciones de inexistencia que emiten los Estados, deben garantizar que la información y documentos solicitados nunca existieron, esto, a fin de garantizar el derecho de recibir información, que se consagra en su artículo 13; señalando además que a fin de garantizar este derecho, los Estados deben conservar sus archivos a fin de garantizar el acceso a los mismos (CIDH, 2014).

Así pues, es que planteado lo anterior, se advierte la necesidad de precisar que dicha determinación resulta ser vinculante para el Estado Mexicano ya que en diciembre de 1998 se aceptó la competencia contenciosa y facultad de interpretación que le asiste a la Corte de conformidad a lo establecido en el numeral 62.3 del Pacto de San José (CIDH, 2019).

Bajo esa tónica, y habida cuenta de lo anterior, es que se cuenta con una perspectiva más clara respecto a la función de una declaración de inexistencia, no obstante a lo anterior, es menester señalar que por un lado, el artículo 53 de la LGPDPPSO y el artículo 87 de la LPDPPSOEJM, sólo refieren en relación a las declaraciones de inexistencia, que los Comités de Transparencia de los sujetos obligados tienen atribuciones para confirmar la inexistencia de datos y para dar vista al órgano de control interno respecto a las presuntas irregularidades respecto de determinado tratamiento de datos personales, especialmente en los casos relacionados con las declaraciones de inexistencia; mientras que por otro lado, el artículo 138 de la LGTAIP y el artículo 86 bis de la LTAIPEJM, señalan las reglas que se deben de observar a fin de declarar la inexistencia de información.

Debiendo precisar que si bien, el Comité de Transparencia tiene la obligación de ordenar la reposición de información (siempre que sea materialmente posible), dar cuenta al órgano de control interno para que inicie el procedimiento de responsabilidad administrativa correspondiente y señalar al servidor público responsable de contar con la información solicitada, dichas medidas no resultan ser suficientes a fin de garantizar el acceso de aquellos documentos que se exhiben como medios de prueba dentro de los procedimientos.

Tabla 1. Atribuciones del Comité de Transparencia respecto a las declaraciones de inexistencia de información, conforme a la normatividad local.

LTAIPEJM	LPDPPSOEJM
*"**Artículo 86-Bis.** Respuesta de Acceso a la Información – Procedimiento para Declarar Inexistente la Información* *(…)* ***3. Cuando la información no se encuentre en los archivos** del sujeto obligado, **el Comité de Transparencia:*** *(…)* ***III. Ordenará, siempre que sea materialmente posible, que se genere o se reponga la información en caso de que ésta tuviera que existir** en la medida que deriva del ejercicio de sus facultades, competencias o funciones, **o** que **previa acreditación de la imposibilidad de su generación, exponga de forma fundada y motivada, las razones por las cuales en el caso particular el sujeto obligado no ejerció dichas facultades, competencias o funciones**, lo cual notificará al solicitante a través de la Unidad de Transparencia; y* ***IV. Notificará al órgano interno de control** o equivalente del sujeto obligado **quien, en su caso, deberá iniciar el procedimiento de responsabilidad administrativa** que corresponda.* ***4. La resolución del Comité** de Transparencia **que confirme la inexistencia** de la información solicitada contendrá los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y **señalará al servidor público responsable de contar con la misma."*** *Énfasis añadido.*	*"**Artículo 87.** Comité de Transparencia — Atribuciones.* ***1. El Comité de Transparencia tendrá las siguientes atribuciones:*** *(…)* ***VIII. Dar vista al órgano interno de control** o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, **de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables;*** *(…)" Énfasis añadido.*

Concluyendo así que dichos instrumentos normativos no se encuentran armonizados con las leyes adjetivas, lo que deja al arbitrio de las entidades tomar alguna medida que eventualmente permita el ejercicio del DAI y los derechos ARCO, lo que se pone en riesgo el efectivo ejercicio de éstos derechos.

IV. Infracciones y sanciones en materia de archivos

Mucho se ha dicho ya respecto a la obligación que tienen las entidades públicas a fin de conservar sus archivos y los documentos que lo integran, así como brindar acceso a los mismos en términos de lo dispuesto por las leyes generales y locales que en materia de acceso a la información pública y protección de datos personales se encuentran vigentes.

Por lo anterior, es que ahora, resulta pertinente señalar cuáles son las infracciones y sanciones que se contemplan en relación al manejo de documentos, los cuales, como ya dijimos, fungen como materia prima para el ejercicio del DAI, los derechos ARCO y otros derechos fundamentales.

Así pues, es que bajo esa tónica, se señala que por un lado, el artículo 122.1 fracciones I y II de la LTAIPEJM contempla como infracciones que una persona física sustraiga, elimine o destruya información (Congreso de Jalisco, 2013); mientras que por otro lado, el similar 146.1 fracción XX de la LPDPPSOEJM contempla con la misma naturaleza, que los sujetos obligados efectúen el tratamiento de datos personales de modo que se impida el ejercicio de los derechos fundamentales previstos en la CPEUM (Congreso de la Jalisco, 2017); y finalmente, el artículo 116 de la LGA contempla como infracciones, la transferencia de la posesión de documentos de los sujetos obligados, salvo aquellas que estén previstas o autorizadas en las disposiciones aplicables, impedir la consulta de documentos de los archivos sin causa justificada, y actuar con negligencia en la ejecución de medidas técnicas, administrativas o tecnológicas, para la conservación de los archivos (Congreso de la Unión, 2018).

No obstante a lo anterior, la LTAIPEJM opta por brindar en sus artículos 124.1 y 127.1, la opción de presentar denuncias para iniciar procedimientos de responsabilidad administrativa y consultar el Código Penal a fin de consultar los delitos que se desprendan de la materia; mientras que por lo que ve a la infracción prevista en la LPDPPSOEJM, el artículo 149.1 fracción III de dicha ley establece como sanción una multa que va de quinientas a mil quinientas veces el valor diario de la Unidad de Medida y Actualización (UMA), lo que equivale a una multa de $42,245.00 a $126,735.00, ya que según datos publicados por el Instituto Nacional de Estadística y Geografía (INEGI), el valor diario vigente de la UMA es de $84.49.

Siendo el caso que finalmente, y por lo que ve a las infracciones que se refieren de la LGA, el artículo 118 de ese mismo dispositivo legal señala que dichas infracciones son graves y que serán sancionadas con multas de diez a mil quinientas veces el valor de la UMA, lo que equivale a multas que van de $844.90 a $126,735.00, atendiendo al valor vigente de dicha unidad de medida.

Lo anterior, se puede verificar mediante la consulta del contenido de los artículos en mención, el cual se encuentra en la tabla que se muestra a continuación.

Tabla 2. Infracciones y sanciones respecto al manejo de documentos.

LGA	LTAIPEJM
Infracciones	
"Artículo 116. Se consideran infracciones a la presente Ley, las siguientes: I. Transferir a título oneroso o gratuito la propiedad o posesión de archivos o documentos de los sujetos obligados, salvo aquellas transferencias que estén previstas o autorizadas en las disposiciones aplicables; II. Impedir u obstaculizar la consulta de documentos de los archivos sin causa justificada; III. Actuar con dolo o negligencia en la ejecución de medidas (…) para la conservación de los archivos; (…)"	**"Artículo 122.** Infracciones - Personas físicas y jurídicas 1. Son infracciones administrativas de las personas físicas y jurídicas que tengan en su poder o manejen información pública: I. Sustraer, ocultar o inutilizar información pública; II. Destruir o eliminar información pública, sin la autorización correspondiente; (…)"
LPDPPSOEJM	
Infracciones	**Sanciones**
"Artículo 146. Infracciones— Causales. 1. Serán causas de responsabilidad y sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes: (…) XX. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos; (…)"	**"Artículo 149.** Infracciones— Sanciones. 1. A quien cometa alguna de las infracciones establecidas en la presente Ley, se le sancionará de la siguiente forma: (…) III. Multa de quinientas a mil quinientas veces el valor diario de la Unidad de Medida y Actualización (…)"

Bajo ese esquema de ideas, es que se advierte que en mayor o menor medida, la llamada triada de la transparencia, contempla medidas tendientes a garantizar la permanencia de los documentos en resguardo de los sujetos obligados a los que pertenecen, no obstante y arriesgando a ser reiterativa, dichas disposiciones resultan ser insuficientes a fin de garantizar el efectivo ejercicio del DAI y los derechos ARCO.

Primero porque en dichos dispositivos legales no se prevé la facultad potestativa que se señala en este artículo y después porque de la literalidad del contenido de las infracciones previstas en las fracciones I, II y III del artículo 116 de la LGA, se advierte lo siguiente:

Si bien en la fracción I se prevé la transferencia de la posesión de los documentos de los sujetos obligados como una infracción, en dicha fracción se establece como salvedad que dicha transferencia no constituirá una infracción cuando su transferencia se encuentre prevista o autorizada en las disposiciones aplicables; de modo que al ser el CPCEJ el que permite exhibir documentos de archivo como medios de prueba, se entiende que la remisión de dichos documentos a las autoridades encargadas de la impartición de justicia, constituye una transferencia autorizada en términos de dicha ley adjetiva.

Ahora bien, en la fracción II de dicho numeral, se establece como fracción el impedir la consulta de documentos de archivo sin causa justificada, de modo que ante la existencia de un procedimiento en el que fue necesaria la remisión de documentos de archivo, para la defensa de los intereses de la entidad pública obligada a conservar los mismos, se presume el intento de justificar el incumplimiento de las obligaciones relativas a la conservación de documentos.

Finalmente, y por lo que toca a la fracción III, se advierte que si bien en dicha fracción se refiere como infracción el actuar con negligencia en la ejecución de medidas para la conservación de archivos, en esta fracción se omite lo relativo los documentos de archivos, de modo que se podría remitir parte de un expediente a otra autoridad sin incurrir en el supuesto previsto en esta fracción.

Con lo anterior se evidencia, en términos generales, que las infracciones previstas en la LGA respecto al manejo de documentos no se acercan al fin deseado: garantizar la conservación y disponibilidad de los documentos que generan y reciben los sujetos obligados.

IV. Gestión documental en otros países.

Ahora bien, en este rubro se analiza la normatividad que se encuentra vigente en los países de Colombia, España y República de Chile, en relación a la gestión documental, esto, a fin de tener noción de las disposiciones que al respecto operan en otros lugares del mundo.

Bajo esa tónica, y por lo que toca a Colombia, se precisa que la Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones (Congreso de Colombia, 2000) contempla, al igual que la LGA, tres tipos de archivos con las mismas características y funciones que las previstas por el legislador mexicano para el caso del archivo de trámite, de concentración e histórico. No obstante, dicha Ley se destaca debido a que reconoce el valor probatorio de los documentos, la responsabilidad que tienen los servidores públicos sobre los de la debida conservación de los mismos, la facultad que tienen las entidades del Estado para autorizar la salida de los documentos por motivos legales, así como el derecho que tienen las personas para consultar todos los documentos de archivo y a que se les expida copias de los mismos.

En lo que respecta a la República de Chile, este país no cuenta con una ley especial en materia de archivos, no obstante, se señala la Ley 20.285 Sobre Acceso a la Información Pública, en razón de que su artículo 13 señala a la letra lo siguiente:

> *"Artículo 13.- En caso que el órgano de la Administración requerido no sea competente para ocuparse de la solicitud de información o no posea los documentos solicitados, enviará de inmediato la solicitud a la autoridad que deba conocerla según el ordenamiento jurídico, en la medida que ésta sea posible de individualizar, informando de ello al peticionario. Cuando no sea posible individualizar al órgano competente o si la información solicitada pertenece a múltiples organismos, el órgano requerido comunicará dichas circunstancias al solicitante."*

De modo que al carecer de disposiciones que regulen la salida de documentos de una entidad a otra, como en el caso de México, la Ley 20.285 Sobre Acceso a la Información Pública, permite que las entidades públicas de la República de Chile remitan las solicitudes de información a la autoridad que tenga los documentos que se solicitan. Advirtiendo así que quien resultó ser el destinatario de documentos ahora es sujeto obligado en términos de acceso a la información pública, conforme al citado artículo 13 de la Ley 20.285. (Congreso Nacional de Chile, 2016)

Finalmente, y por lo que ve a España se precisa que este país cuenta con 89 instrumentos jurídicos que contienen disposiciones relativas a la administración de archivos, no obstante, el único que resulta ser aplicable en todo su territorio es su Constitución, ya que los 88 instrumentos jurídicos restantes resultan ser aplicables en regiones o comunidades de ese país.

Partiendo de lo anterior, es que se precisa también que de esta nación se analizan, además de las disposiciones previstas en su Constitución, y aquellas que se encuentran en la Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía (Boletín Oficial del Estado, 2011).

En esa perspectiva, se señala que el artículo 105 inciso b) de la Constitución Española contempla la obligación que tiene el Estado para regular, y con ello garantizar que los ciudadanos tengan acceso a los archivos y registros administrativos, estableciendo como única salvedad, que se “afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.” (Boletín Oficial del Estado, 2011), no así cuestiones relativas a la deficiencia, negligencia o dolo en la gestión documental.

En otra perspectiva, y entrando en competencia regional, la Ley 7/2011, de 2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía, establece que “Los documentos de titularidad pública solo podrán salir de sus correspondientes unidades administrativas, sistemas de

información y archivos en los casos y con los procedimientos que se establezcan reglamentariamente.”.

Así, bajo esa perspectiva, es que dicha Ley prevé que cualquier persona puede denunciar el incumplimiento de la disposición anterior, es decir, cualquier persona puede denunciar el hecho de que la entidad pública permita que sus documentos salgan de las unidades administrativas y archivos, fuera de los procedimientos reglamentariamente establecidos. Ello, con la finalidad de imponer las sanciones que se muestran en la tabla que se inserta a continuación, pues permitir tal situación constituye una infracción leve que, en caso de reincidencia, se califica como grave.

Tabla 3. Infracciones, sanciones y plazos de prescripción vigentes en Andalucía por la salida ilegal de documentos.

Tipo de infracción	Sanción		Prescripción
Leves	**Multa de hasta cincuenta mil euros.**		**6 meses**
Graves	Multa de cincuenta mil un euros a cien mil euros	Inhabilitación de uno a cinco años para el ejercicio de su profesión en el ámbito de la Administración de la Junta de Andalucía del personal directivo, técnico o profesional.	3 años

Con lo anterior, es que se advierte que se dota de poder a las personas para denunciar la salida de documentos y con ello sancionar al responsable.

V. Resoluciones de procedimientos internacionales y documentos de archivo.

En la jurisdicción internacional, la CIDH resolvió en 2014 el caso Rodríguez y otros (desaparecidos del Palacio de Justicia) vs Colombia, en el que se logró determinar la responsabilidad del Estado en cuanto a la privación ilegal de la libertad, la desaparición for-

zada y ejecución extrajudicial, de diversas personas que se encontraban en el Palacio de Justicia en noviembre de 1985.

Debiendo precisar a este respecto que dichas responsabilidades lograron determinarse debido a que la Corte valoró entre otras cosas, los videos de las cámaras que se encontraban al interior y exterior del Palacio de Justicia, los registros de ingreso y salida de dicha instalación, así como informes, actas y dictámenes que se levantaron por parte de bomberos, policías y equipo médico forense, respecto a los cadáveres que se encontraron en los diferentes pisos del Palacio mencionado.

Pues con tales soportes, se advirtió qué personas ingresaron a las instalaciones del Palacio de Justicia, qué personas salieron con vida y caminando, con vida y en camilla o con ayuda, e incluso qué personas salieron sin vida.

Delimitando además, respecto a las personas que salieron con vida y caminando, cuál fue el curso que tomaron y las personas que las rodearon; mientras que por lo que ve a las personas que salieron sin vida, se logró determinar que los reportes, actas e informes eran irregulares debido a que cadáveres con registro de sexo masculino tenían útero, con lo que se concluyó y confirmó que a los familiares de las víctimas no les entregaron el cuerpo que correspondía.

Por lo anterior, es que este caso resulta ser importante para efectos del presente artículo pues de carecer de disposiciones que regulen el debido resguardo de documentos, no se puede hablar de una garantía normativa mínima para tener acceso a la información y documentos que se generan por parte de las entidades públicas.

Otro precedente relativo a la importancia que tienen los documentos de archivo en los procedimientos, lo encontramos en la resolución que dictó la CIDH en 2010 respecto al caso Gomes Lund y otros (“Guerrilha Do Araguaia”) vs. Brasil, ya que es en dicha resolución que la Corte sostiene que el derecho a recibir información contribuye a garantizar los derechos a la verdad, la justicia y la reparación, “evitando que se produzcan nuevas violaciones graves a derechos humanos”, y añadiendo que negar información a los familiares de las víctimas de delitos, es equiparable a la tortura.

De tal suerte que en esa perspectiva, la Corte no justificó que el Estado de Brasil negará información, por más de 25 años, a los familiares de las 70 personas que integraban el grupo de resistencia Do Araguaia.

Derivado de lo anterior, es que vale la pena precisar que en términos de lo dispuesto por los artículos 49 de la LGPDPPSO y 48.3 de la LPDPPSOEJM, los derechos ARCO concernientes a las personas fallecidas pueden ejercerse a través de aquella persona que acredite tener un interés jurídico sobre los mismos; y que analizado el contenido de los numerales 138 de la LGTAIP, 86 bis de la LTAIPEJM, 53 de la LGPDPPSO y 87 de la LPDPPSOEJM, se advierte que la legislación mexicana vigente prevé la negativa de información en función de su inexistencia, la cual puede determinarse por no tener la misma en su resguardo, lo cual no implica que ésta no se hubiera recibido o generado.

Resultados

De las respuestas atinentes a las solicitudes de información pública que se ingresaron al gobierno federal, se logra advertir que la mitad de las Direcciones Jurídicas de la Secretaría de Gobernación (SEGOB) han exhibido documentos originales como medios de prueba para la tramitación de los 1,023 juicios en los que fungen como parte, esto, sin conservar copia de los mismos ni generar un control de los documentos que salen de su resguardo; situación que se replica en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE); Fiscalía General de la República (FGR); la Secretaría de la Función Pública (SFP); Secretaría de Hacienda Pública (SFP); y Secretaría de Medio Ambiente y Recursos Naturales (SEMARNAT). Pues por lo que ve a la Secretaría de Comunicación y Transportes (SCT), esta informó que sólo exhibe copias certificadas en los procedimientos en los que funge como parte. Debiendo precisar que por lo que ve al Instituto Mexicano de Seguridad Social (IMSS), Secretaría de Salud (SSA), Secretaría de Educación Pública (SEP) y Petróleos Mexicanos (PEMEX), éstos señalaron que no se encuentran en posibilidades de informar la naturaleza de los documentos que remiten a las autoridades para la defensa de sus intereses.

Corroborando así que de ese universo de sujetos obligados, el único que se encuentra en posibilidades de garantizar de manera efectiva el ejercicio del DAI y de los derechos ARCO, es la SCT, esto, debido a que tiene un procedimiento estandarizado al interior de su sujeto obligado, el cual consiste en solamente remitir copias certificadas de sus documentos de archivo a otras autoridades.

Cosa que no se replica en ningún otro sujeto obligado del universo mencionado, ya que incluso en un mismo sujeto obligado se manejan criterios diferentes a fin de exhibir documentos en los procedimientos, como lo es en el caso de SEGOB, pues a señalar como ejemplo, SEMARNAT informó que en 7 solicitudes se negó la entrega de documentos debido a que éstos salieron de su resguardo por ser exhibidos como medios de prueba en diversos juicios de nulidad.

Logrando así advertir que el manejo de documentos que se efectúa por parte de los sujetos obligados en mención guarda estrecha relación con el déficit legal que se ha señalado en el presente artículo.

Conclusiones

Del análisis literal y sistemático de los instrumentos jurídicos anteriores, se concluye por un lado, que México carece de elementos jurídicos que permitan por un lado, garantizar efectivamente el ejercicio de los derechos ARCO y del DAI; y por otro lado, brindar plena certeza jurídica respecto a las declaraciones de inexistencia que los entes públicos realizan de conformidad a lo establecido en la LGTAIP y la LGPDPPSO, cuyas reglas se replican en las leyes locales que en dichas materias se encuentran vigentes en Jalisco.

Dicha afirmación se sostiene toda vez que en los instrumentos jurídicos de referencia se omite señalar el procedimiento que se seguirá respecto a aquellos documentos sobre de los cuales los entes públicos determinen que serán remitidos en original para ser ofertados como medios de prueba en algún procedimiento en el cual funjan como parte ante otra autoridad, ya sea judicial o administrativa.

Derivado de lo anterior, es que no en todos los casos se toman las providencias necesarias para garantizar el derecho de acceso a la información pública y los derechos ARCO de aquellas personas que deseen consultar, acceder o reproducir dichos documentos en copia simple o certificada, con lo que finalmente se termina por vulnerar estos derechos.

Lo anterior es así ya que la leyes generales y locales en mención no contemplan la derivación de competencia para la atención de solicitudes en función del resguardo de documentos que se requieran, como lo es en el caso de la República de Chile (Ley 20.285 sobre el acceso a la información pública, 2008). Dando así lugar a que se emitan declaraciones de inexistencia de documentos en función de un no resguardo o posesión de documentos, que a los supuestos previstos en las multicitadas leyes que en materia de acceso a la información pública y datos personales se encuentran vigentes en México e incluso a la literalidad de la interpretación que realizó la CIDH respecto al derecho de recibir información (CIDH, 2010).

Así las cosas se concluye que, con las declaraciones de inexistencia en mención, se contraviene a los principios de certeza jurídica y verdad material previstos en la Ley del Procedimiento Administrativo del Estado de Jalisco (LPAEJ), pues por un lado, se da vida jurídica a un documento que asevera la inexistencia de otro (s) que en realidad existe, tiene vida jurídica y salió del resguardo o dominio del sujeto obligado por voluntad de éste, sin que al respecto se observara más que lo previsto en la normatividad adjetiva que rige los procedimientos en los cuales se encuentran aquellos documentos que se han ofertado como medios de prueba, por ejemplo, el Código de Procedimientos Civiles del Estado de Jalisco (CPCCEJ) y la citada LPAEJ.

Dicha situación no es cosa menor, ya que por un lado, los documentos fungen como testigos respecto al cumplimiento de las atribuciones, funciones y obligaciones de las entidades públicas, y permiten “descubrir la verdad”; por otro lado, son la base para que los sujetos obligados se encuentren en posibilidades materiales de atender efectivamente las solicitudes que presenten las personas en ejercicio del DAI y los derechos ARCO; y finalmente, se caracterizan por fungir como derechos llave pues con su ejercicio se dota de herramientas a las personas para ejercer otros de sus derechos (Rivera Aguilar, 2004), ya sea en materia civil, laboral, administrativa, penal, y hasta en materia de salud o educación, por señalar algunos ejemplos (Gutiérrez Jiménez, 2008).

Siendo en el último de los casos en el que se genera una violación al derecho de prueba que se ha reconocido mediante Tesis Aislada I.3o.C.102 K (10a.) ya que se impide a las personas obtener los documentos que se solicitan a las entidades con la finalidad, expresa o no, de ser ofertados dentro de algún procedimiento, pues conforme a dicha Tesis, el derecho a la prueba constituye un elemento para garantizar el debido proceso ya que permite al juzgador “alcanzar un conocimiento mínimo de los hechos que dan lugar a la aplicación de las normas jurídicas pertinentes, y dar respuesta a los asuntos de su competencia.” (Tercer Tribunal Colegiado en Materia Civil del Primer Circuito, 2018).

Lo cual, puede generar un daño irreparable en los derechos de las personas pues al carecer de evidencia que acredite sus derechos, se obvia que la imposibilidad material que éstas tendrían para reclamar los mismos, impidiendo a su vez, el ejercicio de los recursos legales y de las garantías procesales pertinentes.

Propuesta

Debido a lo vertido en el presente artículo es que se propone formular una adhesión legislativa a la LGA, en el sentido de que los documentos de archivo originales sólo pueden salir del resguardo de las entidades públicas previa certificación de los mismos, esto, a fin de salvaguardar el ejercicio del DAI y de los derechos ARCO de aquellas personas que eventualmente pretendan acceder a los mismos.

Debiendo precisar a ese respecto, que la certificación correspondiente debe señalar que ésta se emite en razón de que los originales serán remitidos a una autoridad determinada con motivo del trámite de un procedimiento específico.

Lo anterior, a fin de brindar certeza respecto a lo siguiente:

a) Entidad pública que inicialmente tuvo en su resguardo los documentos de archivo en original; y

b) El motivo por el cual ya no se cuenta con los originales, así como la autoridad destinataria y el procedimiento en el que radican.

De modo que la omisión al cumplimiento de dicha disposición constituiría una sanción, por lo que en ese sentido es que se propone también reformar el artículo 116 de la LGA en tal sentido.

Tabla 4. Reforma a las vsanciones previstas en la LGA.

LGA

Vigente	Propuesta de reforma
“Artículo 116. Se consideran infracciones a la presente Ley, las siguientes:	“Artículo 116. Se consideran infracciones a la presente Ley, las siguientes:
I. (…)	I (…)
VII. Cualquier otra acción u omisión que contravenga lo dispuesto en esta Ley y demás disposiciones aplicables que de ellos deriven.”	VII. Omitir la certificación de aquellos documentos de archivo originales que salgan del resguardo de los sujetos obligados; VIII. Cualquier otra acción u omisión que contravenga lo dispuesto en esta Ley y demás disposiciones aplicables que de ellos deriven.”

Karen Michelle Martínez Ramírez

Es licenciada en Derecho por parte de la Universidad Enrique Díaz de León y maestrante en Derecho Constitucional por parte de ese mismo centro de estudios. Actualmente funge como secretario de acuerdos de ponencia en el ITEI y tiene experiencia en la atención y tramitación de recursos de revisión, de transparencia y de datos personales, así como en la coordinación y ejecución de procesos de gestión pública documental.

Referencias

Convención Americana de los Derechos Humanos (Pacto de San José). (1969) Organización de los Estados Americanos (OEA). En Departamento de Derecho Internacional de la OEA. Recuperado el 10 de julio de 2019 de https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

Estado de firmas y ratificación de la Convención Americana de los Derechos Humanos (Pacto de San José). (Sin fecha de actualización). OEA. En Departamento de Derecho Internacional de la OEA. Recuperado el 10 de julio de 2019 de https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos_firmas.htm

Declaración Universal sobre los Archivos. (2012). UNESCO. En International Council on Archives (ICA). Recuperado el día 09 de junio de 2019 de https://www.ica.org/sites/default/files/UDA_June2012_press_SP.pdf

Información para los gobiernos. (2016) ICA. Recuperado el día 09 de junio de 2019 de https://www.ica.org/en/espa%C3%B1ol

Resolución Caso Gomes Lund y otros ("Guerrilha Do Araguaia") vs. Brasil. (2010). En CIDH. Recuperado el día 10 de agosto de 2019 de www.corteidh.or.cr/docs/casos/articulos/seriec_219_esp.pdf

Resolución Caso Rodríguez Vera y otros (desaparecidos del Palacio de Justicia) vs. Colombia. En CIDH. Recuperado el día 10 de agosto de 2019 de http://www.corteidh.or.cr/docs/casos/articulos/seriec_287_esp.pdf

Constitución Española. (2011, Septiembre 27). En Boletín Oficial del Estado (BOE) 311, de fecha 29 de diciembre de 1978. Recuperado el 10 de agosto de 2019 de https://www.boe.es/eli/es/c/1978/12/27/(1)/con

Ley 7/2011, de 3 de noviembre, de Documentos, Archivos y Patrimonio Documental de Andalucía. (2014, Junio 30) En BOE núm. 286, de fecha 28 de noviembre de 2011. Recuperado el 10 de agosto de 2019 de https://www.boe.es/eli/es-an/l/2011/11/03/7/con

Ley 20.285 Sobre Acceso a la Información Pública. (2016, Enero 05). En Congreso Nacional de Chile. Recuperado el 15 de agosto de 2019 de https://www.leychile.cl/Navegar?idNorma=276363

Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. (2000). Archivo General de la Nación de Colombia. Recuperado el 15 de agosto de 2019 de https://normativa.archivogeneral.gov.co/ley-594-de-2000/

Ley General de Transparencia y Acceso a la Información Pública. (2015) En Cámara de Diputados del H. Congreso de la Unión. Recuperado el día 15 de julio de 2019 de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (2017) En Cámara de Diputados del H. Congreso de la Unión. Recuperado el día 15 de julio de 2019 de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ley General de Archivos. (2018) En Cámara de Diputados del H. Congreso de la Unión. Recuperado el día 15 de julio de 2019 de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA_150618.pdf

Ley Federal de Archivos. (2012, abrogada) En Cámara de Diputados del H. Congreso de la Unión. Recuperado el día 15 de julio de 2019 de http://www.diputados.gob.mx/LeyesBiblio/abro/lfa/LFA_abro.pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios (2019, Julio 11). En el H. Congreso del Estado de Jalisco. Recuperado el día Recuperado el día 15 de julio de 2019 de https://congresoweb.congresojal.gob.mx/BibliotecaVirtual/busquedasleyes/Listado.cfm#Leyes

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. (2017) En el H. Congreso del Estado de Jalisco. Recuperado el día 15 de julio de 2019 de https://congresoweb.congresojal.gob.mx/BibliotecaVirtual/busquedasleyes/Listado.cfm#Leyes

Código de Procedimientos Civiles del Estado de Jalisco. (2018, Septiembre 1°) En el H. Congreso del Estado de Jalisco. Recuperado el día 15 de julio de 2019 de https://congresoweb.congresojal.gob.mx/BibliotecaVirtual/busquedasleyes/Listado.cfm#Leyes

Ley del Procedimiento Administrativo del Estado de Jalisco (2019, Mayo 11). En el H. Congreso del Estado de Jalisco. Recuperado el día 15 de julio de 2019 de https://congresoweb.congresojal.gob.mx/BibliotecaVirtual/busquedasleyes/Listado.cfm#Leyes

Lineamientos para la Organización y Conservación de los Archivos. (2016, mayo 04) En el Diario Oficial de la Federación. Recuperado el día 15 de julio de 2019 de http://dof.gob.mx/nota_detalle.php?codigo=5436056&fecha=04/05/2016

Tercer Tribunal Colegiado en Materia Civil del Primer Circuito. (2019, Mayo 03) Tesis I.3º.C.103 K (10ª.). En Semanario Judicial de la Federación. Recuperado el 15 de agosto de 2019 de https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2019776&Clase=DetalleTesisBL&Semanario=0

Primer Tribunal Colegiado en Materia Penal del Primer Circuito. (2018, Septiembre 07) Tesis I.1oP.33 K (10ª). Recuperado el 15 de agosto de 2019 de https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2017816&Clase=DetalleTesisBL&Semanario=0

Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia. (2014, Febrero 07) Diario Oficial de la Federación de México. En Cámara de Diputados del H. Congreso de la Unión, DOF 07-02-2014. Recuperado el 06 de junio de 2019 de http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf

Comisiones Unidas de Puntos Constitucionales; De Estudios Legislativos; De Gobernación y Anticorrupción, et al. (2012, Diciembre 19). En Cámara de Senadores del H. Congreso de la Unión. Recuperado el día 09 de junio de 2019 de http://www.senado.gob.mx/comisiones/estudios_legislativos1/docs/relevantes/RCMT_3-1.pdf

La Administración de los Archivos Municipales. (1985) Instituto Nacional de Administración Pública. Recuperado el 19 de junio de 2019 de https://archivos.juridicas.unam.mx/www/bjv/libros/4/1707/1.pdf

Diccionario Jurídico Mexicano, tomo II, pate ocho. (1982) De Instituto de Investigaciones Jurídicas de la Universidad Autónoma de México. Recuperado el 19 de junio de 2019 de https://archivos.juridicas.unam.mx/www/bjv/libros/3/1168/8.pdf

Fotografía: Mati Mango para Pexels.com

De lo virtual a lo real: en diez meses el SIPOT ha sufrido 77 mil 927 ataques cibernéticos

María Del Rosario Navarro Zamora

Coordinadora de Procesos Normativos en el ITEI

Resumen

El Sistema de Portales de Obligaciones de Transparencia (SIPOT) de la Plataforma Nacional de Transparencia (PNT), fue creado derivado de una política pública transversal de Transparencia, Acceso a la Información y Protección de Datos, ante la falta de homologación en la publicación y actualización de la información fundamental general y específica de los sujetos obligados del país.

Lo anterior, debido a que cada sujeto obligado publicitaba en sus portales de Internet, sin ningún tipo de aprobación o estandarización con los demás países; acarreando un problema para la ciudadanía en la consulta de la información fundamental.

Es por ello, que se crea el SIPOT con los Lineamientos Técnicos Generales de Publicación, Homologación y Estandarización de la Información, para que todos los sujetos obligados del país publiquen la información fundamental de una misma manera; y con ello la ciudadanía pueda consultarla sin complicaciones.

Ahora bien, al ser una Plataforma a través de la cual su acceso es utilizando Internet, sabemos que los límites de éste no existen y es complicada la regulación debido a que en el *ciberespacio interactúan los sistemas informáticos, redes e infraestructura, utilizando medios físicos y el espectro electromagnético para interconectarse.*[1]

En razón de lo antes referido, el SIPOT se ha tornado vulnerable a ataques cibernéticos, dado que cualquier persona con tan solo utilizar un equipo de cómputo, móvil o tableta conectada a Internet puede acceder al Sistema y si éste no cuenta con las debidas medidas de seguridad puede ser vulnerado.

PALABRAS CLAVES:

Plataforma Nacional de Transparencia, Sistema de Portales de Obligaciones de Transparencia, Ciberespacio, Ciberseguridad, Pentesting

[1] Centro de Estudios Estratégicos CEEAG. (2018). La Ciberguerra: Sus impactos y desafíos. Chile: Comité Editorial del CEEAG, página 18.

No obstante que el INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) cuenta con seguridad informática dentro del Instituto necesaria para proteger el SIPOT, así mismo hace uso de herramientas de propósito específico tanto en el perímetro de comunicaciones del Instituto como en los puntos finales, para la protección de la tecnología que contiene éste.[2]

Sin embargo, el SIPOT de la PNT en tan solo diez meses ha sufrido 77 mil 927 ataques cibernéticos; los cuales si bien es cierto el INAI manifestó que fueron contenidos por las capas de seguridad, como consecuencia no se convirtieron en incidentes de seguridad que hayan provocado algún riesgo para el Instituto.

La situación es que lo virtual superó la realidad y a pesar de todas las medidas de seguridad el SIPOT sufrió ataques cibernéticos. Ciertamente *el INAI, es el administrador de la Plataforma, pero también los órganos garantes son responsables de verificar de manera periódica y constantes los sistemas de la PNT.*[3]

Introducción

El presente artículo antes de aterrizar en los ataques cibernéticos que ha sufrido el SIPOT de la PNT, hace un recorrido desde la creación de la Ley General de Transparencia y Acceso a la Información Pública, lo que establece ésta en relación a la PNT y al SIPOT; derivado de lo anterior la necesidad de crear unos lineamientos para implementar y operar la PNT. Se explica brevemente lo relacionado con el ciberespacio y todo lo que éste implica; se hace referencia al *Pentesting* para finalmente explicar el tema central del artículo en comento.

En relación a lo anterior, se establece que el 16 dieciséis de abril del año 2015 dos mil quince, el Congreso General de los Estados Unidos Mexicanos, aprobó el Proyecto de Decreto por el cual se expide la Ley General de Transparencia y Acceso a la Información Pública (Ley General), mismo que fue publicado en el Diario Oficial de la Federación, el 04 de mayo del año 2015 dos mil quince, entrando en vigor al día siguiente de su aprobación.

Ahora bien, en el artículo Quinto Transitorio de la Ley General, se establece que el Congreso de la Unión, las legislaturas de los Estados y la Asamblea Legislativa del Distrito Federal, tendrán un plazo de hasta un año, contado a partir de la entrada en vigor del Decreto aludido en el párrafo que antecede, para armonizar la leyes relativas, conforme a los principios, bases general y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios.

Por otra parte, el artículo 49, de la Ley General, establece que los organismos garantes desarrollarán, administrarán, implementarán y pondrán en funcionamiento la plataforma electrónica que permita cumplir con los procedimientos, obligaciones y disposiciones

[2] Respuesta entregada el 04 de junio de 2019, a la solicitud de información presentada ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a la cual le correspondió el número de folio 0673800104519.

[3] Lineamiento décimo tercero y décimo cuarto del Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales por el que se aprueban los Lineamientos para la implementación y operación de la Plataforma Nacional de Transparencia

señaladas en la Ley General para los sujetos obligados y organismos garantes, de conformidad con la normatividad que establezca el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, atendiendo a las necesidades de accesibilidad de los usuarios.

Asimismo, el artículo 50, de la Ley General, refiere que la PNT se conformará por al menos, cuatro sistemas; esto es: Sistema de solicitudes de acceso a la información (SISAI); Sistema de gestión de medios de impugnación (SIGEMI); Sistema de portales de obligaciones de transparencia (SIPOT), y Sistema de comunicación entre organismos garantes y sujetos obligados (SICOM).

En otro orden de ideas, el 04 cuatro de mayo del año 2016 dos mil dieciséis, se publicó en el Diario Oficial de la Federación el Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales por el que se aprueban los Lineamientos para la implementación y operación de la Plataforma Nacional de Transparencia (Lineamientos de la PNT).

El lineamiento primero de los Lineamientos de la PNT, refiere que éstos tienen por objeto establecer las reglas de operación, garantizando su estabilidad y seguridad, promoviendo la homologación de procesos y la simplicidad del uso de los sistemas que conforman la citada PNT para los usuarios, garantizando en todo momento los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados.

De igual forma, en el lineamiento quinto señala que la PNT es el instrumento informático a través del cual se ejercerán los derechos de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, así como su tutela, en medios electrónicos, de manera que garantice su uniformidad respecto de cualquier sujeto obligado, y sea el repositorio de información obligatoria de transparencia nacional.

En ese sentido, el lineamiento décimo de los Lineamientos de la PNT, refiere que el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI) será el responsable de brindar la capacitación en la operación de la PNT a los organismos garantes y, éstos a su vez, tendrán la responsabilidad de capacitar a sus sujetos obligados.

Asimismo, el lineamiento décimo tercero de los Lineamientos de la PNT, establece que en caso de que ésta presente una falla técnica, el INAI, como administrador, deberá hacer del conocimiento de los organismos garantes y sujetos obligados la magnitud de la falla y el tiempo de recuperación, para que éstos estén en posibilidad de implementar las medidas necesarias para el cumplimiento de sus respectivas responsabilidades.

En relación con lo anterior, el lineamiento décimo tercero de los Lineamientos de la PNT, refiere que el impedimento temporal, por caso fortuito o fuerza mayor, suspenderá los términos establecidos para cualquier trámite realizado a través de la PNT, hasta en tanto dure dicho impedimento; caso en el cual, el INAI comunicará a los organismos garantes que correspondan el periodo de suspensión para que éstos a su vez lo informen a sus sujetos obligados.

Además, el lineamiento décimo cuarto de los Lineamientos de la PNT, señala que será responsabilidad de los organismos garantes verificar de manera periódica y constante los sistemas de la PNT, con la finalidad de dar pronta atención a los mismos.

Por otro lado, los lineamientos vigésimo y vigésimo primero, de los Lineamientos de la PNT, describe que en el caso del SIPOT, el INAI será el responsable de:

a) Realizar la configuración base de los formatos que atiendan lo establecido en la Ley General, y

b) Efectuar las configuraciones a: temas; subtemas; sectores; normatividad general, y formatos generales.

En ese mismo sentido, los lineamientos del vigésimo octavo, al trigésimo primero, de los Lineamientos de la PNT, establecen que el INAI, en relación a la PNT será responsable de:

a) Mantenerla disponible en todo momento, para tal efecto implementará los mecanismos necesarios para que la operabilidad sea garantizada en la medida de lo posible en caso de contingencias o casos fortuitos;

b) Vigilar el correcto funcionamiento;

c) Implementar el mecanismo de recuperación de desastres y contingencias, e

d) Implementar el plan de respaldos de ésta (el cual hará de conocimiento a los organismos garantes).

Por otra parte, los lineamientos vigésimos, vigésimo segundo, vigésimo sexto, vigésimo séptimo, centésimo décimo segundo y centésimo décimo tercero de los Lineamientos de la PNT, establecen que con el apoyo técnico del INAI, los organismos garantes serán responsables de:

a) Realizar la configuración de las particularidades según la normatividad local aplicable en cada entidad federativa;

b) Realizar las configuraciones a: normatividad local; formatos locales; criterios; metodología de evaluación; periodos de evaluación formal; clasificación de sujetos obligados, y asignación de normatividad, formatos y sujetos obligados;

c) Mantener actualizada la información relacionada con el listado, directorio y unidades administrativas de sus sujetos obligados;

d) Configurar los criterios y obligaciones de transparencia adicionales contemplados en la normatividad local correspondiente, y

e) Dar de alta a los sujetos obligados de su competencia.

De la misma manera, el uso de la PNT será obligatorio para todos los sujetos obligados a nivel federal, estatal y municipal, de conformidad con lo establecido en los Transitorios Octavo y Décimo de la Ley General.

Ahora bien, los lineamientos trigésimo tercero al trigésimo quinto de los Lineamientos de la PNT, describen que el uso de ésta no tendrá costo para los usuarios; asimismo algunas secciones requerirán que las personas dispongan de un usuario y contraseña; así como solicitará el uso de equipo de cómputo o dispositivos móviles que cuenten con acceso a Internet.

En relación con lo anterior, los lineamientos trigésimo sexto y trigésimo séptimo de los Lineamientos de la PNT, detallan que como consecuencia, la PNT permitirá la interoperabilidad de la información contenida en cada sistema y entre los diversos sistemas, mediante servicios web a través de un bus de servicios empresariales; y contará con servicios que permitirán exportar información contenida en ésta por cualquier particular, sujeto obligado u organismo garante que así lo requiera.

Para el caso que nos ocupa, es indispensable conocer la definición del SIPOT. Es por ello que el lineamiento centésimo décimo de los Lineamientos de la PNT, señala que es la herramienta electrónica a través de la cual los sujetos obligados de los tres niveles de gobierno, ponen a disposición de los particulares la información referente a las obligaciones de transparencia contenidas en la Ley General, Ley Federal o Ley Local.

Por lo antes vertido, el lineamiento centésimo décimo cuarto, de los Lineamientos de la PNT, refiere que el SIPOT permite tres métodos de carga de la información a través de:

a) Un formulario web;

b) Un archivo xml cuya estructura estará determinada por el INAI; y

c) De un servicio web.

Desde otro ángulo, en una Auditoría Financiera y de Cumplimiento, se estableció que el INAI, señaló que la PNT entraría en operaciones el 5 de mayo de 2016. Para ello el INAI planteó dos etapas para el desarrollo e implementación de la PNT, la primera de septiembre a diciembre de 2015 y su alcance consistía en llevar a cabo mejoras SISAI, SIPOT, y desarrollar el SIGEMI y el SICOM; y la segunda de febrero a diciembre de 2016, para realizar adecuaciones derivadas por la normatividad emitida por el SNT y la armonización con las Leyes Locales de los Estados de la República en la materia y desarrollos adicionales, y mejoras a la PNT.[4]

En relación con lo antes mencionado derivado de una presentación de power point hecha por el INAI, la cual tituló "Pruebas de PNT rediseñada", se refiere que el 12 doce de diciembre del año 2017 dos mil diecisiete, la Comisión de Tecnologías de la Información y Plataforma Nacional de Transparencia, realizaron mejoras a la consulta pública del SIPOT y trabajaron en un rediseño de la totalidad de la Plataforma.

De la misma forma, las citadas láminas establecieron que el 21 veintiuno de septiembre del año 2018 dos mil dieciocho, fueron presentados los avances a las mejoras y el rediseño de la PNT, acordando la retroalimentación de dichos avances y la realización de las pruebas con todos los organismos garantes del país.

Posteriormente, en la aludida presentación se describió que el 15 quince de noviembre del año 2018 dos mil dieciocho, se presentó a los organismos garantes el rediseño y se proporcionó una liga para realizar una revisión y pruebas.

Subsiguientemente, la exposición señaló que el 13 trece de diciembre del año 2018 dos mil dieciocho, el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, mencionó que antes de la puesta en producción de la PNT rediseñada se realizarían pruebas de funcionamiento de los componentes que la integran.

De esta manera, el INAI a través de su presentación plasmó que las pruebas se llevaron a cabo a nivel nacional el 09 nueve y 16 dieciséis de febrero; así como el 09 nueve de marzo del año 2019 dos mil diecinueve.

Finalmente las "Pruebas de la PNT rediseñada" trajeron como consecuencia una reingeniería de los procesos, simplificación del lenguaje y mejora de rutas de navegación, que entró en funcionamiento el 08 ocho de abril del año 2019 dos mil diecinueve.

Por otro lado, el Centro de Estudios Estratégicos (CEEAG) a través de su libro titulado La Ciberguerra: Sus impactos y desafíos (2018.p.31), establece que el Internet carece de fronteras y el contenido ilícito circula de un país a otro en milésimas de segundos, además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, centros educativos, máquinas populares de acceso a Internet y otras donde de forma anónima las personas pueden conectarse y realizar actividades ilícitas.

A lo anterior, el CEEAG (2018.p.45), refirió que se suma el desarrollo de los computadores y software, junto con los aparatos móviles de comunicaciones de grandes capacidades, siendo estos últimos en la actualidad los principales medios por los que se accede a Internet. Este desarrollo tecnológico ha traído consigo acceso a grandes cantidades de data, transmisión de archivos, correos electrónicos, mensajería instantánea, etc., incluyendo el acceso a información general, privada, incluso de tipo personal, lo que facilita y simplifica la vida tanto en los ámbitos personal como profesional.

Para facilitar o gestionar lo anterior, se han creado sistemas de redes, almacenamiento y distribución de megadatos, comunicaciones y otra variedad de infraestructuras que dan sustento al "negocio" de cada una de estas organizaciones en pos de sus fines. Pero así como se facilita y se hace más expedito todo

[4] Respuesta entregada el 17 de mayo de 2019, a la solicitud de información presentada ante la Auditoría Superior de la Federación, a la cual le correspondió el número de folio 0110000043319.

nuestro quehacer, también se hace más vulnerable, surgiendo riesgos que pueden llegar a convertirse en serias amenazas, afectando particularmente los servicios, organizaciones y estructuras que tienen un rol vital en el desarrollo de las actividades esenciales del ser humano del mundo moderno, las que en particular se denominan infraestructuras críticas (IC), cuyo daño o afección puede tener graves efectos en los intereses esenciales y la seguridad de cualquier país. Estos riesgos provienen de múltiples fuentes y se manifiestan mediante actividades de espionaje, sabotaje, fraudes o ciberataques realizados por otros países, por grupos organizados o por particulares, entre otros, surgiendo las denominadas ciberamenazas. (Centro de Estudios Estratégicos, 2018, p. 46)

Por otra parte, el Centro de Estudios Estratégicos, a través de su libro titulado La Ciberguerra: Sus impactos y desafíos, (2018. p. 17), estableció que la complejidad del tema informático aumentó con la conectividad de computadores y bases de datos, generando la aparición de un espacio virtual o "ciberespacio", como medio de transmisión de datos. Ya no bastaba contar con un computador aislado, sino que su integración a la transferencia de información vino a catalizar notoriamente su importancia como medio informático.

El referido Centro de Estudios Estratégicos, estableció que el ciberespacio consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores. Se puede complementar esta definición con lo que conceptualiza la Comisión Europea como *"el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo"* y por último la UIT (Unión Internacional de las Telecomunicaciones) como el lugar creado para la interconexión de sistemas de ordenador mediante Internet.

En la consecuencia del análisis de las múltiples definiciones de ciberespacio tenidas a la vista, hay elementos comunes que se encuentran en cada una de ellas, resaltando la importancia estructural que dichos conceptos revisten, entre los que destacan "espacio virtual", "datos", "interdependencia e interconexión", "información" e "infraestructura de redes", términos todos que confluyen para un mejor entendimiento de lo que la quinta dimensión viene a significar. Por ello, el ciberespacio va a estar caracterizado por una red de información que lo conforma, donde confluyen redes de tecnología de comunicaciones interconectadas que harán que esa información esté globalmente disponible, usando para ello conexiones físicas e inalámbricas, a altas velocidades. (Centro de Estudios Estratégicos, 2018, p. 20).

Algunas de las características del ciberespacio establecidas en el Manual *Cybrespace and Electronic Warfare Operations*, FM 3-12, son: Opera en Red, catalizador social, tecnología, interdependiente e interrelacionada y vulnerable.

En otro orden de ideas, la ciberseguridad[5] puede ser entendida como el conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. Entonces, asegura el uso de las redes propia y niega su empleo a terceros.

La Unión Internacional de Telecomunicaciones, referida en Gómez Abutridy Alejandro, Ciberseguridad y Ciberdefensa, Dos elementos de la Ciberguerra, Memorial del Ejército de Chile No. 492, agosto 2014. Define a la ciberseguridad como *"El conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión, acciones, formación, prácticas idóneas, seguros y tecnologías que vvpueden utilizarse para proteger los activos de una organización y a los usuarios en el ciberentorno"*.

La UIT dice que la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos, cuales son amenazas de seguridad correspondientes en el ciberentorno. Luego, entendiendo que la problemática de la ciberseguridad

[5] Jeimy Cano J. Ciberseguridad y Ciberdefensa: Dos tendencias emergentes en un contexto global, Sistemas (Asociación Colombiana de Ingenieros de Sistemas). Vol. 000, No. 0119 (Abr-Jun. 2011) pp.4-7.

requiere un esfuerzo colectivo y coordinado entre los diferentes países, establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones: desarrollo de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional.

La ciberseguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan afectar los potenciales atacantes. Estos son la confidencialidad, la integridad y la disponibilidad de los recursos, CIA *(Confidentiality-Integrity-Availability)*. (Centro de Estudios Estratégicos, 2018, p. 69).

Ahora bien, refiere Marcos Robledo Hoecker, Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre ciberseguridad, PNCS 2017, p. 9, que *hace bastante tiempo que el ciberespacio dejó de ser parte de la ciencia ficción para convertirse en uno de los principales espacios de interacción social.*

En relación con lo antes vertido, es pertinente conocer el concepto de resiliencia el cual es definido por Arturo M. Calvente, *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales como "las condiciones de un sistema complejo alejado del equilibrio, donde las inestabilidades pueden transformar al mismo para que presente otro régimen de comportamiento, así la resiliencia es medida por la magnitud de perturbaciones que pueden ser absorbidas por el sistema antes de que sea reorganizado con diferentes variables y procesos".

Por lo antes mencionado, el concepto de la resiliencia está directamente asociado con la sustentabilidad de todo sistema complejo; ésta no es una propiedad absoluta y fija sino que, por el contrario, es variable en el tiempo y el espacio y depende, en gran medida, de las acciones y relaciones del sistema y la volatilidad ambiental del contexto en el que se encuentre. (Centro de Estudios Estratégicos, 2018, páginas 147 y 148).

En otro orden de ideas, el Instituto Nacional de Ciberseguridad (INCIBE), a través de un artículo publicado en julio del presente año, ha definido al *"pentesting como el conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas"*.

En ese mismo sentido refiere el artículo publicitado que *las auditorías comienzan con la información almacenada en fuentes de acceso abierto, de información sobre la empresa, los empleados, usuarios, sistemas y equipamientos*.

El INCIBE, establece que *las citadas auditorías examinan las vulnerabilidades que se intentarán explotar, incluso con técnicas de ingeniería social, atacando a los sistemas hasta conseguir sus objetivos*.

De igual forma, el citado artículo reseña que las auditorías emiten un informe a través del cual muestra si los ataques tendrían éxito, y en caso afirmativo por qué y qué información o acceso obtendrían, es decir, se simulan ataques tal y como los llevaría a cabo un ciberdelincuente que quisiera hacerse del control del sistema o de la información en él contenida.

Asimismo, el artículo publicitado relata que las auditorías establecen: *Si el sistema informático es vulnerable o no; evalúan si las defensas con las que cuenta, son suficientes y eficaces, y valoran la repercusión de los fallos de seguridad que se detecten*.

Ahora bien, manifiesta el INCIBE, que en el desarrollo del *pentesting se realiza un plan con un conjunto de ataques dirigidos, según la tecnología que se utilice en la empresa y sus necesidades de seguridad.*

Para ello, los auditores deben de contar con metodologías; elegir qué pruebas se requiere realicen y sobre qué aplicaciones o servicios.

En relación con lo anterior el referido INCIBE menciona que existen diferentes tipos de pruebas de penetración según la información inicial con la que cuenta el auditor, así, pueden ser:

a) **De caja blanca:** si disponen de toda la información sobre los sistemas, aplicaciones e infraestructura, pudiendo simular que el ataque se realiza por alguien que conoce la empresa y sus sistemas;

b) **De caja gris:** si dispone de algo de información pero no de toda;

c) **De caja negra:** si no dispone de información sobre nuestros sistemas; en este caso, se simula lo que haría un ciberdelincuente ajeno.

El Instituto Nacional de Ciberseguridad, concluye que *al realizar el servicio, el auditor o empresa va a intentar traspasar las medidas de seguridad de los equipos informáticos o de aplicaciones, poniendo en riesgo el funcionamiento de los sistemas, así como la información que contengan*.

Una vez expuesto lo anterior y debido a que el presente artículo está relacionado con la ciberseguridad en el SIPOT de la PNT, es pertinente mencionar que el 04 cuatro de junio del presente año, el INAI, dio respuesta a la solicitud 0673800104519, de la cual se desprende que éste no tiene implementado en su totalidad un Sistema de Gestión de Seguridad (SGSI). Sin embargo, actualmente lo está gestionando el área de Seguridad de la Información perteneciente a la Dirección General de Tecnologías de la Información (DGTI) del INAI.

De esta forma, manifiesta el INAI en su respuesta que cuenta con seguridad informática dentro del Instituto necesaria para proteger al SIPOT, misma que comprende desde políticas y controles de seguridad, apegadas al MAAGTICSI, haciendo uso de las mejores prácticas en materia de seguridad informática, alineadas a la norma ISO-27000. De igual forma, refiere que los controles cubren las siguientes áreas en materia de seguridad: Segregación de tareas; Acceso a redes y a los servicios de red; Registro y desregistro de usuarios; Provisión de acceso de usuario; Sistema de gestión de contraseñas; Controles físicos de entrada; Copia de seguridad de la información; Controles de red; Seguridad de servicios de red; Respuesta a incidentes de seguridad de la información; y Aplicación de la continuidad de la seguridad de la información.

De igual forma en la respuesta a la solicitud el INAI, asevera que hace uso de herramientas de propósito específico tanto en el perímetro de comunicaciones del Instituto, en los puntos finales como son *Firewall*, IPS, Antivirus, WAF, para protección de la tecnología que contiene el SIPOT, las cuales son utilizadas para la protección específica, esto es: Control de acceso; Analizador de tráfico; Filtrado *Web*; Prevención y detección de Intrusos; Protección de aplicaciones *Web*; Detección y protección de amenazas avanzadas; y Protección *Antimalware*.

Además, en la respuesta a la solicitud el INAI manifiesta que a través de la programación con la que está construida el SIPOT permite descartar que los sujetos obligados por desconocimiento, malicia y/o negligencia suban archivos que pudieran contener programas dañinos (virus, troyanos, *malware*, etc), toda vez que el SIPOT permite descartar archivos que no cumplen con ciertas características válidas que debe tener un archivo para ser cargado en el SIPOT lo cual disminuye riesgos de cargar programas dañinos. Adicional a esto, la infraestructura del sistema, cuenta con capas de seguridad robustas, desde el perímetro hasta los equipos (*endpoints*).

En su respuesta el INAI manifiesta que las intrusiones no autorizadas al SIPOT que pudieran extraer información, alterarla, borrarla, encriptarla, etc, tales como el *hackeo*, se previene mediante mecanismos de detección y prevención de amenazas avanzadas, así como la protección de seguridad perimetral y seguridad a nivel equipo (*endpoint*).

De igual manera, el INAI refirió en su respuesta que las medidas de resiliencia implementadas en el SIPOT son una alta disponibilidad en los servicios tanto de comunicación como de infraestructura utilizados en los sistemas mencionados.

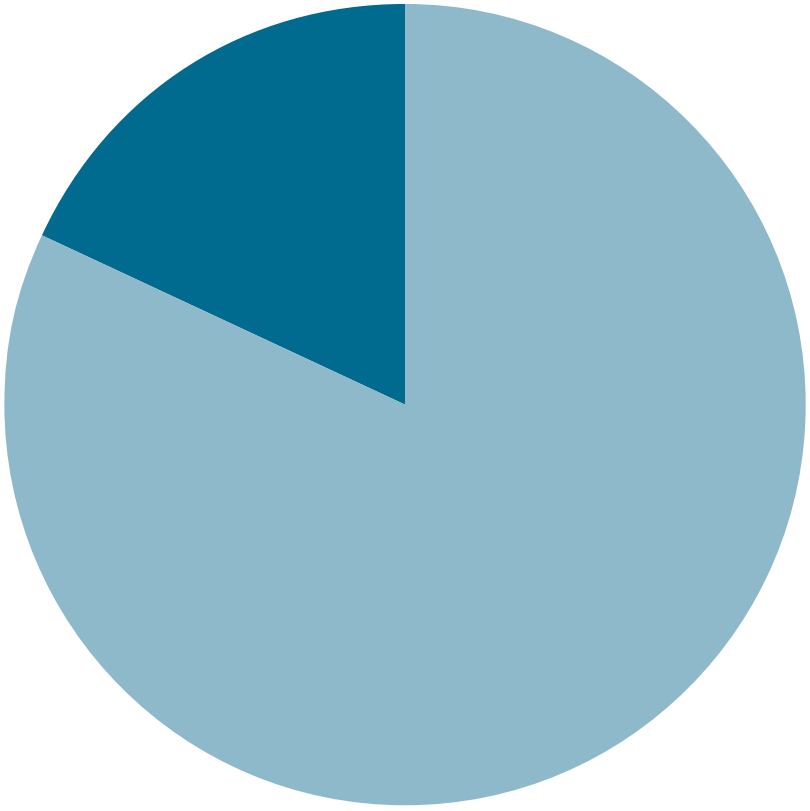
Por otra parte, en relación a ¿cuántos ataques cibernéticos detectados ha sufrido el SIPOT y/o PNT desde su creación y en qué fechas?, el INAI respondió que el SIPOT se encuentra protegido por varias capas de seguridad, las cuales al ser muy robustas generan grandes números de registros mismos que se van sobrescribiendo para la reutilización de recursos de memoria y almacenamiento en los mismos, es por esto que los datos que se proporcionaron son a partir del mes de agosto del año 2018; resaltó el INAI que dichos ataques fueron contenidos por las capas de seguridad, como consecuencia no se convirtieron en incidentes de seguridad que hayan provocado algún riesgo para el citado Instituto. El número de ataques, se ven reflejados en la siguiente tabla:

Periodo	Ago 2018	Sep 2018	Oct 2018	Nov 2018	Dic 2018	Ene 2019	Feb 2019	Mar 2019	Abr 2019	May 2019
No. de ataques	2,564	3,207	891	137	7,064	11,814	12,435	10,620	16,879	12,316

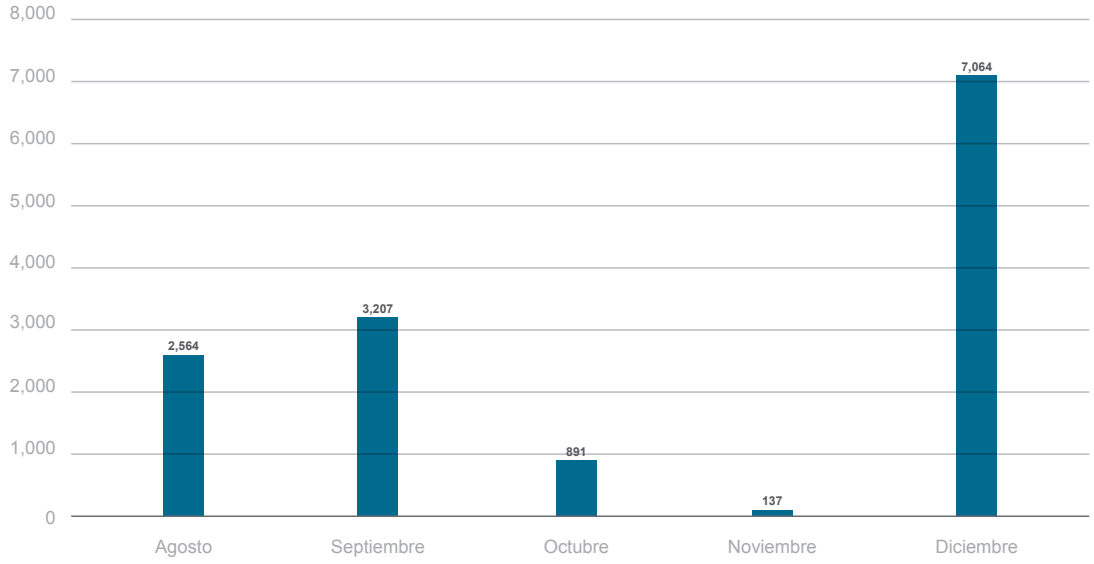
En virtud de lo antes referido la información proporcionada por el INAI, es a partir de agosto del año 2018 (y no desde la implementación del SIPOT, esto es 05 de mayo del año 2016) hasta mayo del año 2019 (derivado que la respuesta a la solicitud de información fue otorgada el 4 de junio del presente año).

De lo anterior se desprende que entre agosto de 2018 a mayo de 2019; ósea en tan solo diez meses el SIPOT recibió **77 mil 927** ataques cibernéticos; lo que se traduce que de **agosto a diciembre del año 2018 fueron 13 mil 863;** y de **enero a mayo del año en curso 64 mil 064** ciberataques, lo cual se ilustra de la siguiente manera:

Número de ataques en 10 meses



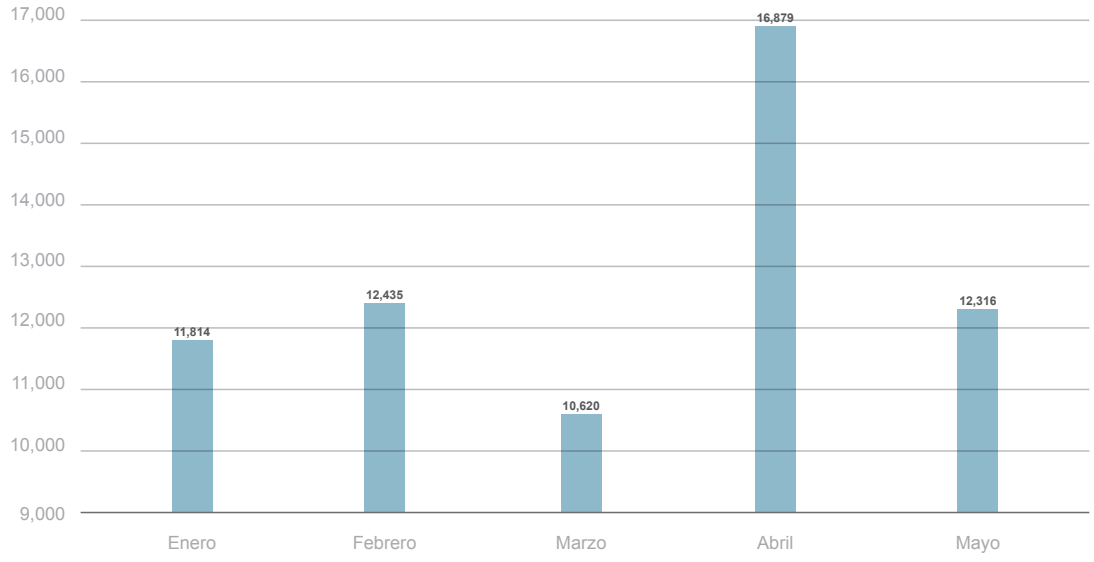
La siguiente gráfica muestra la cantidad de ataques cibernéticos que tuvo en cinco meses el SIPOT, en el año 2018:



2018

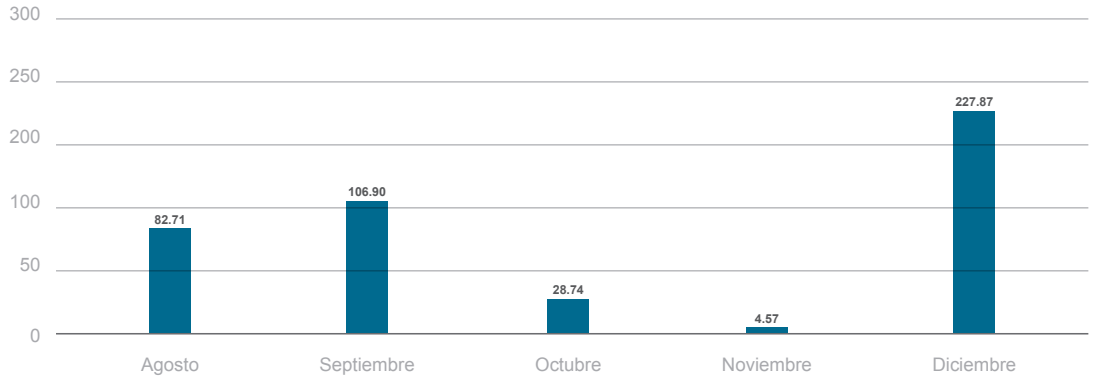
Gráfica de autoría propia

De igual forma, a continuación se visualiza la cantidad de ciberataques que sufrió el SIPOT en cinco meses del año 2019:



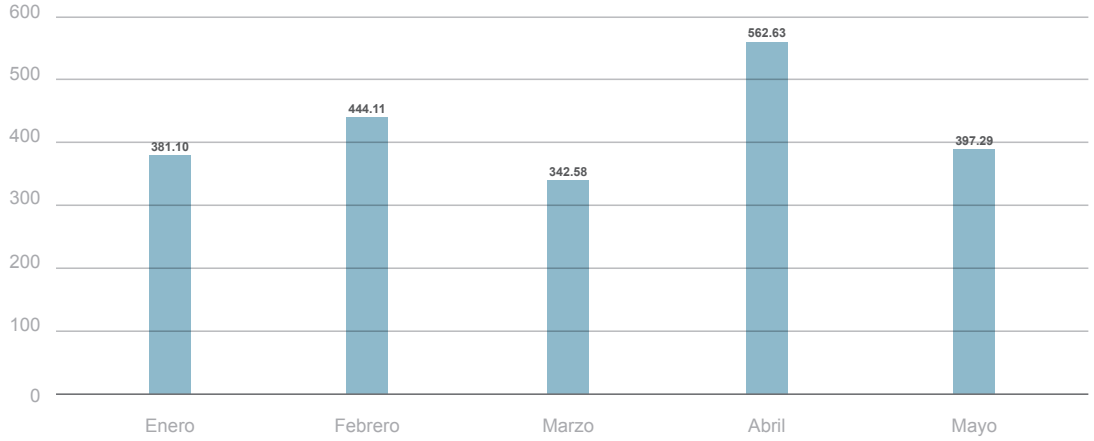
2019

Asimismo, se puede ilustrar la cantidad diaria de ataques cibernéticos recibidos en el SIPOT, por mes durante el año 2018:



2018

En ese mismo sentido, se muestra la cantidad de ciberataques diarios por mes recibidos en el SIPOT, durante el año 2019:



2019

De lo ilustrado en líneas que anteceden, se desprende que en los cinco meses del año 2018, el mes que tuvo menor cantidad de ataques cibernéticos fue noviembre con 137, no obstante el que tuvo más fue diciembre con 7,064.

En ese mismo sentido, en relación al año 2019, el mes que tuvo menor cantidad de ataques cibernéticos fue marzo con 10 mil 620, sin embargo el que tuvo más fue abril con 16 mil 879.

De la información descrita, se puede traducir en que diariamente durante los cinco meses del año 2018, mínimo se recibieron 4.57 ataques ciberataques y máximo 227.87.

Asimismo, se desglosa que diariamente durante los cinco meses del año 2019, mínimo se recibieron 342.58 ataques cibernéticos y máximo 562.63.

Todo lo antes mencionado, se ve reflejado en un acrecentamiento ya sea de una manera anual, mensual o diaria el incrementó de ataques cibernéticos que sufrió el SIPOT entre los cinco meses del año 2018 y de enero a mayo del presente año, es desorbitante.

Es decir, los 13 mil 863 ataques cibernéticos de cinco meses del año 2018 contra los 64 mil 064 ciberataques de enero a mayo del presente año, recibidos por el SIPOT se ve reflejado en un incremento de 362.12% entre 2018 y 2019.

No obstante todas las medidas de seguridad y protección específica con la que cuenta el SIPOT, en 10 meses ha sufrido una cantidad muy considerable de ataques cibernéticos (77 mil 927) y aunque resalta el INAI que dichos ataques fueron contenidos por las capas de seguridad y como consecuencia no se convirtieron en incidentes de seguridad que hayan provocado algún riesgo para ese Instituto; el incremento entre un año y otro es desmedido. Y no estamos hablando de años completos sino de una muestra de cinco meses por cada año; pero el incremento del 362.12% entre un año y otro es preocupante.

Conclusiones

En la política pública transversal de Transparencia, Acceso a la Información y Protección de Datos, sin tomar en cuenta el rediseño de la PNT (08 de abril del año 2019) ha costado alrededor de $40,008.70; esto es en el año 2015 el INAI ejerció 9,663.2 miles de pesos para el desarrollo de la PNT (Primera Etapa). Asimismo, en el año 2016, para continuar la segunda etapa se ejerció un presupuesto de 9,992.6 miles de pesos. En ese mismo, sentido también se invirtió 20,352.9 miles de pesos en la Tercerización de servicios profesionales de informática para los sistemas institucionales.[6]

Por otra parte, como se mencionó al inicio del presente artículo de conformidad con los lineamientos vigésimo, vigésimo primero, del vigésimo octavo al trigésimo primero de los Lineamientos de la PNT, el INAI tiene diversas responsabilidades, entre las que destacan: mantener disponible en todo momento la PNT, para implementar los mecanismos necesarios para que la operabilidad sea garantizada en la medida de lo posible en caso de contingencias o casos fortuitos; vigilar el correcto funcionamiento de la PNT; implementar el mecanismo de recuperación de desastres y contingencias, y el plan de respaldos de la PNT.

No obstante que el INAI es el administrador de la Plataforma, con sus cuatro sistemas SISAI; SIGEMI; SIPOT, y SICOM, de conformidad con el lineamiento décimo cuarto de los Lineamientos de la PNT, será responsabilidad de los organismos garantes verificar de manera periódica y constante los sistemas de la PNT, con la finalidad de dar pronta atención a los mismos.

De igual forma, el Centro de Estudios Estratégicos CEEAG. (2018), a través del libro titulado La Ciberguerra: Sus impactos y desafíos, refiere que el ciberespacio existe en lo virtual, con efectos en lo real, conformando un escenario creado y sustentado, con

[6] Respuesta entregada el 17 de mayo de 2019, a la solicitud de información presentada ante la Auditoría Superior de la Federación, a la cual le correspondió el número de folio 0110000043319.

una intangibilidad en su concreción, pero con un claro impacto cuando es afectado. Los efectos generados en el ciberespacio pueden tener impactos dentro de la dimensión física que ello implica.

En relación con lo anterior, el ciberespacio fue declarado por *The Economist* y las principales potencias mundiales como el quinto dominio después de la tierra, el mar, el aire y el espacio, debido a que durante la primera década del siglo XXI aparecieron nuevos paradigmas de ataque por medio del ciberespacio, los que basados en diferentes motivaciones individuales o colectivas, intentaban afectar a las instituciones, gobiernos y diversas corporaciones empresariales. Lo expresado es ratificado por Clarke, R. y R. Knake (Guerra en la red. Los nuevos campos de batalla, Ariel, 2010) al señalar que: *"el ciberespacio es una zona de guerra donde muchas de las batallas del siglo XXI se van a dar"*, aportando una visualización del ciberespacio como el lugar virtual donde surgirán acciones de amplia variedad y en donde se luchará por ejercer la protección de las redes informáticas.

De igual forma, el CEEAG, en síntesis, establece que el ciberespacio es la expresión de un espacio virtual y vital para que exista la transmisión de la información, razón por lo que se desarrollarán sucesivas acciones de amplia variedad para ejercer el control y la protección de las redes informáticas, originando por consecuencia la necesidad de asegurar el funcionamiento de estos sistemas frente a diversas amenazas.

Es por lo anterior que, en Lineamientos de Política para ciberseguridad y ciberdefensa, Consejo Nacional de Política Económica y Social, elaborados por el Departamento Nacional de Planeación, República de Colombia, la ciberseguridad puede ser definida como la *capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética*.

Ahora bien, en razón a la respuesta entregada el 04 cuatro de junio del año 2019 dos mil diecinueve, a la solicitud de información presentada ante el INAI, a la cual le correspondió el número de folio 0673800104519, nos hemos dado cuenta de los controles que cubren las áreas en materia de seguridad; del uso de herramientas de propósito específico tanto en el perímetro de comunicaciones del INAI como en los puntos finales como son *Firewall*, IPS, Antivirus, WAF, para protección de la tecnología que contiene el SIPOT.

Asimismo, el SIPOT permite descartar archivos que no cumplen con ciertas características válidas que debe cumplir un archivo para ser cargado en el SIPOT lo cual disminuye riesgos de cargar programas dañinos. Adicional a esto, la infraestructura del sistema, cuenta con capas de seguridad robustas, desde el perímetro hasta los equipos (*endpoints*).

De igual forma, las intrusiones no autorizadas al SIPOT que pudieran extraer información, alterarla, borrarla, encriptarla, etc, tales como el *hackeo*, se previene mediante mecanismos de detección y prevención de amenazas avanzadas, así como la protección de seguridad perimetral y seguridad a nivel equipo (*endpoint*).

Aunado a lo anterior, las medidas de resiliencia implementadas en el SIPOT son una alta disponibilidad en los servicios tanto de comunicación como de infraestructura utilizados en los sistemas.

Sin embargo, a pesar de todas las medidas y prevenciones tomadas por el INAI el SIPOT ha sufrido en tan solo diez meses 77,927 ataques cibernéticos, desglosado de agosto a diciembre de 2018 y de enero a mayo de 2019, con 13,863 y 64064 ciberataques respectivamente. Viéndose entre cinco meses de un año y cinco meses de otro un incremento de 362.12%; pero la interrogante sería ¿seguiremos esperando que la cantidad de ataques aumente?, simularemos que no es nuestra responsabilidad, o cambiaremos la mentalidad en buscar una solución a lo antes vertido.

Cabe hacer mención que la responsabilidad no solo le corresponde al INAI por ser el administrador de la PNT junto con sus sistemas entre ellos el SIPOT; sino también a los organismos garantes del país.

El presente artículo es un tema poco explorado, el cual puede utilizarse en futuras investigaciones y servir de base para mejorar la seguridad que contiene la PNT en específico el SIPOT y poder obtener ciertos patrones de ataques.

Propuesta para modificar el estado de las cosas

Por lo antes expuesto, considero que no debemos de ser indiferentes ante el problema planteado, sino buscar soluciones. Es por ello que se propone que no solo el INAI, sino todos los organismos garantes del país y ciertos sujetos obligados de las diversas entidades federativas, que cuenten con los recursos idóneos, realicen la contratación de un servicio de *pentesting*, y éste sea específico y defina la manera idónea de tal suerte que no exista ninguna duda del servicio contratado, entre los temas que se pueden contemplar en la elaboración del contrato, las autorizaciones; la información que estará disponible; la técnica que se utilizara para la intrusión; el tratamiento de la información que se pueda obtener.

María del Rosario Navarro Zamora

Es licenciada en Derecho por la Universidad Michoacana de San Nicolás de Hidalgo, Maestra en Derecho Constitucional y Amparo por el Institutito de Formación e Investigaciones Jurídicas de Michoacán y Especialista en Gestión, Publicación y Protección de Información, por el Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales; cuenta con diversos diplomados en transparencia, protección de datos personales, sistemas anticorrupción, gobierno abierto, gestión documental y seguridad de la información. Actualmente, labora en la Coordinación General de Evaluación y Gestión Documental del ITEI.

Referencias y/o fuentes de consulta

Ley General de Transparencia y Acceso a la Información Pública, Diario Oficial de la Federación, 04 de mayo de 2015.

Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban loa Lineamientos para la implementación y operación de la Plataforma Nacional de Transparencia, Diario Oficial de la Federación, 04 de mayo de 2016.

Respuesta entregada el 04 de junio de 2019, a la solicitud de información presentada ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a la cual le correspondió el número de folio 0673800104519.

Respuesta entregada el 17 de mayo de 2019, a la solicitud de información presentada ante la Auditoría Superior de la Federación, a la cual le correspondió el número de folio 0110000043319.

INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. 29/07/2019, de Instituto Nacional de Ciberseguridad Sitio web: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Centro de Estudios Estratégicos CEEAG. (2018). *La Ciberguerra: Sus impactos y desafíos.* Chile: Comité Editorial del CEEAG.

Calvente Arturo M. *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales.

Cano, Jeimy J. *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global*, Sistemas (Asociación Colombiana de Ingenieros de Sistemas), vol. 000, Nº 0119 (abr-jun. 2011).

Hoecker Marcos Robledo. Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre Ciberseguridad, PNCS 2017.

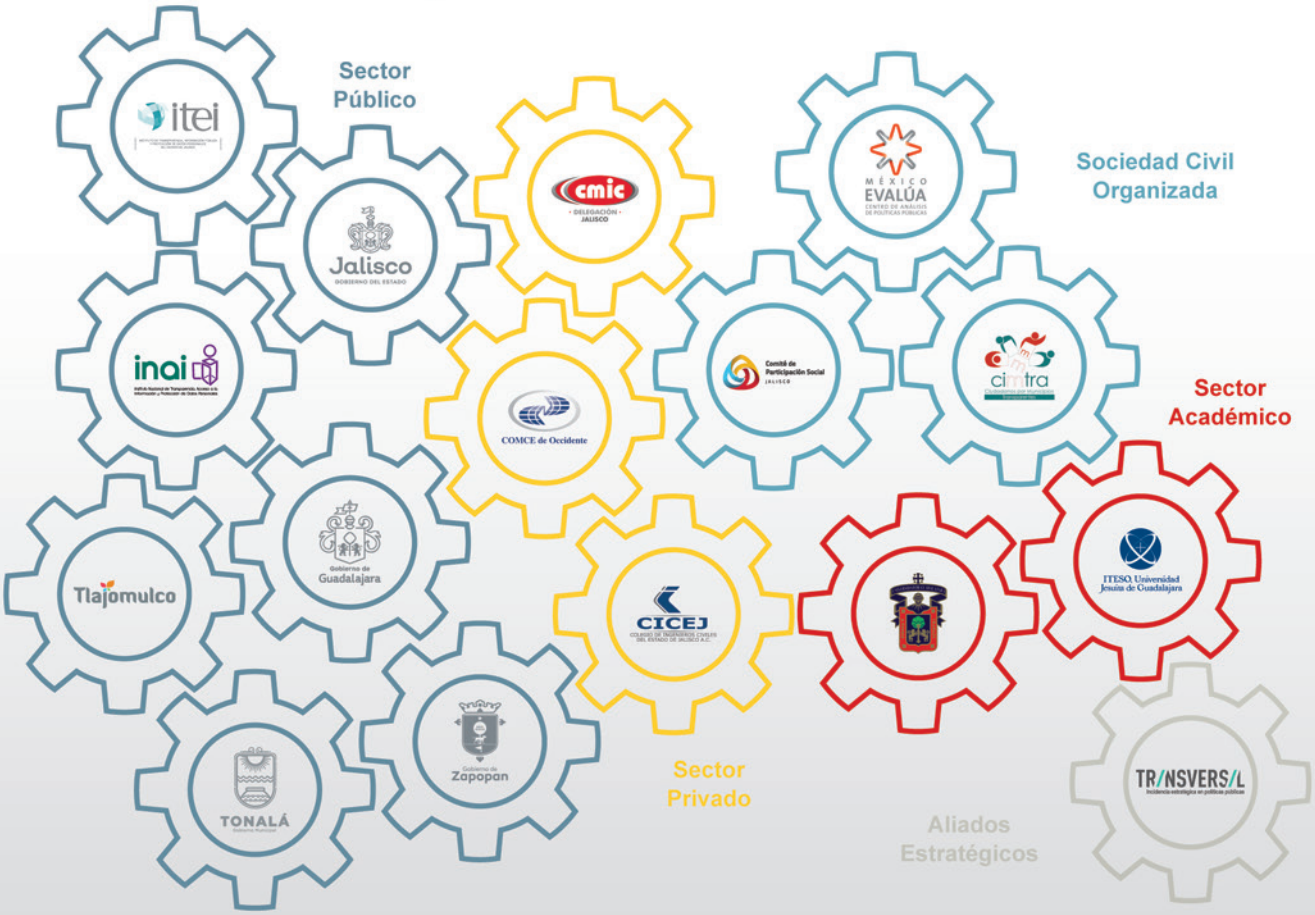
Unión Internacional de Telecomunicaciones, referida en Alejandro Gómez Abutridy, “Ciberseguridad y Ciberdefensa, Dos elementos de la Ciberguerra”, *Memorial del Ejército de Chile*, Nº 492, agosto 2014.

CoST Jalisco

La Iniciativa Internacional de Transparencia en Infraestructura o "CoST" por sus siglas en inglés, es la encargada de promover la transparencia y la rendición de cuentas dentro de las diferentes etapas de los proyectos de infraestructura y obra pública.

Con su implementación en el estado de Jalisco, coordinada por el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, se pretende mejorar la transparencia en los procesos de infraestructura y obra pública, exigiendo la publicación de información que contenga datos claves de todo el ciclo del proyecto (identificación, preparación, contratación, ejecución y evaluación) a través de herramientas tecnológicas basadas en plataformas de información focalizadas que servirán como medio de divulgación.

La iniciativa de CoST en Jalisco está liderada por el Grupo Multisectorial, quien es el responsable de guiar el desarrollo, la implementación y supervisión de la iniciativa en el estado.



Para conocer más de esta iniciativa visita

www.itei.org.mx/cost

Síguenos en @CostJalisco

Fotografía: Peshkov para Adobe Stock

Robo de datos personales a través de ciberdelitos en jalisco

Luis Abraham Rincón Prieto
Coordinador de Archivos del Consejo Municipal del Deporte de Zapopan, Jalisco

Resumen

En este artículo se expone el avance que Jalisco ha obtenido en el tema de las tecnologías de la información y las comunicaciones, así como en tecnología e innovación. Consecuentemente los habitantes de Jalisco haciendo uso de las herramientas tecnológicas y del internet, han creado hábitos de conexión de 24 horas al día.

Los ciudadanos Jaliscienses por falta de capacitación respecto a prevenir los ciberdelitos, y la omisión de una normatividad severa para castigar a los practicantes ciberdelincuentes, hace que sean víctimas de robo de datos personales. Siendo vulnerables en redes sociales, aplicaciones, plataformas digitales, wifi o dispositivos con sensores de monitoreo.

Los Jaliscienses en sus roles de vida interactúan con dispositivos electrónicos que cuentan con sensores que lo monitorean todo y almacenan grandes cantidades de datos personales. Se trate de un reloj (SmartWatch), celular o una bocina inteligente que en muchas ocasiones los conectan con plataformas digitales para realizar diversos servicios como: solicitar transporte; un trámite ante el gobierno; realizar pagos; comprar productos para el hogar; dar mayor productividad en el trabajo o simplemente por entretenimiento, lo que hace que sean más vulnerables en el ciberespacio.

Los ciberdelitos más comunes que se dan en Jalisco son: ciberacoso o ciberbullyng, suplantación de identidad o robo de identidad, cibergrooming o groooming, sexting o packs, ransomware, phishing.

Es necesario que la legislación estatal de Jalisco evolucione y de alcance a regular las tecnologías de comunicación y de la información, y el avance tecnológico e innovador. En especial que regule las redes sociales, aplicaciones, plataformas digitales, wifi o dispositivos con sensores de monitoreo (Internet de las Cosas).

PALABRAS CLAVES:
Ciberdelincuente, Ciberdelitos, Datos Personales, Ciberresilencia, Ciberespacio, Internet de las Cosas

Introducción

En el constante avance de la materia de transparencia y protección de datos personales, nuestros legisladores han emitido reformas a nuestro ordenamiento, me refiero a la Constitución Política de los Estados Unidos Mexicanos en sus artículos 6º y 16, y han emitido Leyes Generales reglamentarias de dichos preceptos constitucionales, para garantizar los derechos humanos de Transparencia y Acceso a la Información Pública, y a la Protección de Datos Personales. Sin embargo, la tecnología e invocación al paso del tiempo ha influido considerablemente en la vida de los mexicanos, facilitando la conexión a internet a través de dispositivos electrónicos inteligentes, que están equipados con aplicaciones y sensores. Logrando ingresar a un ciberespacio que es nutrido cada día con grandes cantidades de información, incluyendo datos personales que se comparten en redes sociales; al momento de descargar aplicaciones; al realizar compras con dispositivos inteligentes con sensores y que se conectan a las redes wifi.

Ciberespacio donde los ciudadanos mexicanos como internautas intercambian y comparten información con libertad y rapidez, y mayor aun con un plus el anonimato. Anonimato que motiva a que se realice un mal uso de la fuente ilimitada de información contenida en el ciberespacio y llamando la atención a los practicantes de ciberdelitos para obtener datos personales y con ello tener beneficios. Derivado de lo anterior, se analizarán estudios del uso del internet en México, así como de Jalisco para determinar que avance han tenido en la tecnología de la información y las comunicaciones, así como se investigará cuáles son las principales redes sociales utilizadas, y que tipos de datos personales recopilan. Incluso se investigará el internet de las cosas y su forma de captar datos personales a través de sensores de monitoreo y qué tipo de ciberdelitos son las más comunes en Jalisco.

La falta de regulación jurídica respecto a las redes sociales, el internet de las cosas e incluso de las wifi públicas y los sitios web falsos como medios por los cuales con consentimiento y sin verificar la seguridad se conectan los usuarios, para compartir información e incluso datos personales, hacen vulnerables a los ciudadanos Jaliscienses.

Surge la necesidad de conocer las definiciones de ciberdelitos cometidos en Jalisco, y su tipificación en el Código Penal para el Estado Libre y Soberano de Jalisco; y conocer algunas recomendaciones de cómo prevenirlos. De aplicar cuestionarios a menores para adquirir qué tanto conocimiento se tiene del tema de ciberseguridad y ciberdelitos, para acreditar la necesidad de crear conciencia de capacitarse en dichos temas, y a su vez se analizará un estudio de hábitos de los usuarios en ciberseguridad.

Finalmente, se emitirán conclusiones para mejorar la problemática encontrada como propuestas, y se genere concientización respecto al uso de internet y sus consecuencias de compartir datos personales en redes sociales; al momento de descargar aplicaciones; al realizar compras con dispositivos inteligentes con sensores y que se conectan a las redes wifi. Proponiendo se emita una Ley de Ciberseguridad y Ciberdelitos en el Estado de Jalisco, y el contenido que podría integrarla.

Desarrollo

México ha tenido un considerable avance respecto a hábitos de uso de internet tal y como se advierte a continuación: 1.- Aumento del 82.7% al 2018 respecto a los usuarios de internet; 2.- El perfil del internauta mexicano es 51% femenino y 49% masculino; 3.- Respecto a la edad el mayor porcentaje es de 25 a 34 años; 4.- El 67% de los internautas en México, perciben que se encuentran conectados en internet las 24 horas; 5.- El 84% de los usuarios se conectan en su hogar; 6.- Las redes sociales son la mayor actividad en línea teniendo un 82%, siendo la principal el facebook; 7.- El 41% de los usuarios de internet solicitan transporte, esto por mayor comodidad y seguridad; y El smartphone es el principal dispositivo para acceder a alguna red social.[1]

Ahora bien en Jalisco, una de las obligaciones del Estado, es garantizar y promover el acceso a la sociedad de la información y economía del conocimiento, mediante el uso y aprovechamiento de las tecnologías de comunicación y de la información. Así como se reconozca, entre otros derechos el de acceso a la tecnología e innovación, con el objetivo de elevar el nivel de vida de los habitantes jaliscienses (Constitución Política del Estado de Jalisco, 2019, art. 4).

Debido al importante avance tecnológico de comunicaciones y de información que ha tenido el Estado de Jalisco, el 70,4 % de los habitantes de Jalisco disponen de conexión a internet en sus hogares. De acuerdo a la Encuesta Nacional realizada por el INEGI respecto a hogares que disponen de conexión a internet por ciudad seleccionada.[2]

La edad de los usuarios de internet en Jalisco media de entre los 6 años a 55 años o más, destacando los usuarios de 25 a 34 años de edad con mayor conexión. Según se advierte de la Encuesta Nacional realizada por el INEGI respecto a usuarios de internet por entidad federativa, según grupos de edad, 2018.[3]

Jalisco ha buscado impulsar la competitividad, y productividad de las PYMES, a través de iniciativas como La Estrategia Estatal de Internet of Things[4], cuyo objetivo es:

> *Desarrollar, fomentar y acelerar en Jalisco, la integración de una plataforma tecnológica de IoT, especializada en innovación de aplicaciones productivas con la colaboración de las empresas globales de IoT, empresas locales tecnológicas, universidades y centros de investigación y desarrollo. La estrategia está impulsada por la Secretaria de Innovación, Ciencia y Tecnología del Estado, a través del Centro de Innovación y Aceleramiento para el Desarrollo Económico (CIADE), el cual ha definido como sectores estratégicos al sector Agroalimentario, Salud y Farma, TIC's e Industrias creativas y Biotecnología en donde a través de Internet of Things se buscará potencializar dichos sectores buscando su innovación y la creación de productos que puedan competir a nivel global (Díaz, 2014).*

En el Estado de Jalisco se encuentra la Ciudad Creativa digital, y ha realizado eventos tan importantes como Talent Land 2019, por lo que siempre los jaliscienses están a la vanguardia de la tecnología.

Sin embargo, el hábito cotidiano que tienen tan arraigado los Jaliscienses de la adicción a la conexión de 24 horas a redes sociales como el facebook, así como chatear mediante WhatsApp y Telegram desde su smartphone o teléfono inteligente para compartir en el ciberespacio imágenes, videos, archivo de sonido e incluso videollamadas, los involucra en riesgos

1 Asociación de Internet. MX. 15º Estudio sobre los Hábitos de los Usuarios de Internet en México 2019. Mayo, 13, 2019. Recuperado de: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/15-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2019-version-publica/lang,es-es/?Itemid=

2 INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares. (ENDUTIH),2018. Recuperado de: https://www.inegi.org.mx/temas/ticshogares/default.html#Tabulados.

3 INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares. (ENDUTIH),2018. Recuperado de: https://www.inegi.org.mx/temas/ticshogares/default.html#Tabulados.

4 Internet de las Cosas.

como perdida de datos personales[5], por desconocimiento de aspectos importantes como: la privacidad en las comunicaciones, por riesgo de suplantación, y no realizan una simple comparación de dichos aspectos. Se analizaron las redes sociales de WhatsApp y Telegram, para determinar qué red social es más vulnerable para que le roben los datos personales:

> *WhatsApp cuenta con 450 millones de usuarios. También destaca por su facilidad de uso, con un diseño simple y fácil de utilizar. En cuanto a seguridad ha ido mejorando, se puede configurar información privada, como hora de conexión, el estado o foto de perfil. Sin embargo, las comunicaciones, que ya van cifradas siguen siendo un punto débil. Su mayor problema relacionado con la seguridad es la facilidad con la que se puede suplantar la identidad de otra persona, debido al sistema que utiliza la aplicación para identificarnos. Pues para conectarte e iniciar sesión WhatsApp sólo necesita un número de teléfono y la dirección MAC (iPhone) o el IMEI (Android), logrando que alguien se haga pasar por nosotros (Oficina de Seguridad del Internauta, 2019).*

> *Telegram cuenta con el número más bajo de usuarios. Es idéntica a WhatsApp. En cuanto a seguridad cuenta con un cifrado calificado de "indescifrable". Y puede utilizar un chat secreto. El código de Telegram es abierto y libre. (Oficina de Seguridad del Internauta, 2019).*

Se determina de las anteriores citas, que WhatsApp es más vulnerable porque se puede suplir la identidad de sus usuarios, sin olvidar que solicita el número de smartphone, así como los demás contactos de la libreta de direcciones y por el contrario Telegram cuenta con más seguridad tiene sistema robusto de cifrado de comunicaciones, tiene chat secreto y es de código libre y abierto.

Consejos para prevenir robo de datos personales, mediante mensajería instantánea:

- No difundir el número de teléfono móvil de otras personas sin su consentimiento.
- Instalar un antivirus en el dispositivo (PC, tableta, smartphone) donde se utilice la aplicación de mensajería instantánea.
- Asegurar de que la persona con la que se comunica es quien dice ser. No caer en engaños.
- Establecer una contraseña de bloqueo en el dispositivo.
- Revisar siempre los ficheros que se descarguen. Tener cuidado de no difundir contenido ilegal.
- No facilitar información privada.
- Eliminar el historial de las conversaciones con frecuencia. De esta forma se evitara que, si alguien accede al dispositivo de manera no autorizada, pueda leerlas y obtener información del usuario que no desea.
- Tener cuidado con las redes WiFi a las que se conectan para chatear. Si no están debidamente protegidas o son redes públicas, una persona malintencionada conectada a la misma red podría capturar las conversaciones y descifrarlas.
- Actualizar la aplicación siempre que aparezca una nueva versión por si ésta, además de incorporar alguna nueva funcionalidad, corrigiese algún fallo de seguridad.
- No olvidar leer la política de privacidad y las condiciones del servicio antes de usarlo.
- Si la aplicación de mensajería instantánea que usas ofrece alguna opción de chat secreto, acostumbrarse a utilizarla (Oficina de Seguridad del Internauta, 2019).

Se analizó la aplicación más comúnmente utilizada en el ámbito del internet en Jalisco, siendo el facebook, al momento de descargarla y para efectos de realizar el registro y gozar del servicio de dicha red social, solicita entre otros datos personales: correo electrónico,

5 Debe recordarse que los datos personales son toda aquella información concerniente a una persona física identificada o identificable.

número de teléfono smartphone y una vez registrado puedes agregar más datos personales como: empleo, formación académica, lugares donde viviste, información de contacto, si eres hombre o mujer, fecha de nacimiento, apodo, situ ación sentimental, gustos, a quien decides seguir dentro del servicio de dicha red social, eventos agendados, además puedes agregar, fotos y videos, estado de ánimo. Pero este es el inicio de compartir datos personales porque muchas de las veces los usuarios publican, eventos a los que asisten sean estos familiares o sociales, fotos intimas, lugares que visitan con frecuencia, su ubicación en tiempo real[6], sus riquezas, videos, tipo de religión, los nombres de sus familiares, en pocas palabras hasta el tipo de sangre.

> *Facebook es la red social que más controversia genera en sus condiciones de uso. Principalmente deja claro en sus términos de uso que todo lo que se suba a su red social (fotos, videos, estados, información) pasa a ser de su propiedad. De hecho, si se sube una foto, y se quiere borrar, la puedes deshabilitar, para que no sea accesible desde el muro, pero queda en sus servidores. (Internauta, Instituto Nacional de Ciberseguridad de España M.P., S.A. , 2015).*

De la anterior cita, se advierte que la información incluyendo datos personales, no se eliminan inmediatamente de los servidores de Facebook. Las condiciones de servicio de Facebook, en la sección denominada “Permisos que se Conceden”, claramente explican que aun eliminando el contenido de la cuenta puede seguir existiendo en parte de sus sistemas hasta por 90 días[7].

También muchas de las veces entre aplicaciones se comparten información, como el caso de whatsapp que trabaja con la empresa de facebook. En ocasiones los datos personales son utilizados para venderlos con fines de mercadotecnia y otras veces se venden en el mercado negro para cometer delitos de extorción o fraudes. “Lo que quiere decir que manipulan, venden y comparten información en las aplicaciones más utilizadas”. (Aguilar., 2017). Como se advierte los usuarios son proveedores de datos personales para dichas aplicaciones y lo peor muchas de las veces otorgan su consentimiento, por no leer los términos y condiciones para hacer uso de los servicios, con tan solo dar un click.

Aquí no termina el tema de las aplicaciones pues algunas dan las opciones de configurar la privacidad[8] del usuario, pero al no realizar la configuración por falta de interés o desconocimiento quedamos vulnerables a ciberdelitos.

> *En 2018, la ENDUTIH indica que 45.5 millones de los usuarios de Internet mediante celular inteligente (Smartphone) instalaron aplicaciones en sus teléfonos. De estos, el 89.5% instaló mensajería instantánea, el 81.2% para acceder a redes sociales y el 71.9% instaló aplicaciones para acceder a contenidos de audio y video. Por otra parte, el 18.1% de los usuarios utilizaron su dispositivo para instalar alguna aplicación que les permitiera acceder a la banca móvil (Social, 2019).*

6 39% pública su ubicación en redes sociales.

7 Información Legal de WhatsApp. 2019. Recuperado de: https://www.whatsapp.com/legal/#terms-of-service

8 El Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales. Emitió Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital. Recuperado en: http://inicio.inai.org.mx/Guias/5RecomendacionesPDP_Web.pdf

Otra manera mediante la cual los Jaliscienses proporcionan datos personales son mediante dispositivos con sensores de monitoreo y aplicaciones, que están conectados a internet. Que gracias a la gran cantidad de información que almacenan de sus usuarios, una vez analizada, son capaces de detección de objetos, transmitir, tomar decisiones y actuar. Este tipo de dispositivos los utilizan el 29% de los usuarios.[9] Es lo que se llama Internet de las Cosas (IoT), una definición es:

> *Tecnología basada en la conexión de objetos cotidianos a internet que intercambian, agregan y procesan información del entorno físico para proporcionar servicios de valor añadido a los usuarios finales. También reconoce eventos o cambios, y tales sistemas pueden reaccionar de forma autónoma y adecuada. Su finalidad es, por tanto, brindar una infraestructura que supere la barrera entre los objetos en el mundo físico y su representación en los sistemas de información (Andrés, 2018).*

Esta nueva forma de conexión cambiará totalmente la forma en que vivimos, la comunicación y revolucionará el mercado, la educación, la salud. Pues la interoperabilidad entre dispositivos inteligentes se impulsará, en consecuencia se captará mayor información, que se utiliza para optimizar procesos y análisis de datos, será de gran beneficio para la sociedad, por lo que se está ante otra etapa de la revolución industrial. “La Cuarta Revolución Industrial es el Internet de las Cosas (IoT, por sus siglas en inglés)”, (Schwab, 2016).

Entre los dispositivos inteligentes de este tipo, los más comúnmente usados son los wearables[10] como las pulseras inteligentes, los smartwatches, los smart rings. Que guardan información personal como monitoreo de actividad física, calorías quemadas, ritmo cardiaco, pulso, temperatura, movimientos, niveles de glucosa, presión arterial, nivel de estrés, detección de deshidratación, preferencias en televisión. Dicha información es almacenada en servidores de la compañía creadora del artículo o captada por aplicaciones como la fitbit para almacenarla en el smartphone.

Así para gozar del servicio que brinda fitbit, solicita datos personales como: su nombre, dirección de correo electrónico, contraseña, fecha de nacimiento, sexo, altura, peso y, en algunos casos, su número de teléfono móvil, rol de alimentación, el peso, los hábitos de sueño. Y si se permite realizar pagos y efectuar transacciones, se debe proporcionar como: número de tarjeta de crédito, débito, fecha de vencimiento de las tarjetas y código CVV[11].

Esto además de que puede conectar con servicios de terceros como facebook de donde obtiene datos como: nombre, dirección email y lista de amigos. Claro está que para poder hacer uso de estos servicios las compañías siempre solicitan el consentimiento de los usuarios, el cual viene en los términos y condiciones que la mayoría de usuarios no lee[12]. No se revisa la política de privacidad. No se configura correctamente para estar protegidos, o se vende el teléfono inteligente sin antes borrar los datos personales, nuevamente son vulnerables a ser víctimas de ciberdelitos.

> *Los fabricantes utilizan tecnología Bluetooth de baja energía para permitir al wearable sincronizarse de forma inalámbrica a un smartphone lo que puede provocar que éste pueda ser monitorizado o rastreado sin necesidad de tener muchos conocimientos técnicos. ¿Riesgos? Por poner un ejemplo, un simple ladrón podría*

9 Asociación de Internet. MX. 15º Estudio sobre los Hábitos de los Usuarios de Internet en México 2019. Mayo, 13, 2019. Recuperado de: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/15-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2019-version-publica/lang,es-es/?Itemid=

10 Wearables es el conjunto de aparatos y dispositivos electrónicos que se incorporan a alguna parte de nuestro cuerpo interactuado de forma continua y con otros dispositivos con la finalidad de realizar alguna función concreta.

11 El Código CVV es un grupo de 3 o 4 números situado en el reverso de la tarjeta de crédito. Recuperado de: https://www.bbva.com/es/que-es-el-ccv-o-cvc-en-las-tarjetas-de-credito/

12 Estudio Hábitos de los usuarios en ciberseguridad en México 2019. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf pag. 14. Donde el 42.05 indicó que no revisa el contenido de los permisos requeridos antes de instalar aplicaciones.

saber perfectamente dónde se encuentra una persona para decidir cuál es el mejor momento para entrar a robar a su casa. También hay vulnerabilidades en los sistemas de almacenamiento relacionados con las contraseñas. Se ha visto que en algunos se transmite en claro (sin utilizar ningún tipo de cifrado) y que la gestión de usuarios es deficiente. ¿Riesgos? Si alguien consigue esa contraseña, accederá a nuestra información privada, entre la que se encuentra, ¡datos médicos relacionados con nuestra salud! En algunos casos, se detecta la ausencia de políticas de privacidad que expliquen de forma clara y sencilla para qué se recogen los datos de los usuarios y qué hacen con ellos. En otros, aunque sí que existen, no están del todo accesibles. ¿Riesgo? Tus datos podrían ser "cedidos" a empresas de terceros. ¿Qué pasa si fuese a una aseguradora médica? Quién sabe, igual podría subir el precio de la póliza contratada de una persona, si gracias a una smartband sabe que practica mucho deporte y tiene más riesgos de sufrir un accidente… Al margen del estudio, tampoco debemos olvidarnos de que los servidores que almacenan todos los datos que voluntariamente facilitamos a las empresas a través de sus wearables, pueden ser objetivo de ataques. Si están correctamente configurados y protegidos, no debería suponernos ningún riesgo de seguridad, pero, ¿qué pasa si encuentran un agujero de seguridad en los sistemas y consiguen acceder a nuestros datos? Eso igual ya no nos hace tanta gracia… (Internauta, Instituto Nacional de Ciberseguridad de España M.P., S.A. , 2015)

Los ciberdelincuentes, que ya han obtenido el número de tarjeta por otros medios, intentan hacerse con el código CVV usando distintos métodos, como correos electrónicos falsos o incluso llamadas de teléfono, haciéndose pasar por la entidad emisora de la tarjeta, por ejemplo (OCU Ediciones, 2009).

En México cada día es más común observar estos tipos de pulseras inteligentes más en el ámbito deportivo. México es ubicado en la posición 18 de los 24 países considerados, con 6.8 dispositivos (IoT) por cada 100 habitantes, donde el 43% de los mexicanos están interesados en controlar dispositivos a través de smartphone, como objetos relacionados con la salud como pulseras y sensores. (Gobierno de México, 2019)

Otros dispositivos son las bocinas inteligentes capaces de reconocer las características físicas del lugar en el que está ubicado, como la marca Apple que funciona con "Siri" lo que da comodidad a sus usuarios pues puede leer mensajes, hacer y contestar llamadas. (SUN, 2018)

Al igual que la bocina inteligente que funciona con "Alexa" capaz de reconocer la voz de los usuarios, controlar diversos dispositivos de la casa como focos, ventiladores, cerradura, cámaras, el refrigerador, el televisor inteligente. (Mariana R. Fomperosa, 2018)

Estos dispositivos con sensores de monitoreo almacenan gran cantidad de datos personales[13], ya que del análisis que realizan a los mismos, van conociendo nuestra voz, nuestros gustos, nuestra agenda diaria, nuestras ubicaciones, nuestros destinos. La justificación de las compañías en general es para rendir un mejor servicio personalizado al usuario.

Estos tipos de altavoces pueden ser hackeados a través del router, que es la puerta de entrada a toda tu red doméstica. Si el pirata informático entra en el router, él o ella pueden comprometer potencialmente cada computadora y dispositivo conectado a la red. Y si alguno de esos dispositivos además del altavoz

[13] Big data. Recuperado de: https://www.webopedia.com/TERM/B/big_data.html

inteligente tiene capacidades de audio, el hacker[14] puede hacer que el dispositivo emita comandos para el altavoz inteligente, por ejemplo, para que desbloquee la puerta delantera o abra el garaje. Antes de que te des cuenta, todos tus pequeños dispositivos se comunican entre sí como un ejército de traidores (Avast, 2018).

Hoy en día es muy común que en los cafés, restaurantes, plazas, tiendas comerciales, hoteles, librerías existan wifi de libre acceso (wifi pública), en las que es muy fácil conectarse.

> *La mayor amenaza para la seguridad de las redes Wi-Fi gratuitas es la capacidad que tiene el hacker de interponerse entre ti y el punto de conexión. Por lo tanto, en lugar de hablar directamente con el punto de acceso, envías tu información al hacker, quien luego vuelve a transmitirla (Kaspersky, 2019).*

También es muy común que desde la laptop al estar realizando investigaciones se entre a sitios webs y una vez que se da click, nos aparece una ventanilla que nos indica ingrese por medio de facebook, y se vuelve nuevamente un riesgo para que nos roben datos personales, pues se otorga el consentimiento para que accedan a información. No se realiza el cercioramiento para verificar que en realidad se trate del sitio web que buscamos. No se verifica que se trate de un formulario que utilice un ciberdelincuente. Se esta tan acostumbrado a dar click y click que se es víctima de sitios webs falsos.[15]

La realidad es que se otorgue o no consentimiento en el ciberespacio[16] nuestros datos personales son oro molido para el practicante ciberdelincuente, experto en acceder de forma no autorizada a sistemas informáticos sean privados o del Estado que formen parte de una laptop, teléfono inteligente, smartphone, pulseras inteligentes, entre otros dispositivos electrónicos, con el objetivo de apoderarse de datos personales a través de ciberdelitos.

A nivel nacional en México en el Código Penal Federal, en sus artículos 211 bis1 al 211 bis 7, tipifican la conducta de acceso ilícito a sistemas y equipos de informática, y establece que se sancionará al que tenga acceso, destruya, conozca o copie la información sin autorización a sistemas particulares o del Estado que cuenten con algún mecanismo de seguridad. Incluyendo la modificación, y los Sistemas Financiero del Estado y las instituciones que forman parte del mismo.

Entre los ataques a Sistemas Informáticos más destacados en México se encuentran el caso del Sistema de Pagos Electrónicos Interbancarios (SPEI), donde se registró en abril y mayo del 2018 un ataque cibernético a los sistemas de conexión al (SPEI), cuyo objetivo fue generar transferencias electrónicas de fondos a cuentas específicas, con el fin de sustraer ilegalmente recursos monetarios. Donde el modus operandi fue: Inserción de operaciones apócrifas, Uso de cuentas beneficiarias válidas y Eliminación de evidencia. Los ataques, utilizaron técnicas comunes como robo de credenciales, escalamiento de privilegios, movimientos laterales entre servidores, inserción de archivos o ejecución de instrucciones y borrado de bitácoras.[17] Al respecto el Banco de México en su carácter de administrador del (SPEI) en su Informe Anual emitido en marzo 2019 informa que: implementó medidas con el objetivo de mitigar los riesgos de materialización de eventos similares a los ocurridos

[14] Ciberdelincuente.

[15] Los virus troyanos pueden atacar los ordenadores de las víctimas y mostrar un cuadro de diálogo o una imagen en los ordenadores de cada usuario. La ventana será una imitación del sitio web del banco del usuario y le solicitará que introduzca su nombre de usuario y contraseña. Recuperado en: https://www.kaspersky.es/resource-center/threats/online-banking-theft

[16] El conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el cual casi todo lo que contiene es información. Término concebido por el escritor William Gibson en su novela de ciencia ficción “Neuromancer” (1984) con el propósito de describir un mundo de redes de información. Recuperado en: https://www.internetglosario.com/90/Ciberespacio.html

[17] Reporte de análisis forenses. Recuperado en: https://www.banxico.org.mx/spei/d/%7B4A977A24-0889-3F24-A717-DF9DBBA118C1%7D.pdf

durante 2018 y reducir las afectaciones a los usuarios de los servicios de transferencias electrónicas, a los participantes del (SPEI), entre los que destacan: Migración de participantes afectados, así como de un perfil de mayor riesgo a una plataforma de operación contingente; Implementación de alertas para detectar anomalías en los mensajes de pagos; Emisión de regulación con el fin de que las entidades que otorgan el servicio de transferencias de fondos implementen medidas de control; Establecimiento de protocolos y procedimientos que documenten las acciones a tomar en caso de que se materialicen riesgos de ciberseguridad; Designación de oficial de seguridad de la información responsable de las políticas de riesgos de ciberseguridad; Implementación de un proceso de autoevaluación. Lo anterior, para solventar las deficiensas de los Sistemas de conexión a (SPEI) y para fortalecer otros Sistemas Financieros.

El ciberdelincuente busca aprovecharse de los fallos de seguridad y sacar un beneficio, es ese hacker negro que busca sacar beneficios, actúa en ocasiones por razones económicas, razones ideológicas o por venganza. El ciberdelincuente tiene amplios conocimientos de seguridad informática, quien utiliza herramientas para llevar a cabo ciberataques (Internauta, Instituto Nacional de Ciberseguridad de España M.P., S.A., 2019)

El ciberdelincuente una vez accediendo a la wifi fácilmente, utiliza herramientas y roba nuestros datos personales, para cometer ciberdelitos o venderlos para su propio beneficio tales como: ciberacoso o ciberbullyng, suplantación de identidad, grooming, sexting, ransomware, phishing. Se analizará cada ciberdelito, su definición, se investigará si hay noticias respecto a esos delitos en Jalisco, se determinará qué datos personales son robados, se determinará si este ciberdelito está contemplado en la legislación estatal, y por último se describirán recomendaciones para evitar cada ciberdelito.

Ciberacoso o ciberbullyng:

> *Acto intencionado, ya sea por parte de un individuo o un grupo, teniendo como fin el dañar o molestar a una persona mediante el uso de tecnologías de la información y la comunicación (TIC) en específico el internet o teléfono celular (Inegi.Org.Mx, 2017).*

Jalisco es el cuarto lugar con más jóvenes de 12 a 19 años que han sido ciberacosados. (Informador Mx, 2019).

El ciberdelincuente roba fotos de desnudos, mensajes íntimos, videos íntimos, descifra contraseñas simples, se hace pasar por menor de edad, solicita datos personales utilizando artimañas.

El ciberacosador puede enviar mensajes a través de redes sociales[18] o correos electrónicos, los cuales en cuestión de minutos llegan a muchos compañeros, con el fin de burlarse o amenazar a su víctima. Las víctimas de ciberacoso se pueden sentir heridas, enojadas, odiadas y con ganas de suicidarse.

En ocasiones la práctica del ciberdelincuente por venganza, crea una identidad digital falsa de su víctima al extremo de hacerla pasar en ocasiones por dama de compañía e inclusive realiza publicaciones de fantasías de su víctima, provocando con ello que la usuaria ponga en riesgo su integridad.

El ciberacoso es un peligro que debemos reconocer, es una realidad que forma parte del mundo digital (Nora Muñiz, 2019).

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Quinto, Capítulo I, que habla de los ultrajes a la moral o a las buenas costumbres e incitación a la prostitución, artículo 135 bis, establece:

> *Quien obtenga de persona mayor de edad, material con contenido erótico sexual y sin su consentimiento lo divulgue original o alterado, se le impondrá una pena de dos*

18 La fábrica de engaños-redes sociales. Recuperado en: https://www.youtube.com/watch?v=i2tSrvLxYbE

a cinco años de prisión. Cuando el ultraje señalado en el párrafo anterior se cometa a través de las tecnologías de la información y la comunicación, se le impondrá al responsable una pena de cuatro a ocho años de prisión. Este delito se perseguirá por querella de la parte ofendida. Se estará a lo previsto en el Código Penal Federal cuando los hechos se adecuen al delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo (Código Penal para el Estado Libre y Soberano de Jalisco, 2019).

Como se advierte del artículo antes citado, prevé cuando se hace uso de las tecnologías de la información y la comunicación. Se considera que este tipo de ciberdelito debe estar en una Ley referente a Ciberseguridad y Ciberdelitos, en el cual se otorgue mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Algunas recomendaciones para evitar el ciberacoso son: Mantener en el caso de los menores de edad la comunicación con sus padres[19], recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, no aceptar invitaciones en redes sociales de desconocidos, mantener cuidado con los datos personales que se suben al internet, en caso de recibir mensajes ofensivos comunicarlo a la autoridad competente,[20] no seguir el juego a los acosadores hay que romper el silencio, configura la privacidad de tus redes sociales[21], descarga antivirus en tu smartphone, computadora, elabora contraseñas robustas, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle que herramientas puede utilizar para su protección.

Suplantación de identidad o robo de identidad:

"El robo de identidad se produce cuando alguien obtiene ilegalmente la información personal de otra persona y la utiliza para cometer fraude o un robo". El tipo de información personal podría ser cualquier cosa, desde datos generales, como tu nombre o dirección, hasta datos más específicos, como los registros de los hospitales, los detalles de la declaración fiscal o la información bancaria. Existen varias maneras habituales de las que se puede cometer el robo de identidad (Karpersky, 2019).

En Jalisco en los últimos días es muy común el robo de identidad en el infonavit[22], víctimas revelan que desconocidos falsificaron su información y pidieron créditos para adquirir viviendas (Informador. Mx, 2019). También es muy común escuchar que han creado un perfil de facebook utilizando tus datos personales. Se aprovecha de la anonimidad que le otorga el ciberespacio.

En Jalisco de acuerdo a un reporte llamado "Roban identidad a Pensiones en Jalisco" realizado por Luis Herrera en Reporte Índigo, informa que los fraudes por suplantación de identidad están desfalcando al Instituto de Pensiones de Jalisco y sus afiliados. Durante el 2019 se han registrado cinco casos y en el pasado sexenio hubo 14, este último dato lo sustenta con un informe que se brindó vía solicitud de transparencia identificada con el folio 04056619.[23] Lo anterior, hace evidente que los practicantes de ciberdelitos cada día roban más datos personales.

19 Prevención del Abuso Infantil. Video Recuperado en: https://www.educacionpas.org/Lobo/Basico/Civismo-Digital/Ciberbullying

20 Policía Cibernética, dependiente de la Fiscalía General de Jalisco.

21 Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

22 Instituto del Fondo Nacional de la Vivienda para los Trabajadores.

23 Roban identidad a Pensiones en Jalisco. Recuperado en: https://www.reporteindigo.com/reporte/roban-identidad-a-pensionados-en-jalisco-fraudes-prestamos-desfalco-infonavit/

El ciberdelincuente vende los datos personales al mejor postor, inclusive en la dark web[24], sitio donde se puede acceder con buscadores de internet especiales y conseguir información ilegal (Netflix, 2017). En ocasiones envían un mensaje de texto para que se visite una página web para robar datos personales, es lo que se denomina Smishing (Condusef, 2019).

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Sexto, Capítulo IV, que habla suplantación de identidad, artículo 143 quáter, establece:

> *Comete el delito de suplantación de identidad quien suplante con fines ilícitos o de lucro, se atribuya la identidad de otra persona por cualquier medio, u otorgue su consentimiento para llevar la suplantación de su identidad, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona. Este delito se sancionará con prisión de tres a ocho años y multa de mil a dos mil veces el valor diario de la Unidad de Medida y Actualización. Serán equiparables al delito de suplantación de identidad y se impondrán las penas establecidas en este artículo:*
>
> *I. Al que por algún uso de medio electrónico, telemático o electrónico obtenga algún lucro indebido para sí o para otro o genere un daño patrimonial a otro, valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;*
>
> *II. Al que transfiera, posea o utilice datos identificativos de otra persona con la intención de cometer, favorecer o intentar cualquier actividad ilícita; o*
>
> *III. Al que asuma, suplante, se apropie o utilice, a través de internet, cualquier sistema informático o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona.*
>
> *Se aumentará hasta en una mitad las penas previstas en el presente artículo, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito; así como en el supuesto en que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico en el rubro de informática, computación o telemática (Código Penal para el Estado Libre y Soberano de Jalisco, 2019).*

Como se advierte del artículo antes citado, prevé en su fracciones I y II ya involucra términos como medio electrónico, telemático o electrónico e internet. Este tipo de ciberdelito debe estar en una Ley referente a Ciberseguridad y Ciberdelitos, en el cual se otorgue mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Para prevenir la suplantación de identidad o robo de identidad: Mantener en el caso de los menores de edad la comunicación con sus padres, recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, no aceptar invitaciones en redes sociales de desconocidos, no dar click a correos que te ofrezcan premios tentadores, en caso de recibirlos hacerlo del conocimiento a la autoridad competente,[25] tener cuidado con los datos personales que se suben al internet, revisa tus estados de cuen-

[24] La web obscura, los sitios ocultos de internet.

[25] Policía Cibernética, dependiente de la Fiscalía General de Jalisco.

tas, configura la privacidad de tus redes sociales[26], descarga antivirus en tu smarphone, computadora, elabora contraseñas robustas, mantén actualizado tu smartphone o computadora, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle qué herramientas puede utilizar para su protección, utilizar las guías emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[27].

La Condusef respecto a este tipo de ciberdelito recomienda: No ingresar nombres de usuario y contraseñas en sitios desconocidos. Evitar compartir información financiera. Utilizar sólo páginas electrónicas que cuenten con certificados de seguridad. En caso de extravío de documentos personales presentar una denuncia ante la autoridad correspondiente. Evitar proporcionar datos personales a encuestadores vía telefónica. Revisar periódicamente tus estados de cuenta para detectar a tiempo cualquier operación irregular.

Cabe destacar que en este artículo del Código Penal para el Estado Libre y Soberano de Jalisco, también contiene la figura del ciberdelito llamado Phishing que es un tipo de fraude mediante el cual hacen pasar por una institución financiera y te envían un mensaje indicándote un error en tu cuenta bancaria, al ingresar tus datos, obtienen tu información confidencial como: números de tus tarjetas de crédito, claves, datos de cuentas bancarias, contraseñas. (Condusef, 2019). El ciberdelincuente realiza llamadas telefónicas o envía correos electrónicos a los usuarios, solicitando datos financieros o datos personales.

Otra forma en la que los ciberdelincuentes roban datos financieros o datos personales, es mediante el ciberdelito Vishing o phishing telefónico, mediante el cual te llaman para comunicarte si tus tarjetas tienen cargos y derivado de ello el usuario proporcione información (Condusef, 2019).

En Jalisco el phishing, vishing, suplantación de identidad son muy comunes en el mes de diciembre, cuando los usuarios realizan compras en el buen fín. (Informador M.X., 2017)

Anteriormente he comentado que los más vulnerables en las redes sociales para que les roben sus datos personales son los menores de edad, son víctimas fáciles en el ciberespacio, tal es el caso que el ciberdelincuente una vez que se empodera de los datos personales los vende a adultos pedófilos que practican el Grooming, en el internet.

Grooming o Cibergrooming:

> *Es el acoso o acercamiento a un menor ejercido por un adulto con fines sexuales. Concretamente, se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor, incluyéndose en este desde el contacto físico hasta las relaciones virtuales y la obtención de pornografía infantil (Inteco, 2019).*

En Jalisco también se dan casos de grooming, pues entre enero y julio de 2018, se sumaron 53 investigaciones por casos de acoso, principalmente en las redes sociales de facebook y whatsapp (Informador Mx, 2018), en las anteriores aplicaciones el ciberdelincuente crea perfiles falsos en caso de facebook o envía mensajes para iniciar una relación con los menores de edad, el objetivo es incitar al menor a participar en actos de naturaleza sexual, solicitándole le envié fotos intimas o videos. Poco a poco el practicante de ciberdelitos va aplicando estrategia para lograr su objetivo. La primera fase seria el sexo virtual y en su caso aplica ciberacoso. La segunda y última fase sería el contacto físico con el menor de edad y logran el abuso infantil.

[26] Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

[27] Guía para prevenir robo de identidad. Recuperado en: http://inicio.inai.org.mx/nuevo/Guia%20Robo%20Identidad.pdf

En el tema que nos ocupa, el ciberdelincuente accede a la red social del menor, roba sus datos personales a través de juegos de aplicaciones como roblox y los vende o utiliza para lograr el grooming.

Cabe destacar que en la mayoría de los casos cambia la conducta del menor a la de víctima, y por la falta de comunicación con sus padres no hace del conocimiento lo que está sufriendo, por lo que es necesario observar al menor porque regularmente cambia sus hábitos respecto al uso de internet pues lo hará a escondidas, perderá el interés por el estudio, tal vez hasta pérdida de apetito, manifestará cambios de humor, manifestará miedos, problemas de salud.

En virtud de que en este ciberdelito el objetivo principal son los menores, la Fundación de la Prevención del Abuso Infantil, en su sección de civismo digital, da a conocer un video dirigido a menores para que conozcan más sobre el grooming.[28]

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Quinto bis, Capítulo I, que habla de Corrupción de Menores, artículo 142-A, establece:

> *Se impondrá de tres a seis años de prisión y multa de cien a doscientas veces el valor diario de la Unidad de Medida y Actualización a la persona que facilite, provoque, induzca o promueva en persona menor de edad o con quien no tenga capacidad para comprender el significado del hecho:*
>
> *I. El hábito de la mendicidad;*
>
> *II. El hábito de consumir alcohol, drogas o sustancias similares;*
>
> *III. La iniciación o práctica de la actividad sexual, la realización de actividades sexuales explícitas, actos con connotación sexual, el envío de imágenes o sonidos de sí misma con contenido sexual o a la aceptación de un encuentro sexual, o*
>
> *IV. La comisión de cualquier delito.*
>
> *Cuando se trate de los actos mencionados y el sujeto activo del delito empleare cualquier tipo de violencia, o se valiese de alguna situación de mando, poder, función pública o autoridad que tuviere, la pena será de cuatro a siete años de prisión y multa de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización.*
>
> *Cuando el acto de corrupción se realice a través de las tecnologías de la información y la comunicación, al responsable se le impondrá de seis a doce años de prisión y multa de doscientos cincuenta a quinientos cincuenta veces el valor diario de la Unidad de Medida y Actualización, sin perjuicio de las penas correspondientes a los demás delitos que en su caso se cometan.*
>
> *Se aumentará en una cuarta parte de la pena que corresponda, cuando la víctima u ofendido de los delitos de este capítulo, sea persona menor de doce años.*
>
> *Cuando la corrupción de la víctima conlleve un beneficio económico para el corruptor se estará a lo previsto en la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos.*

[28] Prevención del Abuso Infantil. Video Recuperado en: https://www.educacionpas.org/Lobo/Intermedio/Civismo-Digital/Grooming

Como se advierte del artículo antes citado, prevé cuando se hace uso de las tecnologías de la información y la comunicación. Ciberdelito que debe estar contemplado en una Ley referente a Ciberseguridad y Ciberdelitos, en el cual se otorgue mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Para evitar el grooming son: mantener en el caso de los menores de edad la comunicación con sus padres[29], recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, no aceptar invitaciones en redes sociales de desconocidos, tener cuidado con los datos personales que se suben al internet en especial con las fotos y videos íntimos, configura la privacidad de tus redes sociales[30], descarga antivirus en tu smarphone, computadora, elabora contraseñas robustas, mantén actualizado tu smartphone o computadora, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle que herramientas puede utilizar para su protección.

Sexting definiciones:

> *Es un término tomado del inglés que une sex (sexo) y texting (envió de mensajes de texto vía SMS desde teléfonos móviles. El término sexting es un nuevo concepto que significa, recibir, enviar, o reenviar mensajes de texto, imágenes o fotografías, que presentan un contenido sexual explícito, vía internet o teléfono celular (Martínez, 2017).*

> *Práctica de riesgo, sobre todo cuando implica a los menores de edad. Mediante el sexting, se envían a través del teléfono móvil u otro dispositivo con cámara, fotografías o vídeos producidos por uno mismo con connotación sexual. El riesgo está en que una vez enviados estos contenidos, pueden ser utilizados de forma dañina por los demás (Is4k, 2019).*

En Jalisco en la mayoría de las escuelas primarias, secundarias, preparatorias e incluso en centros universitarios está presente el ciberdelito de sexting o mejor conocido como packs, pues incluso los usuarios de internet practicantes de esta conducta, forma sus propios grupos en las redes sociales (Informador Mx, 2018), en principio los usuarios los hacen por juego, satisfacción o simplemente para sentirse que son parte del grupo. De hecho en internet en buscador de google si capturamos packs en Jalisco, nos remite a una página de facebook (packs Jalisco.com)[31].

Packs[32] es una modalidad potencializada del sexting (textear respecto al sexo), es un "paquete" de dos o más imágenes. Para intercambiarlas, algunos jóvenes han creado grupos privados en redes sociales. Y de acuerdo con especialistas consultados, alguien del grupo puede traicionar la confianza de los involucrados y difundir las fotografías sin consentimiento de las afectadas. Como consecuencia, surge el bullying (acoso escolar) y, en el peor de los casos, hay riesgo de ser víctima de la trata de blancas. (Universidad de Guadalajra, 2017)

En este ciberdelito el principal dato personal robado son las fotos y videos intimas de las redes sociales como facebook , whatsapp, snapchat, instagram que los usuarios mismos producen, puede ser por voluntad propia del usuario de internet formando grupos muy reservados o porque un ciberdelincuente logró conexión con los dispositivos de los usuarios y roba los datos personales. Datos personales que vende al mejor postor, que en ocasiones son del crimen organizado dedicados a trata de blancas o red de prostitución infantil.

[29] Engaños por internet video ¿Nos conocemos? Recuperado en: https://www.youtube.com/watch?v=NuuppRGDUNk

[30] Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

[31] https://es-la.facebook.com/Packs-Jalisco-com-485705978595311/

[32] Prevención del Abuso Infantil. Video Recuperado en: https://www.educacionpas.org/Lobo-Jovenes/Basico/Civismo-Digital/Que-Hay-de-Los-Nudes-o-Packs

La obtención de datos personales por este ciberdelito, motiva a que se origine el ciberchantaje, que consiste en que una persona exija un beneficio a cambio de no divulgar fotografías o material audiovisual que afecte el honor del amenazado. Nuestro Código Penal para el Estado Libre y Soberano de Jalisco, pronto contemplará dicho ciberdelito (Informador M.X., 2019).

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Quinto, Capítulo I, que habla de los ultrajes a la moral o a las buenas costumbres e incitación a la prostitución, artículo 135 bis, establece:

> *Quien obtenga de persona mayor de edad, material con contenido erótico sexual y sin su consentimiento lo divulgue original o alterado, se le impondrá una pena de dos a cinco años de prisión. Cuando el ultraje señalado en el párrafo anterior se cometa a través de las tecnologías de la información y la comunicación, se le impondrá al responsable una pena de cuatro a ocho años de prisión. Este delito se perseguirá por querella de la parte ofendida. Se estará a lo previsto en el Código Penal Federal cuando los hechos se adecuen al delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo (Código Penal para el Estado Libre y Soberano de Jalisco, 2019)*

El artículo antes citado, prevé cuando se hace uso de las tecnologías de la información y la comunicación. La Ley referente a Ciberseguridad y Ciberdelitos que se propone debe prever este tipo de ciberdelito, y otorgar mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Recomendaciones preventivas para evitar el sexting o packs son: mantener en el caso de los menores de edad la comunicación con sus padres, recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, concientizar a los menores del riesgo de tomarse fotos y videos íntimos y el riesgo que esto conlleva, tener cuidado con los datos personales que se suben al internet en especial con las fotos y videos íntimos que suben en facebok, whatsapp, configura la privacidad de tus redes sociales[33], descarga antivirus en tu smarphone, computadora, elabora contraseñas robustas, mantén actualizado tu smartphone o computadora, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle que herramientas puede utilizar para su protección. Explicar al menor que el hecho de compartir fotos y videos íntimos de una persona desconocida es un delito.

Ransomware:

> *Software malicioso que infecta el ordenador y muestra mensajes que exigen el pago de un rescate para que el sistema funcione de nuevo. Esta clase de malware es un sistema de obtención de dinero criminal que puede instalarse mediante enlaces engañosos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. Tiene la capacidad de bloquear la pantalla de un ordenador o cifrar determinados archivos importantes con una contraseña (Kaspersky, 2019).*

El pasado 18 de marzo del presente año, la Fiscalía General de la República alertó, mediante su cuenta de twitter sobre la entrada de un código que tomaba el control de nuestra computadora con tan solo dar un clic. (Informador M.X., 2019)

[33] Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

El ciberdelincuente ingresa a nuestra laptop y encripta toda nuestra información, solicita rescate pero por lo general no se recupera información y queda en su poder.

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Sexto, Capítulo II, que habla de la obtención ilícita de información electrónica, artículo 143 bis, establece:

> *Al que sin autorización y de manera dolosa, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa (Código Penal para el Estado Libre y Soberano de Jalisco, 2019).*

Las penas previstas en este artículo se incrementarán en una mitad cuando el sujeto pasivo del delito sea una entidad pública o institución que integre el sistema financiero.

Para prevenir se debe realizar un respaldo de la información, actuar con precaución al seguir los enlaces de correos electrónicos, mensajes o en redes sociales, realizar actualizaciones de seguridad, utilizar herramientas anti-ransomware, mantener en el caso de los menores de edad la comunicación con sus padres, recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar.

Los anteriores son los ciberdelitos más comunes en Jalisco. Sin embargo, el ciberespacio es tan amplio y nuestra sociedad Jalisciense va avanzando tan rápido en el tema de las tecnologías de comunicación y de la información, que se originarán nuevos ciberdelitos, los cuales en Jalisco no son muy documentados, como:

Cracking:

> *El término "cracking" hace referencia a la práctica que consiste en atacar sistemas informáticos y software con intención maliciosa. Por ejemplo, se puede crackear una contraseña para acceder a la cuenta de un usuario, o una red Wi-Fi pública para interceptar los datos que circulan por ella. Se puede prevenir utilizando un administrador de contraseñas e instalando antivirus. (Avast, 2019).*

Spyware:

> *"Tipo de malware que los hackers utilizan para espiarle con el fin de acceder a su información personal, detalles bancarios o actividad en línea". Se previene instalando actualizaciones recientes, instalando parches de seguridad recientes, estableciendo niveles altos de seguridad y privacidad, extremando precauciones al momento de llevar intercambio de archivos, no dando click a ventanas emergentes. (Avast, 2019).*

Malware y Antimalware:

> *Malware hace referencia a cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los hackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Se previene utilizando antivirus o antimalware. (Avast, 2019).*

Keylogger:

> *Tipo de spyware que registra en secreto las pulsaciones de su teclado para que los ladrones pueden obtener información de su cuenta, datos bancarios y tarjetas de crédito, nombres de usuario, contraseñas*

y otros datos personales. Se previene utilizando un software anti-keylogger. (Avast, 2019).

Por lo que es necesario preparase tanto en capacitación y normatividad en el tema, caso contrario se estará ante el inminente riesgo de ser víctimas de nuestras propias circunstancias, porque como se cita anteriormente, los usuarios cada segundo que pasa proporcionan datos personales al internet, esos datos que seguramente son almacenados en servidores gigantescos, y que alguien estará analizando los metadatos[34] y creando nueva tecnología (inteligencia artificial).

Inteligencia artificial:

Conjunto de disciplinas de software, lógica, informática y filosofía que están destinadas a hacer que los PC realicen funciones que se pensaba que eran exclusivamente humanas, como percibir el significado en el lenguaje escrito o hablado, aprender, reconocer expresiones faciales, etc. El campo de la inteligencia artificial tiene una larga historia tras de sí, con muchos avances anteriores, como el reconocimiento de caracteres ópticos, que en la actualidad se consideran como algo cotidiano (Hewlett Packard, 2019).

De acuerdo al Estudio de Hábitos de los Usuarios en Ciberseguridad en México 2019, realizado mediante mesas de trabajo los días 28 y 30 de enero, así como el 1de febrero del presente año. Que contó con 5,011 asistentes a las mesas de ciberseguridad la mayoría menores de edad estudiantes de primaria y secundaria. De los cuales 150 fueron participantes de Jalisco. Estudio que reveló que no existe una conciencia clara del uso de redes sociales e internet. Y que día a día en ese tipo de plataformas comparten fotografías, ubicaciones u opiniones, con el fin de relacionarse. Siendo uno de los problemas más preocupantes el que un menor tenga acceso libre a la tecnología, dando click y click a todo lo que encuentra en internet. Dando como resultado la importancia de seguir fomentando las capacidades digitales de los usuarios de forma integral, donde se incluya el uso seguro y responsable de las tecnologías, además de crearse políticas públicas, leyes y programas sociales que lo apoyen. (Gobierno de México, 2019). De lo anterior se advierte que en Jalisco hace falta capacitarse en el tema de ciberseguridad, para consecuentemente no ser víctimas de robo de datos personales a través de ciberdelitos.

[34] Video. Red en Defensa de los Derechos Digitales M.X. ¿Qué son los metadatos? Recuperado en: https://www.youtube.com/watch?v=iKccR3E6jn4

Es importante mencionar que se realizó una encuesta sencilla, cuya vitrina metodológica es:

- Se entrevistó a menores de entre 13 a 16 años de edad, de algunas calles de una colonia del municipio de Zapopan, Jalisco, asegurando el anonimato a los entrevistados y se aplicó de forma aleatoria.
- El trabajo de campo se realizó en el mes de Junio del 2019.
- La muestra se compuso de 96 cuestionarios.
- El margen de error de las estimaciones de la encuesta es de ¬+/-5% en la colonia.
- La encuesta fue llevada por un servidor.
- El número de habitantes de dichas calles es de 500 menores.
- Cuya fórmula es:

N: Población. De calles 500 menores.

n: Muestra.

p: Probabilidad a favor.

q: Probabilidad en contra.

z: Nivel de confianza. 95%

e: Error de muestra.

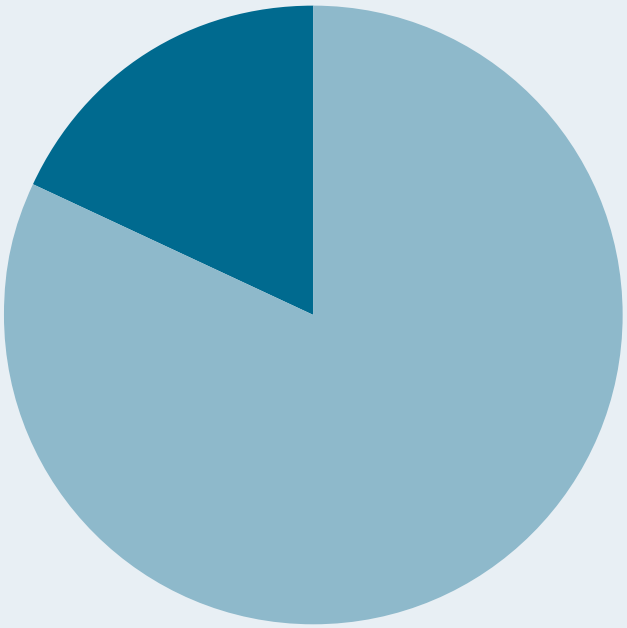
$$n = \frac{z2*p*q*N}{e2(N-1)+z2*p*q} \qquad n = \frac{1.96\text{^}(2)x0.5x0.5x500}{0.05\text{^}(2)x(500-1)+1.96\text{^}(2)x0.5x0.5} = 96 \text{ personas}$$

Las preguntas de cuestionario son respecto: Al tema de ciberseguridad y ciberdelitos, consistentes en:

1. ¿Conoce el ramsomware?, la mayoría de las respuestas fue: no.
2. ¿Comparte datos personales mediante wifi públicas?, la mayoría de las respuestas fue: sí.
3. ¿Conoces los cookies?, la mayoría de las respuestas fue: no.
4. ¿Cómo proteges tu router wifi?, la mayoría de las respuestas fue desconozco.
5. ¿Utilizar una misma contraseña para todos tus sitios?, la mayoría de las respuestas fue: utilizó una distinta.
6. ¿En facebook compartes fotos y videos?, la mayoría de las respuestas fue: sí.
7. ¿En facebook configuras tu privacidad?, la mayoría de las respuestas fue: no.
8. ¿Tienes instalado antivirus en tu laptop?, la mayoría de las respuestas fue: no.
9. ¿Conoces qué es un packs?, la mayoría de las respuestas fue: sí.
10. ¿Sabes qué es el ciberacoso?, la mayoría de las respuestas fue: no.
11. ¿Te han molestado mediante alguna red social?, la mayoría de las respuestas fue: sí.

Lo anterior se puede apreciar en la grafica siguiente:

Respuestas de 96 entrevistados =100%



Derivado de lo anterior, se sugiere que se debe expedir una Ley de Ciberseguridad[35] y Ciberdelitos en el Estado de Jalisco, que en sustancia responda al desarrollo de internet, de las redes sociales y la tecnología y que en el tema de las sanciones remita a nuestro Código Penal para el Estado Libre y Soberano de Jalisco.

Para emitirse deber realizarse en colaboración con autoridades internacionales especializadas en temas de ciberdelitos, toda vez que la tecnología ha tenido un rápido avance y debe existir armonización en las leyes contra ciberdelitos. Y así obtener beneficios para nuestra Ley Estatal.

[35] Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término es amplio y se aplica a numerosos elementos, desde seguridad informática hasta recuperación ante desastres y educación del usuario final. Recuperado en: https://latam.kaspersky.com/resource-center/definitions/what-is-cybersecurity

Autoridades Internacionales con normatividad en temas de ciberseguridad:

En Colombia tienen: CONPES 3701 DE 2011 Lineamientos Ciberseguridad y Ciberdefensa. Ley 527 de 1999- Validez jurídica y probatoria de la información electrónica; Ley 594 de 2000 – Ley General de Archivos – Criterios de Seguridad; Ley 679 de 2001 – Pornografía Infantil – Responsabilidad ISPs; Ley 962 de 2005 -Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas; Ley 1150 de 2007 – Seguridad de la información electrónica en contratación en línea; Ley 1266 de 2008 – Habeas data financiera, y seguridad en datos personales; Ley 1273 de 2008 – Delitos Informáticos y protección del bien jurídico tutelado que es la información; Ley 1341 de 2009 – Tecnologías de la Información y aplicación de seguridad; Ley 1437 de 2011 – Procedimiento Administrativo y aplicación de criterios de seguridad; Ley 1480 de 2011 – Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas; Decreto Ley 019 de 2012 Racionalización de trámites a través de medios electrónicos. Criterio de seguridad; Ley 1581 de 2012, Ley estatutaria de Protección de datos personales; Ley 1623 de 2013 – Ley de Inteligencia – Criterios de seguridad; Ley 1712 de 2014 – Transparencia en el acceso a la información pública (CERTICAMARA SA, 2014).

En Chile tienen: Respuestas y Comentarios a Consulta Ciudadana Política Nacional sobre Ciberseguridad; Respuestas y Comentarios a Consulta Ciudadana Política Nacional sobre Ciberseguridad; Texto consulta pública Política Nacional de Ciberseguridad (2016); Documento Bases Política Nacional sobre Ciberseguridad (2015); DTO-533_17-JUL-2015 Crea Comité Interministerial sobre Ciberseguridad (2015); Reglamento Funcionamiento Comité Interministerial sobre Ciberseguridad (2015); Agenda Digital 2020 (CSIRT CHILE, 2019).

En Unión Europea: "Reglamento 2019/881" (Viafirma, 2019).

En México contamos con la Policía Federal, la cual de conformidad con el Manual de organización General, establece que contará con:

- División Científica que establecerá los mecanismos, lineamientos, políticas, protocolos y procedimientos que permitan la aplicación de herramientas técnico-científicas en las funciones que desarrolla la Institución, mediante la selección e implementación de tecnologías a los procesos y los servicios en especialidades de criminalística, investigación de delitos electrónicos y seguridad de sistemas de información, y aquellos en los que se requiera la aplicación.

- Coordinación para la Prevención de Delitos Electrónicos que conducirá las acciones de investigación de las conductas delictivas que utilicen medios electrónicos para su comisión, así como aquellas que representen amenazas y ataques a los sistemas de información, a través de la respuesta a solicitudes de colaboración, monitoreo de la red pública de Internet y aplicación tecnológica, electrónica, informática y de telecomunicaciones, desarrollada por los laboratorios de innovaciones, para prevenir y combatir aquellas conductas posiblemente constitutivas de delito en el territorio nacional.

- Dirección General de Prevención de Delitos Cibernéticos que dirige las acciones y procedimientos basados en el análisis de la información de la operación de actores o grupos delictivos, así como hechos delictivos en cuya comisión se utilicen medios cibernéticos, mediante el uso de herramientas especializadas para la vigilancia, monitoreo y rastreo de la red pública de Internet, así como la identificación, recolección y análisis de la información contenida en indicios digitales, con la finalidad de prevenir e investigar los delitos en coadyuvancia con las áreas de

la Institución y autoridades competentes conforme a las disposiciones aplicables.

- Dirección General del Centro Especializado en Respuesta Tecnológica que coordinará las respuestas a incidentes de seguridad informática en la estructura informática crítica de México, en colaboración con los diferentes órdenes de gobierno y actores sociales, mediante la aplicación de técnicas científicas para la identificación y mitigación de incidentes cibernéticos, así como de métodos avanzados de investigación y análisis, a fin de prevenir y combatir delitos que se cometan utilizando medios electrónicos o tecnológicos.

- Dirección General de Laboratorios en Investigación Electrónica y Forense que determinará los mecanismos de protección para la infraestructura informática crítica del país en tiempo real, a través de la operación de los laboratorios en investigación electrónica y forense, con la finalidad de implementar canales seguros para el intercambio de información de las investigaciones, con organismos homólogos nacionales y extranjeros conforme a las disposiciones aplicables.

Además la Coordinación para la Prevención de Delitos Electrónicos tendrá la atribución de establecer alianzas de cooperación con organismos y autoridades nacionales e internacionales relacionados con la prevención de delitos electrónicos.[36]

En Jalisco se cuenta con la Policía Cibernética que fue creada con la finalidad de detectar por medio del patrullaje en la red, los sitios, procesos y responsables de las diferentes conductas delictivas que se puedan cometer en contra y a través de medios informáticos y electrónicos. La Fiscalía General del Estado a través de la coordinación de Policía Cibernética brinda orientación a la ciudadanía respecto de los pasos que deberá seguir para presentar una denuncia en caso de ser víctima de un delito cometido a través del uso de las tecnologías de la información, además de que la Policía Cibernética colabora con el Ministerio Publico de así requerirlo en las investigaciones.

Es necesario destacar que al tener conexión con internet se ingresa al ciberespacio donde el usuario adquiere una identidad digital e incluso una vida que en ocasiones es anónima, y hace cosas que en su vida física no se atreve hacer o decir.

Se propone que entre los temas que debe contener la Ley de Ciberseguridad y Ciberdelitos en el Estado de Jalisco, se consideren los siguientes:

1.- Disposiciones Generales:

En las que se establezca la naturaleza e interpretación de la Ley.

2.- Objetivos de la Ley:

Donde se establezca que regulará las plataformas digitales, las redes sociales, aplicaciones, el internet de la cosas, entre otras comunicaciones digitales.

3.- Glosario de la Ley:

Que se deberá entender por amenaza, sujeto activo, sujeto pasivo, activo de información, ciberdefensa, datos personales, riesgo, entre otros.

Donde se explique conceptos propios de la Ley.

4.- Supletoriedad.

5.- De la comunicación digital:

Donde con apoyo de expertos en ciberseguridad que formen parte de las mesas de trabajo se establezca en específico cada tema referente a: Plataformas digitales, aplicaciones, redes sociales, del internet de las cosas, de la inteligencia artificial, el wifi público, sitios web.

6.- De las autoridades cibernéticas:

En este apartado se debe establecer qué autoridades deben intervenir en caso de ciberdelitos, sus obligaciones, funciones y facultades. Centro de reacción a incidentes. Policías cibernéticas.

[36] Artículo 27, fracción VII, del Reglamento la Ley de la Policía Federal.

7.- De la Cooperación de asociaciones privadas en temas de ciberseguridad:

En virtud de que en un futuro muy cercano todo será digital, por lo que es necesario involucrar a las asociaciones privadas, recordando que la ciberseguridad es un compromiso de todos.

8.- De la cooperación de autoridades internacionales.

9.- Capacitación en temas de Ciberseguridad:

Este apartado deberá establecerse que se otorgará presupuesto a las autoridades cibernéticas para efectos de capacitar en temas de ciberseguridad, manejo de portales, registro de identidades digitales, el internet de las cosas y sus riesgos, estudio de ciberdelitos, prevención de ciberdelitos, inteligencia artificial, big data, creando guías, videos educativos, se lleven a cabo campañas para elaborar contraseñas seguras, se den herramientas para detectar las fake news en redes sociales, como proteger wifi, como hacer compras seguras en internet, como proteger a nuestro menores en internet, como descargar antivirus, como proteger nuestros smartphone, como cifrar nuestros datos personales, crear juegos educativos para menores en temas de ciberseguridad, ciberdelito y cómo prevenirlos, celebrar convenio con autoridades internacionales para formar perito ciberforenses y porque no ciberabogados, formas de autenticación en el ciberespacio.

El ciberabogado deberá tener conocimientos informáticos y en ciberseguridad, puesto que todo se encontrará en la red, para asesorar a su cliente desde el ciberespacio; con formación digital; y con conocimientos de las normas que intentan ordenar el ciberespacio, donde asesora a ciudadanos, organizaciones y empresas en materias TIC (Tecnologías de la Información y la Comunicación) y por otro lado asesora a ciberciudadanos y ciberempresas en el nuevo entorno, con nuevos paradigmas, conflictos y normas (Campus Internacional Ciberseguridad, 2019).

La capacitación de ser de acuerdo al sector que vaya dirigida, sea seguridad pública, militar, educacional, ambiental, entre otras.

Con el objetivo de lograr la ciberresilencia: capacidad de los sectores público, privado, y de la sociedad para enfrentar este entorno sin que afecte su habilidad de operar día con día se denomina (McKinsey&Company, 2018). Es importante invertirle a la educación ya que no hay tiempo, la tecnología nos está superando y debemos tener el control.

10.- De los ciberdelitos, apartado donde se establezca:

Descripción, en específico de cada ciberdelito con apoyo de experto en la materia.

11.- Evidencia digital:

Donde se establezca qué elementos son necesarios para acreditar el tipo de ciberdelito, procedimiento para llevar acopio de evidencia, si deben ser certificaciones de publicaciones ante notario, cómo ofrecer peritos o informes, cómo llevar la actuación mediante orden de un juez, análisis de imágenes y videos, qué métodos debemos utilizar para análisis de evidencia, cómo deducir a qué redes sociales estuvo conectado el ciberdelincuente, cómo acreditar si la evidencia fue borrada intencionalmente, cómo descubrir las huellas en el ciberespacio. Valdría la pena agregar un apartado de ciberforense e informática forense.

Informática forense: Aplicación de técnicas científicas y analíticas especializadas en la infraestructura y dispositivos tecnológicos que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. En la actualidad la estructura documental de presentación de cualquier reclamación judicial, querellas o escrito tiene una estructura clara y definida, que permanece invariable, y que de no ser así se rechaza por defecto de forma (Es Ciber, 2019).

12.- Sanciones:

Donde se establezca que se aplicarán las penas establecidas en nuestro Código Penal para el Estado Libre y Soberano de Jalisco, pero haciendo reformas en el sentido de que serán más severas, dependiendo del modus operandi del ciberdelincuente.

Conclusiones

Ante el evidente y acelerado avance de las tecnologías de información y comunicaciones, es necesario concientizar a las autoridades y a los usuarios de internet, de los riesgos que hay en el ciberespacio, pues como quedó demostrado en el contenido del presente artículo, los practicantes ciberdelincuentes se ponen a la vanguardia de la tecnología para obtener robo de datos personales, ingresando de forma no autorizada a sistemas informáticos y financieros, creando aplicaciones y sitios webs falsos, accediendo a dispositivos inteligentes que se conectan a internet y están vinculados a los smartphone o teléfonos inteligentes como las pulseras inteligentes, enviado correos electrónicos falsos, por medio de bocinas inteligentes, y todo para obtener un beneficio económico, idealista o por venganza.

Es de suma importancia otorgar información de los ciberdelitos a los ciudadanos Jalisciense tales como: 1.- Ciberacoso o ciberbullyng; 2.- Suplantación de identidad; 3.- Grooming; 4.- Sexting; 5.- Ransomware; 6.- Phishin; 7.- Smishing; y 8.-Vishing. Los ciudadanos Jalisciense deben conocer las amenazas y riesgos que enfrentarán cuando utilizan la tecnología y el ciberespacio.

Se debe estar a la vanguardia en tecnología porque surgirán nuevos ciberdelitos, por lo que es necesario cooperar con autoridades internacionales como Estonia, Colombia, Chile, España, Singapur, Estados Unidos, Japón respecto al tema de ciberdelitos, de acuerdo a informes de la Condusef en el primer trimestre de 2019, las quejas por fraudes cibernéticos crecieron un 19% respecto al 2018 y representan cada año una mayor proporción[37].

Es necesario destinar mayor presupuesto a campañas de publicidad respecto a la cultura de ciberseguridad, para lograr que se realice vía radio, televisión, redes sociales, sitios webs, realizar foros, infografías, folletos que lleguen como coloquialmente se menciona al ciudadano de a pie.

[37] Fraudes cibernéticos y tradiciones. Consultado en: https://www.condusef.gob.mx/gbmx/?p=estadisticas

Se generen políticas públicas donde se involucren a las autoridades de los tres niveles Federal, Estatal y Municipal competentes en el sector educativo y tecnológico, para que se establezca como materia en las escuelas el tema de ciberseguridad y ciberdelitos, toda vez que los menores son los más expuestos a ciberdelitos. Y se capacite respecto al uso de wifi seguras, antivirus, sitios webs, compras online, cuidado de datos personales, redes sociales, correos electrónicos infectados, servicios en la nube seguros, herramientas para dispositivos para evitar robo de datos personales.

Es necesario se expida una Ley de Ciberseguridad y Ciberdelitos en el Estado de Jalisco, que en sustancia responda al desarrollo de internet, de las redes sociales y la tecnología y que en el tema de las sanciones remita a nuestro Código Penal para el Estado Libre y Soberano de Jalisco.

Dar al Internet de las cosas, uso responsable, por ejemplo en el caso de pulseras inteligentes pueden ayudar para integrar debidamente el expediente clínico de los usuarios. El análisis de las grandes cantidades de información puede ser utilizada para un fin positivo mejoraría nuestra calidad de vida e incluso nuestro planeta, seriamos un Jalisco digital de primer mundo y tendríamos control en: ciberambiente, cibereducación, cibergobierno, cibercomercio, cibersanidad.

Debemos estar muy preparados en temas de ciberseguridad y ciberdelitos, es necesario que nuestras normas evolucionen, caso contrario la gran información que es almacenada, puede ser utilizada para obtener el control total de todos los servicios.

Se debe cuidar a los menores cuando estén usando la conexión de internet, porque son los más vulnerables, se debe hablar y tratar los temas de ciberdelitos para lograr concientizarlos, y lograr que cuando haya reuniones familiares convivan y no estén únicamente conectados a las redes sociales.

Luis Abraham Rincón Prieto

Abogado egresado de la Universidad de Guadalajara. Egresado de la Especialidad en Gestión, Publicación y Protección de Información por el CESIP del ITEI. Notificador en Juzgados de Primera Instancia del Poder Judicial. En el Supremo Tribunal de Justicia del Estado como encargado del archivo en la Sala Auxiliar Mixta. Litigante en despacho jurídico. Coordinador Especializado “A” en el Despacho del C. Gobernador. Coordinador de archivos del OPD Consejo Municipal del Deporte de Zapopan, Jalisco.

Referencias

(s.f.).

Aguilar., R. (27 de julio de 2017). *Andro4 Cill.* Obtenido de Así es como te la cuelan con los términos y condiciones de usuario.: Ricardo Aguilar (27 de julio de 2017). Así es como te la cuelan con los términos y condiciones de usuario. Andro4all. Recuperado de https://andro4all.com/2017/07/terminos-condiciones-problemas-android

Andrés, M. B. (2018). *Internet de las Cosas.* Madrid: Reus.

Avast. (24 de Septiembre de 2018). *¿Podrián los altavoces inteligentes desmontar tu hogar inteligente?* Obtenido de https://blog.avast.com/es/podrian-los-altavoces-inteligentes-desmontar-tu-hogar-inteligente

Avast. (2019). *Cracking.* Obtenido de https://www.avast.com/es-es/c-cracking

Avast. (2019). *Keylogger.* Obtenido de https://www.avast.com/es-es/c-keylogger

Avast. (2019). *Malware y Antimalware.* Obtenido de https://www.avast.com/es-es/c-malware

Avast. (2019). *Spyware.* Obtenido de https://www.avast.com/es-es/c-spyware

Campus Internacional Ciberseguridad. (2019). *¿Por qué son necesarios los ciberabogados en la nueva ciber-realidad?* Obtenido de https://www.campusciberseguridad.com/blog/item/123-por-que-son-necesarios-los-ciberabogados-en-la-nueva-ciber-realidad

CERTICAMARA SA. (01 de Marzo de 2014). *Instrumentos Normativos de Ciberseguridad.* Obtenido de https://web.certicamara.com/app/webroot/media/import/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf

Código Penal para el Estado Libre y Soberano de Jalisco. (11 de Mayo de 2019). Periódico Oficial “El Estado de Jalisco”. México, Jalisco, México: Congreso del Estado de Jalisco.

Condusef. (2019). *Portal de fraudes financieros.* Obtenido de https://phpapps.condusef.gob.mx/fraudes_financieros/informate.php

Constitución Política del Estado de Jalisco. (09 de Abril de 2019). Periódico Oficial “El Estado de Jalisco”. México, Jalisco, México: Congreso del Estado de Jalisco.

CSIRT CHILE. (2019). *Ciberseguridad.* Obtenido de https://www.ciberseguridad.gob.cl/documentos/

Díaz, F. N. (Diciembre de 2014). *Promexico. Mx.* Obtenido de http://promexico.mx/documentos/mapas-de-ruta/internet-of-things.pdf

Es Ciber. (29 de Mayo de 2019). *Curso Forense.* Obtenido de https://www.es-ciber.com/ciberseguridad/cursos-forense/

Gobierno de México. (2019). *Estudio "Hábitos de los usuarios en ciberseguridad en México 2019".* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

Gobierno de México. (15 de marzo de 2019). *Procuraduría Federal del Consumidor.* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/445899/DIA_MUNDIAL_DE_LOS_DERECHOS_DEL_CONSUMIDOR_2019.pdf

Hewlett Packard. (2019). *¿Que es la inteligencia artificial?* Obtenido de https://www.hpe.com/mx/es/what-is/artificial-intelligence.html

Inegi.Org.Mx. (2017). *Módulo sobre ciberacoso 2017.* México.

Informador M.X. (29 de Diembre de 2017). *Crecen denuncias por fraude en Jalisco; diciembre es el mes con más casos.* Obtenido de https://www.informador.mx/Crecen-denuncias-por-fraude-en-Jalisco-diciembre-es-el-mes-con-mas-casos-l201712290001.html

Informador M.X. (18 de Marzo de 2019). *Alertan sobre programa malicioso que toma control dela computadora.* Obtenido de https://www.informador.mx/mexico/Alertan-sobre-programa-malicioso-que-toma-control-de-la-computadora-20190318-0112.html

Informador M.X. (05 de Febrero de 2019). *Congreso de Jalisco aprueba que el "ciberchantaje" sea delito.* Obtenido de https://www.informador.mx/jalisco/Congreso-de-Jalisco-aprueba-que-el-ciberchantaje-sea-delito--20190205-0146.html

Informador Mx. (22 de Agosto de 2018). *Tras reforma, crecen denuncias porciberdelitos contra menores de edad.* Obtenido de https://www.informador.mx/Tras-reforma-crecen-denuncias-por-ciberdelitos-contra-menores-de-edad-l201808220001.html

Informador Mx. (06 de Mayo de 2019). *Jóvenes jaliscienses, de los más ciberacosados.* Obtenido de https://www.informador.mx/jalisco/Jovenes-jaliscienses-de-los-mas-ciberacosados-20190506-0020.html

Informador. Mx. (24 de Abril de 2019). *Sufren calvariopor fraude en créditos del Infonavit.* Obtenido de https://www.informador.mx/Sufren-calvario-por-fraude-en-creditos-del-Infonavit-l201904240001.html

Inteco. (2019). *Instituto Nacional de Tecnologías de la Comunicación.* Obtenido de https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

Internauta, O. d. (16 de Febrero de 2015). *Instituto Nacional de Ciberseguridad de España M.P., S.A.* . Obtenido de https://www.osi.es/es/actualidad/blog/2015/02/16/lee-antes-de-aceptar-lo-que-no-leemos-de-las-condiciones-y-terminos-de-uso

Internauta, O. d. (18 de Diciembre de 2015). *Instituto Nacional de Ciberseguridad de España M.P., S.A.* . Obtenido de https://www.osi.es/es/actualidad/blog/2015/12/18/la-privacidad-en-wearables-en-que-punto-se-encuentra

Internauta, O. d. (2019). *Instituto Nacional de Ciberseguridad de España M.P., S.A.* Obtenido de Los ciberdelincuentes, ¿quiénes son?: https://www.osi.es/es/campanas/los-ciberdelincuentes-quienes-son

Is4k. (2019). *Internet Segura ForkiDs.* Obtenido de https://www.is4k.es/necesitas-saber/sexting

Karpersky. (2019). *Robo de Identidad: hechos y preguntas frecuentes.* Obtenido de https://www.kaspersky.es/resource-center/threats/identity-theft-facts-and-faq

Kaspersky. (2019). *¿Qué es el clickjacking?* Obtenido de https://www.kaspersky.es/resource-center/definitions/clickjacking

Kaspersky. (2019). *¿Que es el ransomware?* Obtenido de https://www.kaspersky.es/resource-center/definitions/what-is-ransomware

Kaspersky. (2019). *Cómo evitar los riesgos de seguridad asociados a las redes Wifi públicas.* Obtenido de https://latam.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Mariana R. Fomperosa. (21 de Diciembre de 2018). *Milenio.* Obtenido de https://www.milenio.com/tecnologia/resena-echo-amazon-bocina-inteligente-alexa

Martínez, J. G. (2017). *Bullyingg, sexting y grooming .* Colombia: San Pablo.

McKinsey&Company. (2018). *Perspectiva de ciberseguridad en México.* México: Comexi.

Netflix. (2017). *La red obscura.* Obtenido de https://www.netflix.com/mx/title/80182553

Nora Muñiz. (25 de Junio de 2019). *Plumas Atomicas.com.* Obtenido de https://plumasatomicas.com/noticias/extraordinario/que-hacer-ante-el-ciberacoso/

OCU Ediciones, S. (06 de Novimembre de 2009). *Organización de Consumidores y Usuarios.* Obtenido de https://www.ocu.org/dinero/tarjetas/noticias/tarjetas-cuidado-con-el-cvv-472704

Oficina de Seguridad del Internauta. (2019). *Mensajeria Instantanea.* Obtenido de https://www.osi.es/es/mensajeria-instantanea

Oficina de Seguridad del Internauta. (2019). *WhatsApp, Telegram y Line. ¿Cuál es más segura para chatear?* Obtenido de https://www.osi.es/es/actualidad/blog/2014/05/09/whatsapp-telegram-y-line-cual-es-mas-segura-para-chatear

Red en Defensa de los Derechos Digitales M.x. (28 de Mayo de 2015). *¿Que son los metadatos?* Obtenido de https://www.youtube.com/watch?v=iKccR3E6jn4

Schwab, K. (2016). *La Cuarta Revolución Industrial.* Suiza: Penguin Randon House.

Social, C. (02 de Abril de 2019). *INEGI.* Obtenido de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/OtrTemEcon/ENDUTIH_2018.pdf

SUN. (28 de Octubre de 2018). *Informador MX.* Obtenido de https://www.informador.mx/tecnologia/Apple-HomePod-el-nuevo-sonido-de-la-casa-20181028-0048.html

Universidad de Guadalajra. (27 de Diciembre de 2017). *La Red Universitaria de Jalisco.* Obtenido de http://www.udg.mx/es/noticia/packs-intercambio-imagenes-eroticas-redes-sociales-pasatiempo-alto-riesgo

Viafirma. (20 de Junio de 2019). *La nueva Ley de Seguridad Cibernética de la Unión Europea .* Obtenido de https://www.viafirma.com/blog-xnoccio/es/ley-seguridad-cibernetica-union-europea/

Fotografía: Jijomathai para Adobe Stock

La doctrina del *transformative use* del Copyright (derecho de autor), en beneficio del derecho a la información, a través de los motores de búsqueda

Rafael Ríos Nuño
Jefe de Apoyo Técnico en la Unidad de Transparencia de la UdeG

Resumen

En la actualidad son sabidas las constantes tensiones y conflictos a los que se enfrentan las instituciones de educación e investigación, las bibliotecas, los museos y los archivos en su labor de digitalizar los documentos que poseen o administran, ya sea por mandato legal o administrativo. Lo anterior, en virtud de que los libros y los archivos también pueden ser depositarios de otros derechos como el de autor, la privacidad y la protección de datos, que, en algunas ocasiones prohíben la reproducción o difusión de obras artísticas o literarias y para el caso que nos ocupa, le otorgan al titular el derecho exclusivo a autorizar o prohibir la transformación de la obra (digitalización). Por lo tanto, mediante una búsqueda documental y hermenéutica, se dejará a disposición del lector, una interpretación progresiva del derecho de transformación de las obras protegidas.

Avanzando en nuestro razonamiento, se propondrá una solución a la colisión de derechos para determinar si se encuadra en una causal de infracción al derecho de autor y en consecuencia será necesario contar con el consentimiento expreso del titular, o si, por el contrario, derivado de las interpretaciones de las doctrinas del *fair use* y *transformative use*, así como del principio de la progresividad y no regresividad, el juicio de proporcionalidad y el de la prueba de los tres pasos del Convenio de Berna se usarán como base de la propuesta para la configuración de una nueva política pública, amparada en beneficio de la sociedad y la búsqueda amigable de la información en Internet.

PALABRAS CLAVES:
Derecho a la Información, Derecho de Autor, Motores de Búsqueda, Derecho de Transformación, Juicio de Proporcionalidad, Prueba de los Tres Pasos

I. Introducción: Límites y alcances del derecho a la información y los derechos de autor

Según Villanueva (2006, p. 23) la expresión es la forma a través de la cual la persona exterioriza sus pensamientos en signos, palabras o gestos que tengan como propósito comunicar algo. En virtud de lo anterior, el tratadista refuerza la idea a través de la interpretación que hace el Tribunal Constitucional Español al advertir que "…la libertad de expresión tiene por objeto pensamientos, ideas y opiniones, concepto amplio dentro del que deben incluirse también creencias y los juicios de valor" (Villanueva, 2006, p. 23).

En la misma línea argumentativa, la Suprema Corte de Estados Unidos en una de sus labores más recientes de interpretar la primera enmienda, instaura que, la libertad de expresión conlleva la libertad de escuchar y la prohibición al Estado de limitar la información a la cual pueden recurrir los miembros del público (Ackerman y Sandoval, 2015, pp. 16 y 17). En consecuencia, se puede afirmar que, la libertad de expresión es uno de los derechos fundamentales de las personas porque representa la prolongación de la garantía individual de pensar, ejercicio sin el cual no es posible aventurar la posibilidad del desarrollo de las personas en sociedad (Villanueva, 2006, p. 23).

Como se afirmó arriba, la consolidación contemporánea de la libertad de expresión es resultado inequívoco del desarrollo educativo de las personas. La educación hace las veces de instrumento esencial de transmisión de conciencia y del vehículo que habilita a las personas para el ejercicio pleno del sentido de ciudadanía, cuya aprehensión colectiva entraña una sociedad civil con mayores espacios de participación e injerencias en la res pública (Villanueva, 2006, p. 25).

Por otra parte, es menester señalar que todos los derechos humanos tienen como característica primordial la interdependencia, así como la progresividad y la no regresividad, esto quiere decir que existe una obligación de los Estados de generar en cada momento histórico una mayor protección y garantía de los derechos humanos, de tal forma que siempre estén en constante evolución y bajo ninguna justificación en retroceso (Comisión Estatal de Derechos Humanos Jalisco)[1].

En ese orden de ideas, de la Parra (2015b, p. 18) asevera que:

> *"la libertad de expresión deja de ser un derecho humano que imponía una abstención al Estado para que no se entrometiera en la comunicación de opiniones y pensamientos, transformándose en el moderno derecho a la información: un derecho humano que amplía el contorno tradicional de la libertad de expresión, integrado por un haz de facultades jurídicas que, incluso, reclaman la actividad del Estado para la salvaguarda del intercambio de información".*

De suerte que se puede afirmar que el derecho a la información viene a reforzar las prerrogativas consistentes en la libertad de buscar, recibir y difundir información e ideas por cualquier medio, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro medio de expresión, conocido o por conocerse.

En esa sintonía, Cendejas (2010, pp. 8 a 10), advierte que es importante delimitar el contenido de las libertades de investigar, difundir y recibir información, y para ello se dio a la tarea de concretarlas de la siguiente manera:

a) La libertad de investigar información: es la facultad de acceder directamente a las fuentes de la información adecuadas, a la información y a las opiniones que son necesarias para elaborar el mensaje informativo que se pretende transmitir.

b) La libertad de difundir información: es la libertad de informar, de difundir el mensaje

[1] Para más información, consulte la página de la Comisión Estatal de Derechos Humanos Jalisco, apartado de Principios constitucionales en materia de derechos humanos, disponible en: http://cedhj.org.mx/principios_constitucionales.asp

informativo. Es la facultad activa que tutela no sólo el hecho mismo de la difusión, sino también el contenido y la actividad de búsqueda de la información.

c) La libertad de recibir información: comprende la posibilidad para toda persona de recibir información libremente, sin restricciones o trabas injustificadas. Asimismo, la libertad de recepción comprende el derecho de recibir libremente toda la gama de informaciones y opiniones que puedan darse.

Ahora veamos que la libertad de información ve a la persona receptora siempre como un sujeto pasivo que tiene la facultad de elegir el medio por el cual ha de recibir esa información.

Habría que decir que en el momento en que haya una sola información, o una sola opinión, o ideología, Cendejas (2010 pp. 8 a 10) propone que puede decirse que la facultad de recibir información y opiniones no se facilita plenamente, es decir, en el momento en que cualquiera de las opciones existentes o posibles desaparece está sufriendo una limitación al derecho a optar como una forma de ejercitar el derecho a recibir.

Como se advirtió arriba, se puede argumentar que el derecho a la información ha evolucionado y crecido lo suficiente para convertirse en un derecho humano autónomo y justiciable. No obstante de lo anterior, se le sigue llamando tradicionalmente como "libertad de expresión"; asimismo, se le suele confundir con una de sus extensiones, el "derecho de acceso a la información pública gubernamental" (de la Parra, 2015, p. 14).

Todavía cabe señalar que Cendejas (2010, p. 17) asegura que, resulta importante mencionar que la información en un Estado democrático se concibe como un bien de interés general necesario para la participación ciudadana en la democracia, y como tal bien, además de ser tutelado jurídicamente, debe ser prestado a todos los ciudadanos por los poderes públicos.

En otro orden de ideas, la Organización Mundial de la Propiedad Intelectual (OMPI, 2017), define al derecho de autor como un conjunto de derechos exclusivos encaminados a la protección de las obras literarias y artísticas. La finalidad del derecho de autor es retribuir los esfuerzos intelectuales de los autores a la vez que promover las ciencias, la cultura y las artes.

Por esa razón, los Estados le otorgan una serie de derechos exclusivos a los creadores de las obras, reconociéndoles ese conjunto de derechos, también los amparan a través de diversas medidas de protección. En el caso de México, el autor o el titular que considere violentado su derecho puede recurrir a las vías administrativas, civiles o penales para solicitar a las autoridades competentes el cese de la violación; dichas vías pueden iniciarse paralela o conjuntamente, sin necesidad de agotar una previamente, es decir, se confiere a los autores una serie de derechos patrimoniales y morales exclusivos. Los derechos patrimoniales están relacionados con la explotación económica de la obra, mientras que los derechos morales protegen los intereses personales del autor sobre la obra.

En otro sentido, la OMPI (2017) ha señalado en las aportaciones de la tradición del derecho anglosajón o *common law*, que la prioridad en esta tradición es la explotación económica de la obra y, por consiguiente, el derecho de autor es considerado un derecho patrimonial, o sea, de propiedad, y constituye un título que facilita la explotación económica.

Antagónicamente, la OMPI (2017) ha sostenido que, en la tradición del derecho codificado o derecho civil, da por sentado que la expresión creativa constituye un elemento inherente a la persona y de la personalidad del ser humano y, en consecuencia, el derecho de autor se inscribe en la órbita de los derechos naturales de la persona, con lo cual ese derecho natural queda ligado íntimamente a la persona del autor. En esa tradición se considera que el derecho de autor es un derecho personal, una extensión de la libertad de expresión, es decir, un derecho que forma parte de los derechos humanos.

Simultáneamente la OMPI (2017) concluye que, pese a sus aparentes diferencias, en ambas tradiciones se establece la necesidad de proteger al autor, pues es éste quien crea obras que son necesarias para las industrias culturales, sin desmedro de la necesidad de poner al alcance del público las expresiones creativas de dicho autor. En otras palabras, aunque ambas tradiciones parten de criterios totalmente distintos, no cabe duda de que, tanto en una tradición como en la otra, la finalidad práctica suele ser la misma, aunque se llegue a ella por diferentes sendas.

Asimismo, Corredoira (2012, p. 20) afirma que en el derecho anglosajón y el español cualquier de los dos sistemas la clave o "core" del asunto es el mismo: se protege la obra original o derivada, no la simple idea, que se plasma en un soporte tangible o intangible sin necesidad de registro ni de acciones específicas para su reconocimiento.

Igualmente, recordemos que los derechos de autor no protegen las ideas, quien lea tal obra, podrá servirse libre e impunemente, de las ideas, principios, hipótesis y reglas que encierra (Rogel, 2012, pp. 19 y 20).

A. Los derechos morales

De la Parra (2015a, p. 209) explica que aunque en un principio el derecho de autor tenía un contenido meramente económico, con el tiempo se fueron regulando aspectos para proteger los aspectos no pecuniarios, es decir, los intelectuales.

En esa sintonía el citado autor continúa exponiendo que los derechos morales tienen como fin último proteger la dignidad de los autores, toda vez que, las obras se consideran manifestaciones de la personalidad del autor.

Asimismo, de la Parra (2015a, p. 209) afirma que los derechos morales se han ido reconociendo tanto en el sistema del derecho civil o codificado como en el del copyright (anglosajón).

Volviendo al tema que nos ocupa, de la Parra (2015a, p. 211) advierte que el derecho moral del autor no es un derecho innato, es decir, no se adquiere por el simple hecho de ser persona, sino que se necesita de un acto de creación intelectual.

Bajo la misma línea argumentativa, la OMPI propone a los Estados miembros el reconocimiento mínimo de las siguientes facultades del derecho moral:

a) El derecho de paternidad; y

b) El derecho a oponerse a algunas modificaciones de la obra.

A su vez, las leyes y la doctrina se han dado a la tarea de delimitar y definir dichas facultades. Magaña (2013, pp. 41 a 43) advierte que los mismos se pueden enlistar en los siguientes tipos y los define de la siguiente manera:

a) El derecho de divulgación: también es conocido como derecho de edición o publicación y consiste en que el autor tiene derecho a dar a conocer su obra –así como a elegir la forma de hacerlo– o mantenerla inédita.

b) El derecho de paternidad: consiste en ser reconocido como autor de todo acto de reproducción o comunicación de su obra, a través de su nombre o su seudónimo.

c) El derecho de respeto: el autor tiene la facultad de exigir respeto sobre la integridad de su obra, es decir, que su obra no sea modificada o deformada por un tercero.

d) El derecho de modificación: el creador de una obra puede modificarla posteriormente.

e) El derecho de retracto: llamado también derecho de arrepentimiento. El autor tiene la prerrogativa de retirar su obra del comercio en cualquier momento. Sin embargo, puede ser acreedor al pago de daños y perjuicios que dicha acción ocasione.

f) El derecho de oposición: esto, es, impedir que se le atribuya una obra que no es de su autoría.

Hay que mencionar además que la vigencia de los derechos morales es imprescriptible y son derechos irrenunciables (Magaña, 2013, p. 40).

B. Los derechos patrimoniales

Según la OMPI (2017), los derechos patrimoniales que se conceden a los autores pueden dividirse en tres categorías principales:

a) El derecho de reproducción;

b) El derecho de traducción y adaptación; y

c) El derecho de interpretación o ejecución públicas, de radiodifusión y de comunicación al público.

Al mismo tiempo, de la Parra (2015a, p. 233 a 249) asegura que las formas más usuales de explotación son la reproducción, la distribución, la comunicación pública y la transformación; mismas que las define de la siguiente manera:

a) El derecho de reproducción: es la facultad clásica del derecho de explotación, y es aquella por virtud de la cual se pueden autorizar o prohibir los actos de reproducción de una obra.

Como se señaló arriba, de la Parra, cita el artículo 16, fracción VI de la Ley Federal del Derecho de Autor, con el objeto de evidenciar, lo que se debe entender por reproducción:

Artículo 16.- La obra podrá hacerse del conocimiento público mediante los actos que se describen a continuación:

(…)

VI. Reproducción: La realización de uno o varios ejemplares de una obra, de un fonograma o de un videograma, en cualquier forma tangible, incluyendo cualquier almacenamiento permanente o temporal por medios electrónicos, aunque se trate de la realización bidimensional de una obra tridimensional o viceversa.

Avanzando en nuestra investigación de la Parra (2015a) advierte que en la actualidad se debe contar con una definición más amplia y para ello cita a Lipszyc quien lo define como:

"El derecho de reproducción es la facultad de explotar la obra en su forma original o transformada, mediante su fijación material en cualquier medio y por cualquier procedimiento que permita su comunicación y la obtención de una o varias copias de todo o parte de ella".

b) El derecho de distribución: es el complemento tradicional a la facultad de reproducción, en tanto se refiere a la circulación de los ejemplares de la obra.

Dicho lo anterior, cabe resaltar que uno de los aspectos a considerar desde la óptica del citado autor, es la figura del agotamiento del derecho, es decir, el agotamiento de la facultad de distribución consiste en que, una vez verificada la primera venta de un ejemplar concreto de una obra, se agota o extingue la facultad de distribución.

c) El derecho de comunicación pública: según de la Parra (2015a), la comunicación pública es un acto de explotación conceptualmente opuesto a la distribución, en tanto que ésta última se refiere a la posibilidad de adquirir la propiedad o el uso de los ejemplares de la obra, mientras que en la comunicación pública no hay esa posibilidad.

Por lo tanto, la comunicación pública es la difusión de la obra sin circulación de copias destinadas a ser apropiadas o usadas por el público.

d) Derecho de transformación: en virtud de que no existe una definición de qué se debe entender por transformación en nuestra legislación, de la Parra (2015a) cita a Lipszyc quien lo define como “El derecho de transformación consiste en la facultad del autor de explotar su obra autorizando la creación de obras derivadas de ella: adaptaciones, traducciones, revisiones, actualizaciones, resúmenes, extractos, arreglos musicales, compilaciones, antologías, etc.”.

Cabe recordar que, en relación con el derecho de traducción, adaptación, trasformación o, dicho de otra forma, las obras derivadas, serán protegidas en lo que tengan como original, pero sólo podrán ser explotadas cuando hayan sido autorizadas por el titular de los derechos de la obra primigenia o que sirvió de base para realizar la obra derivada (Magaña, 2013, p. 46).

Además, podemos destacar que la vigencia de los derechos patrimoniales es la vida del autor, más cien años (en el caso de México), existen países donde la vigencia varía, pero en ningún motivo puede ser menor a cincuenta años según lo señalado por el Convenio de Berna.

C. Límites y excepciones del derecho de autor

Por otra parte, es generalmente aceptado que, bajo ciertas circunstancias y en determinados casos, exista la necesidad de crear un balance entre los derechos de los autores y el interés general (Valles, 2015, pp. 428 y 429).

Es por eso que, esos derechos patrimoniales están supeditados a las limitaciones que estén expresamente establecidas en el Convenio de Berna, a saber, en la regla de los tres pasos de naturaleza acumulativa, estas son: a) en ciertos casos especiales; b) que no entren en conflicto con la explotación normal de la obra; y c) que no perjudiquen injustificadamente los intereses legítimos del autor; misma que da origen a algunas excepciones o uso justo (*fair use*) en el derecho anglosajón; tales como cita de textos, a la copia privada, la copia de seguridad, la crestomatía, así como la transformación de la obra, para que las personas con discapacidad puedan acceder a ella, mismas que no necesitarán del consentimiento del titular, ni retribuirle económicamente.

La diferencia de ambas tradiciones es que por un lado en el derecho codificado o civil, se prevé un listado concreto y restrictivo de excepciones a los derechos patrimoniales; listado que el legislador construye con base en la prueba de los tres pasos. Por su parte, el régimen del *fair use* en el derecho de los Estados Unidos es un sistema abierto en el que, utilizando determinadas reglas, la procedencia o no de la excepción deberá analizarse caso por caso y su interpretación, en última instancia corresponderá a un juez (Valles, 2015, pp. 428 a 432).

Valles (2015, p. 428) asegura que la *Copyright Law*, proporciona un esquema mucho más abierto y flexible, así como una lista no limitativa de excepciones. Sin embargo, la citada ley establece que para determinar si el uso de una obra se considera como *fair use*, deberá realizarse un análisis caso por caso de los siguientes factores:

a) el propósito y carácter del uso, considerando si este último es de naturaleza comercial o si es para propósitos educativos sin fines de lucro;

b) la naturaleza de la obra protegida;

c) la cantidad y sustancia de la porción utilizada en relación con la totalidad de la obra protegida; y

d) el efecto del uso respecto del mercado potencial o valor de la obra protegida.

Como resultado, se evidencia que tanto las excepciones del derecho codificado o civil y el *fair use* del *copyright* tienen como objetivo salvaguardar la libertad de expresión de los individuos y el derecho del público a la información, lo cual promueve el libre flujo de la información (Valles, 2015, p. 431).

II. El análisis de la doctrina del uso justo (*fair use*) y su extensión a la doctrina del derecho de transformación (*transformative use*) para facilitar la búsqueda de información en Internet

El advenimiento del internet ha creado una verdadera revolución de la información. Sin embargo, con la llegada de los nuevos medios tecnológicos e informáticos de difusión, a través de los cuales se accede a las obras literarias, el contexto inicial en el cual nació el derecho de autor se ha ido modificando, imponiendo nuevos retos (Herrera, 2015, p. 61). Lo que ha provocado la movilización de diversos sectores para proteger sus intereses, lo que ha traído como consecuencia, la destacada participación del juez quien, en última instancia, es el único que puede interpretar la ley, cuando ésta no cuenta con la capacidad de dar respuesta a la controversia.

Por otra parte, los motores de búsqueda son sistemas tecnológicos que permiten al usuario de Internet explorar y acceder a la información. Además, con ellos se facilita la búsqueda sistemática y ordenada de la información. Los argumentos de defensa cuando los motores de búsqueda publican en línea contenidos protegidos, han sido el *fair use*, el uso transformativo (*transformative use*), el derecho de cita y la licencia implícita (Rengifo, 2016, pp. 33 y 34).

Es importante tomar en cuenta que cuando el *fair use* se esgrime como medio de defensa en un litigio, el juez debe analizar los ya mencionados cuatro factores: 1) el propósito del uso de la obra originaria dentro de la obra derivada, teniendo en cuenta si se trata de una sátira o una parodia y si el uso es comercial o no comercial; 2) la naturaleza de la obra, mirando por ejemplo, si es una obra de ficción o si es una obra académica; 3) la cantidad y relevancia de las excertas que han sido tomadas por el trabajo derivado de la obra original; y 4) el criterio de si la obra transformada le quita mercado o valor a la obra original (Rengifo, 2016, p. 36).

Por fortuna, recientemente la jurisprudencia norteamericana elaboró el criterio del *transformative use*, que al parecer ha venido adquiriendo mayor importancia que los otros cuatro mencionados (Rengifo, 2016, pp. 36 y 37). La base de dicho criterio descansa en el "uso creativo", siempre y cuando el propósito de la obra original sea transformado, permitiendo a la vez que se cumplan los objetivos primordiales del derecho de autor: el acceso al conocimiento y la promoción de las artes, la ciencia y la cultura (Herrera, 2015, p. 61).

En este apartado trataremos de analizar la jurisprudencia norteamericana del *fair use* y el *transformative use* aplicado a los motores de búsqueda, se citan a continuación algunos extractos de los casos previamente analizados por el catedrático Rengifo (2016, pp. 37 a 47):

Caso *Kelly vs. Arriba Soft Corp*: El Noveno Circuito señaló que el uso de los motores de búsqueda de los *thumbnails* o imágenes reducidas que se usaban en respuesta a la información requerida era justo en la medida en que las pequeñas versiones de la imagen original no suplantaban la necesidad de ésta; asimismo certificó que los *thumbnails* eran transformativos y que el uso era justo por el *public benefit* que los motores proporcionaban a la sociedad. Es decir, se trataba del mejoramiento del acceso a la información en internet versus la expresión artística. Luego afirmó que sería improbable que alguien hiciese uso de las imágenes reducidas con propósitos estéticos ya que al ampliarse las imágenes perdían claridad (Rengifo, 2016, p. 37). Por tanto, el Noveno Circuito resolvió que no había infracción al derecho de autor, en virtud de que Arriba transformó la obra de Kelly, misma que al descargarse y ampliarse se distorsionaba, por tanto, no podía competir y causar un detrimento a los intereses económicos del autor; por lo cual, pesó más el beneficio social por encima del particular.

Caso *Perfect 10: Perfect 10* es una revista muy similar a Playboy. Google como parte de su servicio de búsqueda de imágenes, hace una reducción de las imágenes, copias en miniatura o *thumbnails* para permitir que vayan direccionadas a un sitio donde el

usuario puede verlas completas. *Perfect 10* demandó a Amazon y a Google por estar reproduciendo ilícitamente las imágenes sobre las cuales tiene *copyright*. El juez consideró que no había violación, puesto que el propósito del uso de las obras había cambiado para convertirse en mecanismos de búsqueda e información. Asimismo, se concluyó que transformando la obra artística en un instrumento de referencia electrónica se proporciona un beneficio a la sociedad (Rengifo, 2016, pp. 38 y 39). En este caso es evidente que el juez tomó por analogía los criterios del anterior caso, donde también el beneficio general prevaleció sobre los intereses del autor.

Caso *Google Books*: En el presente caso, los titulares demandaron a Google por cuanto para ellos el *Library Project* y el *Google Books Project* infringían sus derechos de autor. Google hace y retiene copia de los libros, permite que las bibliotecas descarguen y retengan una copia digital, y facilita que el público busque los textos o los libros digitalmente copiados o reproducidos y pueda ver representaciones de *snippets* del texto (vista recortada o tijereteada de los libros) (Rengifo, 2016, p. 41).

La primera instancia consideró que el *Google Books Program* no constituía un mercado substituto de las obras originales. El juez del Distrito de New York exoneró a Google por cuanto, aún en presencia de reproducción de la obra, su finalidad es la de facilitar la búsqueda de libros por internet. Así, ofrece información de los libros a través de extractos, o *snippets*, los cuales no constituyen un instrumento que suplante al libro, sino un medio que facilita su acceso; por lo tanto, produce un alto beneficio social y no hay violación del *copyright* (Rengifo, 2016, p. 41).

Llegando a este punto, la Corte de Apelaciones sostuvo y dictaminó que la información relacionada con el libro no es monopolio del titular, sino que otro sujeto la puede suministrar. Sin embargo, es sabido, que una obra no se puede digitalizar sin la autorización de su creador. Entonces, ante esta dificultad la Corte diferencia entre la obra derivada, la cual, por supuesto, hace parte de los derechos exclusivos del autor, y distingue por otro lado la información relacionada con la obra original, la cual no se halla dentro del alcance de los derechos exclusivos (Rengifo, 2016, p. 43).

La Corte concluyó que, el propósito de la copia es altamente transformativo; que la exhibición pública del texto es limitada; que las revelaciones no implican un significativo mercado sustituto de los aspectos protegidos de las obras originales, y que la naturaleza comercial y la motivación de ganancia de Google no justifica rechazar la limitación del *fair use* (Rengifo, 2016, p. 47).

Así que, las decisiones de la Corte en el caso de Google han creado un precedente importante, mismos que podría servir de base en posteriores decisiones jurisprudenciales. Algunos especialistas sostienen que posiciones como la asumida en este caso promoverán mayor innovación y creación (Herrera, 2015, p. 82).

III. El juicio de proporcionalidad y la prueba de los tres pasos del Convenio de Berna, para construir una nueva excepción al derecho de autor en México para beneficiar a las instituciones de educación e investigación, las bibliotecas, los museos y los archivos

Una vez estudiado someramente el marco teórico conceptual de los derechos en colisión y el análisis de las doctrinas del *fair use* y *transformative use*, se pasará a la última parte de la investigación, para argumentar a través del juicio de proporcionalidad, si el derecho codificado o civil, específicamente si en el derecho mexicano encuadraría la posibilidad de que las instituciones de educación e investigación, así como las bibliotecas, los museos y los archivos pueden transformar obras, con el objetivo de facilitar la búsqueda amigable y sencilla de la información, ya sea a través de la doctrina del *transformative use* o partes de ésta e inclusive a través del juicio de proporcionalidad y la prueba de los tres pasos del Convenio de Berna.

En la actualidad, el juez se ha convertido en la figura primordial de la interpretación y argumentación creativa para la solución de casos, es decir, la hermenéutica jurídica ha permitido que los jueces no sólo basen sus decisiones en los aspectos lógicos-formales del pensamiento, sino que además permite tomar en cuenta los factores y circunstancias propios del comprender no sólo lingüísticos, sino de las barreras culturales y la distancia entre el texto y la época actual de necesidades y realidades de la sociedad contemporánea (Aguilera y López, 2014, pp. 83 y 84).

Es así que, la proporcionalidad se ha convertido en una herramienta que ya no pertenece únicamente a la labor del juez constitucional, sino que en la actualidad cualquier juez está llamado a cumplir con la ley fundamental (Aguilera y López, 2014, p. 85).

Para reforzar lo antes dicho, por mandato constitucional, el artículo primero de la Constitución Política de los Estados Unidos Mexicanos, en sus párrafos segundo y tercero, contiene la obligación de interpretar las normas en materia de derechos humanos conforme a la Constitución y con los tratados internacionales, favoreciendo la protección más amplia a la persona; también advierte que, “toda autoridad pública”, en el ámbito de sus competencias, están obligadas a promover, respetar, proteger y garantizar los derechos humanos, bajo los principios de universalidad, interdependencia, indivisibilidad y progresividad.

De igual manera, la labor del interprete constitucional se ha constituido al día de hoy como uno de los pilares fundamentales del Estado constitucional democrático, por tanto, el principio de proporcionalidad se ha vuelto un instrumento indispensable para justificar las decisiones judiciales relacionadas con la limitación o restricción de los derechos fundamentales (Aguilera y López, 2014, p. 87).

Al mismo tiempo, resulta importante destacar que Herrara (2015, p. 60) advierte que hay quienes esgrimen que Europa debería acoger la doctrina del *fair use*; abarcando también a los países del derecho codificado o derecho civil, esto es, los países latinoamericanos; lo anterior para darle mayor autonomía interpretativa al juez. A fin de reafirmar el mencionado criterio, la autora cita a Griffiths, mismo que sostiene:

> *“El desarrollo de dicha teoría no solo permitiría aliviar la inflexibilidad de aquellas predominantes corrientes europeas, sino que además, reduciría la ventaja competitiva que tiene Estados Unidos sobre Europa, y además aseguraría un grado de armonización dado el aumento de jurisdicciones que han acogido la doctrina en análisis”.*

En virtud de lo anteriormente narrado y fundado al momento, se pasará al *test* de proporcionalidad, para tratar de encuadrar los supuestos en cada uno de los subprincipios del *test*, es decir, la idoneidad, la necesidad y la proporcionalidad en *strictu sensu*.

El subprincipio de idoneidad o adecuación:

Dicho principio establece que toda intervención a los derechos fundamentales debe tener un fin constitucionalmente legítimo y que ésta sea para favorecer su obtención (Aguilera y López, 2014, p. 89). Asimismo, que la restricción que sufre el derecho resulte realmente útil para justificar el fin perseguido, dicho en sentido negativo, que no sea absolutamente inútil (Perello, s.f., p. 70).

Por consiguiente, a fin de dar cabal cumplimiento a la noble misión de las instituciones de educación e investigación, las bibliotecas, los museos y los archivos, esto es, el convertirse en verdaderos ecosistemas de la información, el aumentar el número de lectores, incentivar la investigación y difundir el conocimiento; resulta importante considerar las ventajas de contar con un sistema digital de búsqueda, amparado en las nuevas tecnologías, con el objeto de facilitar al usuario la investigación; de ahí que, al tener una vista en miniatura de los resultados (*thumbnails*) y con base en ello, se pueda encontrar el libro más rápido, guiándose por la portada, el diseño de la misma, los colores o cualquier otro signo visible que haga identificable la obra del resto, sin duda trae grandes ventajas paralos usuarios.

Además, el poder contar con una vista recortada o tijereteada de los libros (*snippets*), le ayudaría a los usuarios a seleccionar de un mar de opciones, cuáles obras le servirán de base para su investigación y al mismo tiempo sabrá dónde buscarlos o bien, cuando sea el caso, dónde comprarlos. Si se analiza detenidamente el presente párrafo y el anterior, resulta evidente que el usuario se vería altamente beneficiado; pues ahorraría tiempo y dinero considerablemente, sin dejar de lado que la búsqueda de la información también trae como consecuencia, el acceso al conocimiento y a la promoción de las artes, la ciencia y la cultura, sin dejar de lado la toma de decisiones bajo una opinión objetiva, oportuna y veraz.

Al mismo tiempo, a fin de dar cabal cumplimiento a la prueba de los tres pasos del Convenio de Berna y proporcionar mayor peso al argumento vertido, resulta sustancial analizar el primero de los puntos del *test*, que también podrían permitir la intromisión al derecho de autor. Valles (2015, p. 435) advierte que el elemento se refiere a que las excepciones serán únicamente aplicables en “determinados casos especiales”. Por lo cual, la autora añade que en el informe del Grupo Especial de la Organización Mundial del Comercio de junio de 2000 (Grupo Especial), en “determinados” se refiere que:

> *El término significa que, con arreglo a la primera condición, una excepción o limitación prevista en la legislación nación debe estar claramente definida. Sin embargo, no es necesario identificar explícitamente todas y cada una de las situaciones posibles a las que podría aplicarse la excepción siempre que su alcance sea conocido y particularizado. Esto garantiza un grado de suficiente certidumbre jurídica.*

Además, cuando explica el significado de “especiales” establece que:

> *Las excepciones o limitaciones deben ser limitadas en cuanto a su campo de aplicación o excepcionales en su alcance […] una excepción o ilimitación debe ser estricta en sentido cuantitativo y en el cualitativo. Esto sugiere un ámbito reducido, así como un objeto excepcional o característico […].*

Consideramos ahora la importancia de señalar que la excepción o limitación no necesariamente debe estar en la ley de forma expresa, es decir, que el juez en su caso, puede a través de este criterio, pronunciarse a favor de la intromisión, al advertir que dicha intromisión es en beneficio de la sociedad; también hay que recordar que no sólo la ley es fuente del derecho, sino que las resoluciones de otros tribunales, la jurisprudencia o incluso la doctrina pueden fungir como pilares para que el juez pueda sustentar sus determinaciones.

El subprincipio de necesidad:

Este principio señala que toda intervención debe ser la más benigna con el derecho fundamental intervenido, además, implica la comparación adoptada por el legislador y otros medios alternativos (Aguilera y López, 2014, p. 89). Es decir, habrá de optarse por aquella intromisión que implique una menor restricción en la esfera jurídica de los afectados, esto, es que no se imponga un sacrificio claramente innecesario (Perello, s.f., p. 70).

Por consiguiente, la creación de un sistema digital de búsqueda es precisamente para la ubicación de obras, no así para la lectura de las mismas; de lo contrario, habrá que tener cuidado, pues podríamos encuadrar en una causal de infracción. Si bien es cierto, han existido casos como *Sony Corp. of Am. v. Universal City Studios y Bill Graham Archives*, donde las Cortes norteamericanas han determinado que en ciertas ocasiones la copia completa de una obra puede considerarse como un uso justo (Herrera, 2015, p. 66), siempre será recomendable atender al caso particular. Como ejemplo, en el derecho mexicano existe la posibilidad de que las instituciones de educación e investigación, las bibliotecas, los museos y los archivos puedan reproducir la totalidad de la obra, siempre que la misma ya no se halle en el mercado y que exista el riesgo fundado de su posible desaparición por su deterioro natural.

De igual modo, los sistemas digitales de búsqueda se basarán en la información relacionada con la obra original, no así con el derecho exclusivo que tienen los autores de autorizar o prohibir su digitalización; en consecuencia, las obras se convertirían en una herramienta de búsqueda, restricción que resulta la más generosa al derecho de autor. No obstante, las instituciones de educación e investigación, las bibliotecas, los museos y los archivos también pueden ampararse bajo las excepciones que permiten las legislaciones nacionales, como el caso del derecho de cita, la copia privada, la copia de seguridad o cuando la obra se encuentre en el dominio público. Asimismo, para el sustento del citado criterio, resulta importante destacar, que la información relacionada con la obra no puede convertirse en un monopolio del autor, de lo contrario, tal como afirma Herrera (2015, p. 68), se crearía en algunas circunstancias, no expansiones del conocimiento sino limitaciones al mismo.

A fin de dar una mayor argumentación a la intromisión del derecho de autor, y analizar el segundo de los elementos de la prueba de los tres pasos del Convenio de Berna, Valles (2015, p. 436) indica que el segundo elemento establece que “no se debe atentar contra la explotación normal de la obra”. Al respecto, el Informe del Grupo Especial manifiesta que el concepto de explotación: “[…] se refiere […] a la actividad mediante el cual los titulares del derecho de autor utilizan los derechos exclusivos que le han sido conferidos para obtener un valor económico de sus derechos a esas obras […]”.

Por otro lado, en cuanto al concepto de explotación “normal” el Informe del Grupo Especial expone que: “[…] significa evidentemente algo menos que el pleno uso de un derecho exclusivo”.

Derivado de los conceptos antes mencionados, el Grupo Especial concluye que: “[…] se presumirá que las excepciones o limitaciones no atentan contra la explotación normal de las obras si se limitan a un campo o grado de aplicación que no suponga competencia económica con los usos no exentos. Más allá el Grupo Especial infiere que no deberán considerarse únicamente las formas de explotación actualmente conocidas, sino aquellas que, probablemente, pudieran adquirir una importancia considerable económica o práctica. Así, en el contexto de las nuevas tecnologías y el entorno digital, en la medida en que el autor o el titular de derecho vayan adquiriendo control sobre las formas de explotación comercial, las excepciones dejarán de ser procedentes, llegando al punto en el que no resulte viable la aplicación de excepciones en el entorno digital.

Resulta sustancial rescatar del punto anterior, que la intromisión al derecho de autor, es la más benigna, toda vez que no hay un detrimento al derecho de explotación de la obra, pues el sistema digital de búsqueda se basarán en la información relacionada

con la obra original, no así con el derecho exclusivo que tienen los autores de autorizar o prohibir su digitalización con o sin fines de lucro, pues como ya se advirtió en párrafos anteriores, los motores de búsqueda, no tienen como objeto la venta de los libros o bien suplantar la obra original, sino que se limitan a proporcionar secciones tijereteadas o extractos de la misma (*snippets*), para que el usuario pueda determinar si el libro le servirá para su investigación o no; asimismo, los buscadores señalarán, en su caso, dónde el usuario puede comprar el libro, por tanto, tampoco existe una competencia económica.

Se considerando que al tener una vista en miniatura de los resultados (*thumbnails*), tampoco constituiría una violación al derecho de autor, en virtud de como ya se mencionó, las transformaciones no compiten ni estéticamente, ya que al aumentarse se distorsiona, ni tampoco intentan competir económicamente con la obra original, toda vez que su labor es únicamente para buscar información.

Proporcionalidad en sentido estricto (*strictu sensu*):

Este principio obliga a que la intervención debe estar justificada por la importancia de la realización del fin perseguido por la intervención legislativa. Esto significa que las ventajas que se obtienen mediante la intervención legislativa en el derecho fundamental deben compensar los sacrificios que ésta implica para sus titulares y para la sociedad en general (Aguilera y López, 2014, pp. 89 y 90). Es decir, debe comprobarse si existe un equilibrio entre las ventajas y perjuicios; o en todo caso los beneficios y ventajas derivados de la restricción del derecho deben ser siempre superiores a los perjuicios sobre otros bienes o intereses en conflicto.

Como se ha dicho, el transformar una obra en *thumbnails* o *snippets* con el objeto de mejorar el acceso a la información a través de los motores de búsqueda en las instituciones de educación e investigación, las bibliotecas, los museos y los archivos, se proporciona un beneficio social, dicho beneficio social se podría colocar incluso por encima de los derechos del titular para justificar esa reproducción de la imagen en miniatura (*thumbnails*), así como vistas tijereteadas (*snippets*), en virtud de que se está colaborando para promover el conocimiento público (Rengifo, 2016, p. 39).

Resulta importante advertir que, sobre la transformación de la obra, Murray citado por Herrera (2016, p.71) ha sostenido que un determinado uso será transformativo cuando ha habido una modificación sustancial del propósito para el cual fue creada la obra original, y cuyos efectos sean benéficos para el público en general, garantizando así el cumplimiento de los fines primordiales de la doctrina del uso justo. Aunado a ello, se ha afirmado que no es necesario que el contenido o la forma de expresión sean modificados, siempre y cuando las funciones o finalidades de la obra original cambien completamente (Herrera, 2015, p. 71).

En virtud de lo antepuesto, es necesario señalar que transformar las obras con el propósito de proporcionar al público su búsqueda y realizar un diseño que permita su vista en miniatura o bien recortada, constituiría una excepción o *fair use*, en razón de que la exhibición pública del texto sea limitada; que las revelaciones no impliquen un significativo mercado sustituto de los aspectos protegidos de las obras originales; y que en algunos casos la naturaleza comercial y la motivación de la ganancia cuando se trate de instituciones privadas no justifiquen rechazar la limitación del *fair use* (Rengifo, 2016, p. 47).

A su vez, Valles (2015, p. 437) asegura que el tercer elemento en la prueba de los tres pasos del Convenio de Berna, determina que no debe causar un “perjuicio injustificado a los intereses legítimos del autor”. Este último factor, de antemano, presupone que el uso conforme a la excepción podría generar un perjuicio a los intereses legítimos del autor pero que, en ningún momento ese perjuicio debería ser injustificado. Así, el Grupo Especial determina que “[…] el perjuicio de los intereses legítimos de los titulares de derechos llega a un nivel injustificado si una excepción o limitación causa o puede causar una pérdida

de ingresos injustificada al titular del derecho de autor".

La citada autora aprecia que el criterio de determinación del perjuicio es exclusivamente económico, con lo cual pone la balanza en favor de los titulares de los derechos económicos sobre la obra. Sin embargo, a su entender, sería precisamente un interés superior al económico del autor o del titular el que podría inclinar dicha balanza a favor de los usuarios, refiriéndose precisamente al interés público o a los derechos fundamentales que dan origen a determinados tipos de excepciones, tales como la libertad de expresión o el derecho a la información que es el caso que nos ocupa, por lo cual, se puede argumentar válidamente que la intervención podría estar justificada en el interés público, es decir, los beneficios y las ventajas para buscar información son superiores a los intereses económicos de los autores, tal como quedó demostrado en los párrafos anteriores.

IV. Conclusiones

Con base en lo descrito al momento, se puede advertir que es de suma importancia la libertad de expresión, así como sus extensiones, es decir, el derecho a la información y el derecho de acceso a la información pública, lo anterior, para que las personas puedan tomar decisiones en un Estado democrático y plural como lo es el nuestro, o bien para ejercitar otros derechos, como el de la educación, la cultura y el de acceso a la justicia, por citar algunos.

Pero dichas libertades no deben ser entendidas sólo como una acción de no hacer por parte de los gobiernos en turno de los Estados, sino que dichos Estados deben entablar acciones tendientes a la discusión de las ideas y la información.

Se debe garantizar que la información tenga cierta calidad o veracidad, debe ser prestada de tal suerte que cualquier persona de a pie pueda buscarla, recibirla o difundirla de una forma sencilla, accesible y amigable.

Por suerte, las nuevas tecnologías de información y la comunicación han creado una serie de herramientas a través de las cuelas es más fácil y sencillo acceder y difundir las ideas, así como la información por cualquier medio de expresión. Empero, en algunas ocasiones es complicado entregarla en formatos amigables. Es más, las leyes de transparencia, por ejemplo, exentan de toda obligación de procesar o transformar la información, por lo tanto, cabe la posibilidad de entregarse como se encuentra.

Es de reconocer que algunos tribunales y órganos encargados de administrar justicia han comenzado por emitir sus sentencias en formatos amigables, es decir, adjunta a la resolución se antepone una infografía.

Empero, la cuestión se complica cuando el documento está protegido por derecho de autor y se entra en una encrucijada, de poner a disposición del público la obra de una forma más amigable.

Por lo tanto, se pretende que únicamente las instituciones de educación e investigación, las bibliotecas, los museos y los archivos (con independencia de su naturaleza, es decir, si son públicos o privados), puedan transformar las obras que poseen, para ser puestas a disposición de los usuarios de una forma amigable, accesible y sencilla.

Recordemos que las citadas instituciones son ecosistemas de la información, que tienen una noble labor de difundir sus acervos, para que puedan ser consultados por los usuarios, mismos que probablemente se convertirán en autores y así continuaría el ciclo.

Hay que mencionar que el desafío a resolver es la adaptación de la teoría del *fair use* al derecho codificado o al derecho civil, principalmente por los operadores del poder judicial. Por fortuna, Herrera (2015) asegura que en un contexto de globalización como el actual, los efectos de una determinada decisión repercuten inmediatamente en los desarrollos jurídicos de otras latitudes, y esto sucede con mayor razón respecto de Estados Unidos, la economía líder mundial, es decir, que los criterios dictados por los tribunales estadounidenses pueden servir de base para que los jueces latinoamericanos comiencen a dar respuesta a los casos concretos que se les presenten.

Cabe señalar que los jueces, al ser una autoridad pública, están obligados a resolver los casos que se les presenten con base a los principios que el artículo primero de la Constitución General de la Republica les manda. En virtud de lo anterior, se puede comenzar a crear criterios jurisprudenciales, que con el tiempo adquieran el carácter de obligatorios, tomando como antecedentes los casos de la jurisprudencia del *transformative use*, sin necesidad de copiar el sistema de excepciones del *copyright*.

También hay que recordar que no es la primera vez en donde los sistemas anglosajones y el codificado o civil se complementan. Como ejemplos de lo analizado, tenemos el caso del *safe harbor*, figura que se utiliza tanto en el *copyright* en los Estados Unidos como en el derecho de protección de datos personales en Europa. Sin dejar de lado los juicios orales en Latinoamérica, donde el sistema acusatorio adversarial de los Estados Unidos vino a reemplazar el sistema inquisitivo (que con independencia de si funcionan o no, ya se está aplicando).

Por otro lado resulta importante destacar los retos que les imponen a los legisladores o en su caso a los jueces, las nuevas tecnologías y los progresos del Internet en las ciencias jurídicas. Por tanto, es sumamente necesario que los derechos en colisión se resuelvan de manera armónica y a falta de esta, se solucione a través de un juicio de proporcionalidad, con el objeto de dar respuesta a los casos que se presentan.

Habría que decir también que las instituciones de educación e investigación, las bibliotecas, los museos y los archivos, en ningún momento buscar violentar los derechos de los autores, sino que dichas instituciones buscan más y mejores excepciones para cumplir su tarea. Aunado a lo anterior, debemos destacar que ambos, es decir, las instituciones y los usuarios, se necesitan, o sea, los autores requieren de dichas instituciones para poder generar sus obras, convirtiéndose en usuarios y las instituciones necesitan de las obras de los autores para difundir el conocimiento, la información, fomentar la investigación y la promoción de las artes, la ciencia y la cultura.

Por lo tanto, es significativo considerar las ventajas de contar con un sistema digital de búsqueda en las citadas instituciones, con el objeto de facilitar al usuario la investigación y la búsqueda de información; pues resultaría de gran ayuda seleccionar de un mar de opciones, cuáles obras le servirán de base para su investigación y al mismo tiempo sabrá dónde buscarlos o bien, cuando sea el caso, dónde comprarlos.

Finalmente, recordar que en el derecho norteamericano hacer una copia exacta de una creación precedente es transformativo en la medida en que la copia tiene una función diferente a la obra original y las imágenes reducidas no son mercados sustitutos de las imágenes originales (Rengifo, 2016). En Mé-

xico se puede hacer uso de la obra, no como un derecho transformativo, sino a través de una excepción como la copia privada o con fines de preservación. Sin embargo, estás excepciones no alcanzan a cubrir las necesidad más importantes de las instituciones de educación e investigación.

Rafael Ríos Nuño

Abogado y maestro en Transparencia y Protección de Datos Personales por la Universidad de Guadalajara (UdeG), maestro en Propiedad Industrial, Derechos de Autor y Nuevas Tecnologías por la Universidad Panamericana, egresado de la Especialidad en Gestión, Publicación y Protección de Información por el ITEI.

Jefe de Apoyo Técnico en la Unidad de Transparencia de la UdeG. Presidente fundador del Instituto Autónomo de Occidente y de su Centro de Derecho Corporativo, Derechos Humanos y Paz.

V. Bibliografía

ACKERMAN, J. Y SANDOVAL, I. (2015). *Leyes de Acceso a la Información en el Mundo.* Cuadernos de Transparencia. Vol. 07. México: INAI.

AGUILAR J. (2008). *Transparencia y democracia: claves para un concierto.* En: Cuadernos de Transparencia Vol. 10. México: INAI.

AGUILERA R. Y LÓPEZ R. (2014). *El principio de proporcionalidad en la jurisprudencia mexicana (Límites y restricciones a los derechos fundamentales).* México: Instituto de investigaciones jurídicas de la UNAM.

ALBERCH, R. (2008). *Archivos y derechos Humanos.* España: TREA.

ALEXY, R. (2007). *Derechos sociales y ponderación.* México-España: Fontamara.

APARICIO, J. Y BATUESCAS A. (s.f.) *Preguntas frecuentes sobre derecho de autor.* Universidad de Salamanca, España.

ARAUJO, E. (2009). *El derecho a la Información y a la protección de datos personales en México.* México: Porrúa.

ARIAS, F. (2012). *Estudios de Propiedad Intelectual.* Colombia: Universidad Santo Tomás.

CENDEJAS, M. (2007). *Evolución histórica del derecho a la información.* Revista de Derecho Comparado de la Información, número 10, Julio – Diciembre 2007. México: Instituto de Investigaciones Jurídicas de la UNAM.

CENDEJAS, M. (2010). *Derecho a la Información. Delimitación conceptual.* En derecho comparado de la información. México: Instituto de Investigaciones Jurídicas de la UNAM.

CORREDOIRA, L. (2012). *La protección del talento. Propiedad intelectual de autores, artistas y productores con especial atención a internet y obras digitales.* España: Tirant lo Blanch.

CRUZ, O. (2011). *Antecedentes Jurídicos de la Transparencia en México. Revista de Derecho Comparado de la Información,* número 17, Enero – Junio 2011. México: Instituto de Investigaciones Jurídicas de la UNAM.

DE LA PARRA, E. (2015a). *Derechos Humanos y Derechos de Autor. Las restricciones al derecho de explotación.* México: Instituto de Investigaciones Jurídicas de la UNAM.

DE LA PARRA, E. (2015b). *Libertad de expresión y acceso a la información. Colección de textos sobre derechos humanos.* México: Comisión Nacional de los Derechos Humanos.

FLORES, M. (2009). *Diccionario de Derechos Humanos.* México: FLACSO.

GARCÍA, P. (2014). *Derechos y libertades, internet y tics.* Valencia: Tirant lo Blanch.

GÓMEZ, A. (2007). *Definiciones básicas sobre la transparencia y el acceso a la información pública.* En: Acceso a la Información: Un derecho de avanzada en Jalisco. México: ITEI.

GÓMEZ, P. (2012). *Derecho a la información, reflexiones contemporáneas.* México: Universidad Autónoma Metropolitana.

HERNÁNDEZ, M. Y ALVAREZ J. (2015). *La transparencia y el derecho de acceso a la información en México.* México: Tirant lo Blanch.

HERRERA, L. (2015). *La doctrina del fair use frente a los retos impuestos por el entorno digital. Estudio del caso Google Books.* Revista La Propiedad Intelectual n°, 20. Universidad Externado de Colombia, julio-diciembre 2015.

HIDALGO, A. (2013). *Derecho Informático.* México: Flores editor y distribuidor.

INSTITUTO DE TRASPARENCIA, INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE JALISCO (2007). *Acceso a la Información: Un derecho de avanzada en Jalisco.* México: ITEI-ITESO.

JIMÉNEZ, J. (1999). *Derechos Fundamentales: Concepto y Garantías.* España: Trotta.

KUBLI-GARCÍA F. (2010). *El Principio de máxima publicidad.* En: Homenaje al Doctor Emilio O. Rabasa, 2 Ejemplares, Coedición con: UNAM, Facultad de Derecho, 2010. México: UNAM.

LATHROP, D. Y RUMA, L. (2010). *Open Government: Collaboration, Transparency and Participation in practice.* Sebastopol: O'Really Media.

LIMA, M. (2010). *Museos y propiedad intelectual.* Los desafíos de la digitalización de contenidos. Argentina: FLACSO-Sede Académica Argentina.

MAGAÑA, J. (2013). *Curso de derechos de autor en México.* México: Novum.

MAGAÑA, J. (2015). *Estudios en materia de propiedad intelectual.* México: Novum.

MENDEL, T. (2008). *Libertad de Información: Comparación Jurídica.* Segunda Edición. París: Unesco.

OMPI (2017). Apuntes del Curso DL-201 Sobre Derecho de Autor y Derechos Conexos de 2017.

PABÓN, J. (2006). *Hipertexto, links y derecho de autor.* Revista de derecho informático. Perú.

PAHUAMBA, B. (2016). *El derecho humano a la rendición de cuentas objetiva y el uso debido de los recursos públicos.* México: Express.

PERELLO, I. (s.f.). *El principio de proporcionalidad y la jurisprudencia constitucional.* Madrid: Asociación Pro Derechos Humanos de España.

RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN (2006), *El Derecho de Acceso a la Información en el marco jurídico americano.* Comisión Interamericana de los Derechos Humanos.

RENGIFO, E. (2016). *Derechos de Autor de las obras reproducidas y publicadas en línea por los motores de búsqueda.* Revista La Propiedad Intelectual n°, 22. Universidad Externado de Colombia, julio-diciembre 2016. Madrid: Asociación Pro Derechos Humanos.

RODRÍGUEZ, J. (2008). *Estado y Transparencia: un paseo por la filosofía política.* Cuadernos de transparencia, número 4, Quinta Edición. México: IFAI.

ROGEL, C Y SERRANO, E. (2013). *Tensiones y conflictos sobre derecho de autor en el siglo XXI.* Materiales para la reforma de la Ley de la propiedad intelectual. México-España: Fontamara.

ROGEL, C. Y SERRANO, E. (2008). *Manual de derecho de autor. Colección de Propiedad Intelectual.* España: Reus.

SALAZAR, P. Y VÁSQUEZ, P. (2008). *La reforma al artículo 6o. De la Constitución mexicana: contexto normativo y alcance interpretativo.* En Salazar Ugarte, Pedro, Coordinador, *El Derecho de Acceso a la Información en la Constitución Mexicana: razones, significados y consecuencias.* México: Instituto de Investigaciones Jurídicas de la UNAM.

SOLORIO, O. (2007). *Derechos de autor para universitarios.* México: Universidad de Colima.

TACTUK, A. (2009). *Tesis Doctoral: El derecho de transformación. Especial referencia a la parodia.* España: Facultad de Ciencias Sociales y Jurídicas de la Universidad Carlos III de Madrid.

UGALDE, L. (2001). *La Rendición de Cuentas en los Gobiernos Estatales y Municipales.* Serie Cultura de la Rendición de Cuentas. México: Auditoría Superior de la Federación.

VALLES, A. en MAGAÑA, J. (2015). *Estudios en materia de propiedad intelectual.* México: Novum. Excepciones a los derechos patrimoniales de autor y sus implicaciones en el entorno digital.

VILLANUEVA, E. (2006). *Derecho de la información.* México: Miguel Ángel Porrúa-Universidad de Guadalajara.

VILLANUEVA, E. (2009). *Diccionario de Derecho a la información.* México: Porrúa.

VUELVAS, M. (2015). *Letras libres vs. La Jornada: la libertad de expresión ante los tribunales.* México: Universidad de Colima.

ZEA, G. (2009). *Derechos de autor y Derechos Conexos. Ensayos.* Colombia: Universidad Externado de Colombia.

Legislación

Código Civil Federal. Diario Oficial de la Federación, México, Distrito Federal, 26 de mayo, 14 de julio, 3 y 31 de agosto de 1928.

Código Nacional de Procedimientos Penales. Diario Oficial de la Federación, México, Distrito Federal, 05 de marzo de 2014.

Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación, México, Distrito Federal, 05 de febrero de 1917.

Convención Americana sobre Derechos Humanos. San José, Costa Rica del 07 al 22 de noviembre de 1969.

Convención Interamericana sobre el Derecho de Autor en Obras Literarias, Científicas y Artísticas, Diario Oficial de la Federación, México, Distrito Federal, 24 de octubre de 1947.

Convenio de Berna para la Protección de las Obras Literarias y Artísticas del 09 de septiembre de 1886.

Declaración Americana de los Derechos y Deberes del Hombre. Adoptada en la IX Conferencia Internacional Americana en Bogotá, Colombia, 1948.

Declaración Universal de los Derechos Humanos. Resolución 217 A (III) de la Asamblea General de las Naciones Unidas. París, Francia. 10 de diciembre de 1948.

Ley Federal del Derecho de Autor. Diario Oficial de la Federación, México, Distrito Federal, 24 de diciembre de 1996.

Ley General de Contabilidad Gubernamental. Diario Oficial de la Federación, México, Distrito Federal, 31 de diciembre de 2008.

Ley General de Transparencia y Acceso a la Información Pública. Diario Oficial de la Federación, México, Distrito Federal, 04 de mayo de 2015.

Ley General del Sistema Nacional Anticorrupción. Diario Oficial de la Federación, México, Distrito Federal, 18 de julio de 2016.

Protocolo Adicional a la Convención Americana sobre Derecho Humanos en Materia de Derechos Económicos, Sociales y Culturales “Protocolo de San Salvador”. Diario Oficial de la Federación, México, Distrito Federal, 01 de septiembre de 1998.

Fotografía: Worawut para Adobe Stock

La importancia de la regulación de las redes sociales digitales en un estado democrático

Salvador Romero Espinosa
Comisionado Ciudadano del ITEI

Resumen

El impacto social, cultural, mediático, económico, legal y político-electoral de las redes sociales digitales es cada día mayor en México (y en todo el Mundo) y sigue creciendo exponencialmente. Dicho impacto y crecimiento se ha presentado en un periodo de tiempo excesivamente breve (apenas poco más de una década) y casi totalmente al margen de las leyes mexicanas, incluidas las electorales, las de comunicación social, las de transparencia y de derecho a la información, así como las de protección de datos personales, que se han quedado "pasmadas" ante la complejidad que dicha regulación representa, dejando en manos de los juzgadores y de los organismos garantes de transparencia, la labor de definir y delimitar los alcances y restricciones de su uso por parte de autoridades y funcionarios públicos.

Por ende, considero que nos encontramos ante una coyuntura tecnológica histórica, que hace impostergable que desde el Poder Legislativo (Federal y el de cada una de las entidades federativas) se realicen las reformas y adecuaciones normativas necesarias para evitar que estas lagunas legales en materia de redes sociales digitales, puedan pervertir el uso político-electoral y propagandístico de dichas herramientas de comunicación tan poderosas, en posible violación al artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, así como generar restricciones al derecho a la información pública y a la libertad de expresión, en perjuicio del artículo 6 de la referida Carta Magna, o incluso permitir o fomentar violaciones al derecho a la privacidad en perjuicio del artículo 16 de la Constitución.

PALABRAS CLAVES:
Redes Sociales, Internet, Democracia, Información Pública

I. Algunos antecedentes

Aunque posiblemente existan cientos o miles de antecedentes sobre el impacto de las redes sociales en la gestión pública, la difusión de información pública y la propaganda electoral, únicamente señalaré aquellos que considero más representativos para acreditar la necesidad del análisis profundo y serio que estamos obligados a realizar como país, para regular el uso y manejo de las redes sociales con el fin de fortalecer nuestra democracia.

El objetivo de este listado no es ser exhaustivo, por supuesto, sino que además de presentar un contexto sobre la materia, generar en el lector una inquietud, curiosidad o incluso preocupación sobre los posibles alcances y riesgos que actualmente existen por la falta de regulación de este tema.

I. a. Difusión en redes sociales de información calumniosa.

En el mes de octubre del año dos mil catorce, un alto funcionario del gobierno estatal de Querétaro, difundió desde sus cuentas personales de redes sociales ("Twitter" y "Facebook"), un supuesto comunicado de la Procuraduría General de la República en el que se imputaban delitos y vínculos con el crimen organizado a un diputado federal de dicha entidad. Éste último interpuso una queja en contra del referido funcionario estatal, argumentando que se estaba violentando la ley electoral que prohíbe a los servidores públicos utilizar indebidamente recursos públicos para favorecer o perjudicar a un candidato o partido político dentro de un proceso electoral.

El denunciado, señaló que era falso que hubiera desviado recursos públicos, toda vez que la información la había compartido desde sus "cuentas personales" y además lo había realizado en un día inhábil (sábado) por lo que era evidente para él que no existía ninguna irregularidad en su actuar.

I. b. El uso de "bots" para favorecer o desvanecer tendencias.

El día diecisiete de marzo del año dos mil quince, el portal de noticias británico BBC, dio a conocer un fenómeno que se había presentado el día anterior en la red social "Twitter" (Najar 2015), en el cual había aparecido un "hashtag" (#endíadepuente) aparentemente inducido desde miles de cuentas de redes sociales denominadas como "bots", para reducir la atención a otro tema de interés recurrente (*trending topic*) relacionado con el aparente despido injustificado de una renombrada periodista mexicana (#EnDefensadeAristegui2).

Aunque desde antes de ese acontecimiento ya habían existido menciones y denuncias por el uso de "bots" para favorecer al presidente de la República Mexicana (bautizados popularmente como "peñabots"), fue a partir de 2015 que crecieron los señalamientos y se realizaron investigaciones objetivas y documentadas que aseguraban que existían y que costaban una importante cantidad de dinero cuyo origen cierto era desconocido (Villanueva 2016). Incluso, en el año 2016, un "hacker" colombiano sentenciado a 10 años de prisión, de nombre Andrés Sepúlveda, habría reconocido haber manipulado las redes sociales mexicanas en el proceso electoral del año 2012 (Buentello 2017).

I. c. La renuncia de un edil por culpa de un "tweet".

En el mes de junio del año dos mil quince, apenas unas horas antes de que tomara el cargo una nueva administración municipal encabezada por la alcaldesa de "Ahora Madrid", se dieron a conocer una serie de antiguos tweets publicados por quien había sido anunciado como el Concejal de Cultura de la ciudad, en uno de los cuales, concretamente, realizó un chiste cruel de judíos (Olaya 2015).

Quienes sacaron a la luz estos "tweets", tuvieron que buscar entre alrededor de 50,000 mensajes publicados por dicho personaje, hasta encontrar dos o

tres tweets -publicados cuatro o cinco años antes de la elección-, para exhibirlo públicamente y posteriormente, en un par de días de acusaciones masivas, orillarlo a renunciar al cargo al que había sido electo. Ninguna explicación sobre la razón, origen y contexto de los "tweets" bastó para evitar su "sacrificio".

I. d. Proselitismo en redes sociales por parte de personajes públicos.

En el año dos mil quince, durante el periodo de veda electoral[1] en México, entre los días cuatro y siete de junio, al menos cuarenta y dos personajes públicos de amplio reconocimiento -y número de seguidores- por la naturaleza de sus diferentes trayectorias profesionales (artistas, cantantes, deportistas, conductores, comediantes, etc.), expresaron en sus cuentas públicas de la red social "Twitter", un apoyo claro, directo, sistemático y manifiesto a favor del Partido Verde Ecologista.

Dichas muestras de apoyo se tradujeron en diversas denuncias en contra de dichos personajes y del partido político al que beneficiaban esas muestras de apoyo "digitales", argumentándose que éstas no podían considerarse como ejercicios aislados de la libertad de expresión, sino como propaganda electoral tendiente a influir al electorado en un momento de prohibición; acusación que fue negada desde luego por dichos personajes públicos, quienes dijeron hacerlo en ejercicio genuino de su libertad de expresión.

I. e. La ruptura entre un fiscal y un alcalde en Jalisco.

En el mes de febrero del año dos mil diecisiete, un par de mensajes hechos desde la cuenta personal de "Twitter" del Fiscal General del Estado de Jalisco, en los cuales se criticaba de manera directa y con alusiones a cuestiones de la vida personal del entonces Alcalde de Guadalajara, llevó a que éste último acusara al fiscal de orquestar una campaña oficial en su contra y la de su familia, y a declarar que no era posible volver a tener una relación institucional con él.

Por su parte, el fiscal declaró posteriormente que él no había escrito esos mensajes y que los atribuía a que su cuenta personal había sido "hackeada", o en su defecto, su contraseña había caído en manos de una persona no autorizada.

I. f. La orden de desbloqueo a un ciudadano por parte de un alcalde en Sonora.

En agosto del año dos mil diecisiete, un ciudadano interpuso un juicio de amparo en contra del alcalde del municipio de Nogales, Sonora, debido al bloqueo que había sufrido en la red social "Twitter" por parte de dicho funcionario público. El agravio principal consistió en que al impedirse al ciudadano "seguir" dicha cuenta, se vulneraba en su perjuicio su derecho constitucional de acceso a la información pública por el tipo de información que en ella se publicaba. También señaló que se violaba su libertad de expresión y se constituía como un acto de discriminación.

El alcalde alegó en su defensa que no se trataba de un acto de autoridad, toda vez que la cuenta de "Twitter" era de naturaleza personal (no se trataba de una cuenta oficial del Ayuntamiento que presidía, ni del cargo que ostentaba) y que por lo tanto, el bloqueo no podía ser considerado ni acto de autoridad, ni mucho menos una violación a algún derecho constitucional o humano del quejoso.

I. g. Solicitud de los nombres de usuario de las cuentas de redes sociales.

En los meses de noviembre y diciembre del año dos mil diecisiete, en diversas resoluciones emitidas por el organismo garante en materia de transparencia del estado de Jalisco (ITEI 2017), se resolvieron una serie de recursos de revisión derivados de sendas

[1] Es el periodo de tres días previos a la elección, más el día de la jornada electoral, en que el derecho electoral mexicano prohíbe realizar actos de proselitismo.

solicitudes de acceso a información pública. En dichas solicitudes se pidió a diversos ayuntamientos y al Poder Legislativo, ambos del Estado de Jalisco, se informara cuáles eran las cuentas de redes sociales "oficiales" de los ediles y legisladores de dichos sujetos obligados, habiendo sido éstos omisos en entregar -total o parcialmente-, esa información.

Los argumentos para negarla, básicamente consistían en que dichos funcionarios públicos de elección no tenían cuentas de redes sociales "oficiales" o pagadas con recursos públicos, mientras que por otra parte, el Instituto de Transparencia Jalisciense consideró que se debió valorar tanto la naturaleza de las cuentas de las redes sociales de dichos funcionarios como la información que en ellas se vertía cotidianamente para efecto de poder determinar si dicho dato –el nombre de usuario de la cuenta- se constituía o no como información pública.

I. h. Uso electoral de información personal obtenida de las redes sociales.

En el mes de marzo del dos mil dieciocho, el medio de comunicación "New York Times" dio a conocer en un reportaje periodístico, que los asesores políticos de la campaña del Presidente de los Estados Unidos de Norteamérica utilizaron información y datos personales de más de 50 millones de usuarios de Facebook, de manera aparentemente ilícita, para influir o al menos tratar de influir, en el sentido de su voto (Rosenberg 2018).

Aunque han existido réplicas y contra-réplicas sobre el tema, al parecer es un hecho que la empresa "Cambridge Analytica" logró efectivamente tener acceso a dicha información personal, a través de la publicitación de "tests" o cuestionarios dirigidos a los usuarios de "Facebook", quienes al participar en dichos ejercicios autorizaban a que el administrador o realizador de los mismos tuviera acceso a sus datos personales para "propósitos académicos". Sin embargo, una vez en posesión de dicha información personal, la misma fue utilizada para elaborar "perfiles digitales" de dichos usuarios, para poder determinar sus preferencias electorales y de esa forma poder dirigir campañas personalizadas para inclinar su preferencia por uno de los dos candidatos a la presidencia norteamericana.

I. i. La orden de desbloqueo a un ciudadano por parte del Presidente de los Estados Unidos de Norteamérica.

El día veintitrés de mayo de dos mil dieciocho, un juzgado de distrito del Estado de Nueva York, ordenó al presidente de los Estados Unidos de Norteamérica, el desbloqueo de un ciudadano de su cuenta personal de Twitter, considerando que dicha cuenta, a pesar de haber sido abierta originalmente como "personal", se constituía como un foro público de expresión del titular del Ejecutivo, y que por tanto, cualquier impedimento a un ciudadano para pronunciar su opinión respecto a las cuestiones que desde dicha cuenta se publicaban, era una violación a la Primera Enmienda de la Constitución Norteamericana, en materia de libertad de expresión.

I. j. Gasto sin control en redes sociales.

Apenas el pasado mes de agosto de dos mil dieciocho, el portal de Internet de noticias "Sin embargo" (Ojeda 2018), dio a conocer que producto de una investigación realizada en el portal de Internet del Sistema de Gastos de Comunicación Social (Comsoc), descubrió que el gobierno del Presidente de México (2012-2018), había gastado cuando menos $2,758,000,000.00 (Dos mil setecientos cincuenta y ocho millones de pesos 00/100 M.N.) en Internet y redes sociales, con el objeto de difundir su imagen y el trabajo de su administración.

Dicha nota periodística señala que la totalidad y los detalles de los servicios, proveedores y costos de estos materiales aún permanece en la opacidad, pero que existe evidencia de que las redes sociales del titular del Ejecutivo buscaron promover su imagen en todas las plataformas posibles, ya que además de las

más populares como “Facebook” y “Twitter”, también existía evidencia de que incursionaron en Pinterest, Google+ e incluso SnapChat.

I. k. Políticas para la difusión de información pública mediante redes sociales digitales.

El día pasado mes de junio de 2019 se aprobó por el Consejo Nacional del Sistema Nacional de Transparencia, Información Pública y Protección de Datos Personales, el proyecto aprobado el cuatro de marzo por las comisiones Jurídica, de Criterios y Resoluciones, y de Vinculación, Difusión, Promoción y Comunicación Social de dicho Sistema, de “Políticas Generales para la difusión de información pública mediante las redes sociales digitales”, las cuales se constituyen como un código de buenas prácticas en materia del uso de redes sociales digitales por parte de autoridades y servidores públicos, y por consecuencia, en el primer cuerpo materialmente normativo que aborda el tema en México.

I. l. La ratificación de la orden de desbloqueo en la cuenta personal de un servidor público a un ciudadano, por parte de la Suprema Corte de Justicia de la Nación.

El día veinte de marzo de dos mil diecinueve la Segunda Sala de la Suprema Corte de Justicia de la Nación, ratificó el criterio sostenido en el año 2017 por el juez de distrito en Sonora, y rechazó la revisión interpuesta por el Fiscal General del Estado de Veracruz, en contra de la orden de un juez de distrito de dicha entidad, que le ordenó el desbloqueo de un ciudadano de su cuenta personal de Twitter. En la resolución se argumentó que dicho bloqueo constituía una restricción de acceso a información de interés público, toda vez que el referido funcionario sí publicaba información directamente derivada del ejercicio de su encargo y del cumplimiento de sus funciones y atribuciones, y que por consecuencia esa restricción era en perjuicio del derecho humano de acceso a la información previsto en el artículo 6 de la Carta Magna.

II. Los principales problemas

En este apartado, tomando como punto de partida los antecedentes existentes, vamos a tratar de delimitar cuáles son los problemas que consideramos más importantes producto de la falta de regulación legislativa relacionada con el uso de las redes sociales por parte de autoridades, servidores públicos y actores políticos.

Como premisa natural cabe señalar que las redes sociales digitales son básicamente una extensión del Internet. En otras palabras, si el Internet es el género, las redes sociales vendrían a ser una especie, al igual que el correo electrónico o muchas de las aplicaciones y juegos que funcionan exclusivamente con acceso a Internet. De acuerdo al diccionario en línea de la editorial “Merriam-Webster” una red social (*social network*) es: *“Un servicio en línea o portal a través del cual la gente puede crear y mantener relaciones interpersonales.”*[2]. Por su parte, las “Políticas para la difusión de información pública mediante redes sociales digitales” aprobadas por el Consejo del Sistema Nacional de Transparencia las definen de la siguiente manera: *“Son portales y/o plataformas de Internet, formadas por comunidades de individuos o personas (físicas y/o jurídicas), en las que se permite el contacto o la interacción entre éstos, de manera que se puedan comunicar y/o intercambiar información digital, también conocidas como redes sociodigitales.”*

II. a. ¿Qué debemos entender por “oficial”?

A diferencia de los portales de Internet (dominios), los correos electrónicos, las computadoras, los teléfonos, los vehículos, las armas, bienes inmuebles, etc., en los cuales es muy fácil delimitar el carácter de “oficial” atendiendo al “dueño” de los mismos, en las redes sociales tradicionalmente no se reconoce como tal a un “dueño” de la cuenta, pues en todo caso a quienes “abren” y utilizan una cuenta se les considera como

[2] Traducción libre de: *“an online service or site through which people create and maintain interpersonal relationships.”*

"usuarios" y el único requisito que se les impone es que acepten los términos y condiciones del servicio de dicha red social y cumplan los mismos.

En el caso de los portales de Internet, por ejemplo, existe una entidad que se encarga de verificar la identidad de aquellos administradores de un dominio determinado con extensión oficial ".gob.mx" (e.g. www.te.gob.mx) de tal forma que se garantice que el contenido y la información que se publique en dichos portales, efectivamente tenga origen en una o más personas debidamente legitimadas para "subirla" al sitio correspondiente. En ese sentido, si una sentencia o la convocatoria a un concurso de ensayo es publicada en el portal www.te.gob.mx, cualquier persona que descargue de ahí dichos documentos, parte de una presunción de que dicha sentencia o convocatoria sí corresponde con un documento aprobado por alguna de las instancias competentes del Tribunal Electoral del Poder Judicial de la Federación, y no corresponde a un documento apócrifo elaborado y cargado por alguna otra persona ajena a dicho tribunal.

Lo mismo sucede con los correos electrónicos de una entidad pública y sus trabajadores, toda vez que existe un administrador de los mismos, que se encarga de asignarlos, modificarlos o eliminarlos, previa acreditación de que la persona que se encargará de utilizarlos (el usuario final), se trate de un servidor público de la dependencia (e.g. otaloramalassisj@te.gob.mx) o bien, labore en el área correspondiente a dicho correo electrónico, cuando éste no sea personal sino de algún área de la institución (e.g. ensayos.transparencia@te.gob.mx), con lo cual nuevamente se le otorga certeza a la ciudadanía sobre la validez de dichas direcciones electrónicas, como instrumento de contacto con los servidores públicos o dependencias de gobierno correspondientes.

En otras palabras, es muy claro que cuando un servidor público administra, crea, genera o utiliza una dirección de correo electrónico o un portal de Internet con extensión ".gob.mx", lo hace precisamente en su carácter de servidor público. Por ello, tanto el portal como las cuentas de correo electrónico con dicha extensión se definen como "oficiales" porque se tiene certeza plena del "dueño" o titular de las mismas, y porque existe una autoridad responsable de vigilar su utilización, aunado a que toda la información que se publica o genera desde ellas tiene la presunción –salvo prueba en contrario- de ser "información pública" según lo ha señalado el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI); de manera opuesta a la ambigüedad que existe con el uso, administración, manejo y naturaleza de la información publicada en las redes sociales digitales, según veremos más adelante.

II. b. ¿Cómo generar una "cuenta oficial" de redes sociales?

Las cuentas de redes sociales no son creadas ni vigiladas directamente por los servidores públicos que las "abren", sino que siguen siendo "propiedad" de la empresa propietaria de la red social correspondiente. De acuerdo con los términos y condiciones del servicio de "Twitter" (TWITTER, 2018), por ejemplo:

1. Quién puede hacer uso de los Servicios

Puede hacer uso de los Servicios solo si accede a firmar un contrato vinculante con Twitter y no es usted una persona vetada para hacer uso de los servicios de conformidad con la legislación de su jurisdicción aplicable. En cualquier caso, usted deberá tener al menos 13 años, o 16 años en el caso de Periscope, para hacer uso de los Servicios. Si acepta estos Términos y usa los Servicios en nombre de una empresa, organización, gobierno u otra entidad jurídica, afirma y garantiza que está autorizado a hacerlo y cuenta con los poderes necesarios para obligarla al cumplimiento de estos Términos, en cuyo caso el uso de las palabras "usted", "su" y "sus" en estos Términos hará referencia a dicha entidad jurídica."

En ese sentido, si bien es cierto que quien abre una cuenta asume la responsabilidad de ser quien dice ser y/o de representar a quien dice representar, en términos prácticos no se tiene conocimiento de que la empresa realice verificaciones adicionales a la

validez del correo electrónico o número telefónico que se vincula con cada cuenta que es creada.

Así las cosas, actualmente es imposible que una cuenta de redes sociales, al menos de aquellas más populares como "Facebook", "Twitter", "Instagram" o "Youtube", pueda cumplir con los requisitos tradicionales para ser considerada "oficial", que se señalaron en el apartado inmediato anterior, al referirnos a los portales y correos electrónicos oficiales, y que se pueden sintetizar así:

1. Que sean utilizadas exclusivamente por servidores públicos en el ejercicio de sus funciones;

2. Que una autoridad pública se encargue de validar que así sea;

3. Que ningún ciudadano pueda crear una cuenta que haga referencia a alguna autoridad sin antes haber acreditado que está legitimado para hacerlo por el cargo que ostenta; y

4. Que la población tenga certeza plena de que la información que consulta o recibe de una red social es información fidedigna de naturaleza pública.

Es verdad que existen en muchas redes sociales procesos de verificación de la cuenta, pero dicha verificación está sujeta a restricciones ajenas a las dependencias de gobierno o al servidor público, por lo que no existe un proceso de verificación gubernamental que le pueda dar plena certeza al ciudadano de si se trata o no, verdaderamente, de una cuenta "oficial".

Retomando a la empresa "Twitter" (TWITTER, 2018), por ejemplo:

> *"¿Qué tipos de cuentas se verifican?*
>
> *Una cuenta se puede verificar si se determina que es de interés público. Generalmente, se trata de cuentas de usuarios que pertenecen al ámbito de la música, la actuación, la moda, el gobierno, la política, la religión, el periodismo, los medios de comunicación, los deportes, los negocios y otras áreas de interés clave."*

En consecuencia, es completamente subjetivo y hasta cierto punto unilateral el que se verifiquen o no ciertas cuentas, y no se encuentra disponible al público en general información detallada sobre cuáles son los criterios específicos ni los requisitos concretos que se solicitan a un usuario que pretende verificar una cuenta. Cabe señalar, como ejemplo, que la cuenta institucional de "Twitter" del Tribunal Electoral del Poder Judicial de la Federación (@TEPJF_informa) y de los magistrados que integran su Sala Superior sí se encuentran verificadas. Sin embargo, la cuenta que supuestamente pertenece a la Sala Regional Guadalajara del mismo tribunal (@TEPJF_GDL) no se encuentra verificada, ni tampoco la que supuestamente pertenece a una de las magistradas que forman parte de dicha Sala (@GabrieladeValle).

En este breve ejemplo, un "ciudadano de a pie" tendría válidamente razones para dudar de la veracidad de la información que se comparte en las cuentas "no verificadas" y probablemente confiará más de la información que se comparte de las cuentas "verificadas"; pero el problema de fondo, es que gracias a la falta de regulación legislativa, hasta cierto punto el Estado Mexicano está dejando en las manos de una empresa particular (en este caso "Twitter") y no de un órgano del Estado o autoridad competente, la responsabilidad de verificar o certificar la veracidad del origen y naturaleza de determinadas cuentas.

Esto es relevante, pues como ya hemos visto en el apartado de antecedentes, la magnitud de las consecuencias de un solo "tweet" puede ser gigantescas, y es inevitable preguntarnos cuestiones como: ¿Qué pasaría si "Twitter" se equivoca? ¿Qué pasaría si verificara erróneamente una cuenta que no le pertenece realmente a quien dice ser?, ¿Quién sería responsable de las consecuencias derivadas de la información vertida desde esa cuenta? Evidentemente habría que analizar el caso concreto y el tamaño de sus consecuencias, pero es muy probable que un "monstruo" como "Twitter" se pudiera lavar las manos, y en el mejor de los casos asumir el "golpe mediático" de su

error, pero difícilmente habría alguna otra consecuencia pues no existe legislación específica en la materia.

En ese sentido, debemos de decirlo con claridad: No existen actualmente elementos suficientes para poder considerar como "oficial" ninguna de las cuentas de redes sociales de ninguno de los órganos del Estado ni de los servidores públicos que los presiden o integran, y lo más cercano que nos encontramos a ello, es la "verificación" realizada por los propios proveedores sobre la identidad del titular de dichas cuentas, sin que se encuentre regulado con claridad, cuál es el vínculo de responsabilidad que existe entre el usuario verificado, la empresa proveedora de la red social correspondiente y el usuario receptor de la información que en ellas se publica.

Sobre este rubro las ya referidas "Políticas para la difusión de información pública mediante redes sociales digitales" han dado ya un primer intento de dar claridad a esta materia, al definir las cuentas oficiales como: Cuenta de redes sociales digitales cuyo nombre hace alusión a un sujeto obligado, a alguna área, dependencia o cargo perteneciente a éste, y que es administrada y supervisada, directa o indirectamente, por dicho sujeto obligado.

II. c. ¿Qué implicaciones legales tiene la falta de certeza sobre cuáles son las "cuentas oficiales de redes sociales"?

Muchas. Además de las que se dejaron como inferencia en el apartado anterior, para la población en general el tema de las noticias falsas (#fakenews) se ha convertido en una de las "epidemias de la desinformación" más graves que existen para los usuarios de redes sociales, al grado que en México, el Instituto Nacional Electoral trató de contenerlas en el proceso 2018, a través de la firma de convenios con las empresas de redes sociales con mayor número de usuarios como Facebook. En ese sentido, así como cada día incrementa el uso de las redes sociales como la fuente principal de información de la ciudadanía, en la misma proporción se incrementa la necesidad de los usuarios de las mismas de tener plena certeza de la legitimidad del origen de la información.

Como ya lo mencionamos en los antecedentes, un juez de distrito en Sonora, el órgano garante de la transparencia en Jalisco, el Sistema Nacional de Transparencia y la Suprema Corte de Justicia, ya se pronunciaron en el sentido de que la información que se difunde por redes sociales, desde las cuentas utilizadas por servidores públicos (personales o institucionales) para dar a conocer cuestiones relativas al ejercicio de su encargo, debe ser considerada como "información pública" o "información de interés público" en los términos del artículo 6 de la Constitución Política Mexicana. En ese sentido, cobra mucho más relevancia el que exista plena certeza de que el servidor público que está detrás de una cuenta de redes sociales es efectivamente quien dice ser o en tratándose de una cuenta "institucional", represente legítimamente a la autoridad que dice representar.

Solo basta usar un poco la imaginación, para darnos cuenta de la gravedad que podría representar para un ciudadano el seguir una "cuenta oficial falsa", en el sentido de que no corresponde a quien aparentemente dice corresponder, de una autoridad o de una institución pública, por el tipo de errores o acciones a los que pudiera ser inducido a través de ella.

Cuando el entonces Papa, Benedicto XVI y la Agencia Central de Inteligencia Norteamericana (CIA, por sus siglas en inglés) abrieron por primera vez sus cuentas de "Twitter", (en diciembre de 2012 y junio de 2014, respectivamente) hubo muchos usuarios de esa red social que dudaron de que efectivamente correspondieran a dichas instituciones. Cabe destacar, que la cuenta utilizada por Benedicto XVI no se introdujo como cuenta personal, sino como cuenta institucional y, por ende, cuando asumió el cargo el Papa Francisco, éste absorbió el control de dicha cuenta y de sus seguidores. Este tema es importante, según veremos en el siguiente apartado.

II. d. ¿Quién es el propietario de las cuentas de redes sociales?

Hace tiempo una alcaldesa electa me preguntó -unos días antes de tomar posesión constitucional del cargo-: "¿Qué hacemos si no nos quieren entregar las contraseñas para las redes sociales oficiales de Facebook, Twitter y YouTube del Municipio?"

Sin duda alguna, otro de los grandes problemas derivados de la falta de regulación del uso de las redes sociales, es que el creador de una cuenta de una red social, es quien asigna: el nombre de usuario; la clave o contraseña de acceso; las preguntas de seguridad; el correo electrónico de verificación e incluso el número de teléfono vinculado a esa cuenta. En pocas palabras, se vuelve el administrador único de la cuenta ante la empresa proveedora del servicio. El problema es que estos administradores no están formalmente obligados a "entregar" dicha información sobre la cuenta a quien se ostente públicamente como el titular de la misma.

En el caso de los gestores de cuentas o "Community Managers" (como tradicionalmente se les conoce), por ejemplo, fungen como los encargados de administrar ciertas cuentas de redes sociales de personas, empresas o instituciones, con el objetivo de darles contenido e interacción "en nombre" de dichos usuarios. El "CM" suele ser muchas veces no solo una persona, sino varias o incluso toda una agencia publicitaria, quienes tienen acceso total a la cuenta, y dentro de ciertos parámetros (en teoría claramente establecidos) libertad de publicar lo que se considere mejor para la persona, empresa o institución que representan en dicha red social.

No son pocos los escándalos derivados del uso indebido o inapropiado de las cuentas por parte de los "CM", que van desde deslices menores hasta faltas de respeto más escandalosas, como por ejemplo cuando en el año 2014 la aerolínea holandesa "KLM" se burló de los mexicanos segundos después de que la selección holandesa eliminara a la selección mexicana en un partido del Mundial de Fútbol de Brasil celebrado ese año, o cuando en el año 2016 la marca de lentes de sol "Hawkers" se burló también de los mexicanos con un "tweet" referente a la construcción del muro con los Estados Unidos de Norteamérica.

Ambos "tweets" produjeron reacciones iracundas de personajes muy famosos como Gael García, en el primer caso, y Sergio "Checo" Pérez en el segundo, quien incluso dio por terminada su relación comercial con "Hawkers", también mediante un "tweet". Una de las preguntas obligadas en estos casos es: ¿Fueron real y legalmente las empresas "KLM" y "Hawkers" quienes se burlaron de los mexicanos?, ¿se reunieron en asamblea de accionistas y aprobaron por mayoría la decisión de publicar dichos "tweets"? o ¿fue simplemente una decisión equivocada de marketing de la o las personas que contrataron para manejar sus cuentas de redes sociales?. Y en última instancia: ¿Quién sería el responsable del daño que se causó o se hubiera causado por la transmisión de esa información en contra de una o más personas?. Cabe señalar que en ambos casos, los "tweets" fueron eliminados en muy poco tiempo, y además existieron disculpas públicas a través de la propia red social.

Esto refleja la importancia y la gravedad que puede representar la falta de regulación de las redes sociales públicas de autoridades, gobernantes y políticos en general, porque a diferencia de los personajes públicos (que no hacen política) o de las empresas comerciales, las consecuencias de un "tweet" equivocado nacido de la cuenta de redes sociales de una autoridad, pudieran ser mucho más graves que la simple pérdida de seguidores o potenciales clientes. En tratándose de autoridades, temas como proceso electoral, seguridad pública, seguridad nacional, vialidad, desastres naturales, salud pública, educación, servicios públicos, etc., no pueden ser tratados ni difundidos sin consecuencias, por los efectos y naturaleza de quienes los emiten. De igual manera, en cuestiones político-electorales, tampoco se puede tomar a la ligera el uso que se pueda dar a dichas cuentas con el propósito de incidir en el electorado a favor o en contra de determinada persona o proyecto político. Imaginemos, por ejemplo, los efectos políticos y sociales que tendría que desde la cuenta verificada del INE, se emitieran ofensas contra un candi-

dato presidencial y preguntémonos: ¿Quién sería el responsable y por qué?

En conclusión, lo que debemos de generar es regulación legislativa para evitar tener que responderle a esa alcaldesa que no sabía qué hacer si quienes salían no le entregaban las contraseñas de las cuentas de redes sociales institucionales del Ayuntamiento, y que lamentable y muy probablemente, nada, porque no existe regulación en la materia.

II. e. ¿A dónde se va el dinero público utilizado en redes sociales institucionales?

Si no existen cuentas públicas de redes sociales "oficiales" del gobierno y gobernantes, entonces ¿Cómo se justifica el gasto que se eroga para difundir información a través de dichas cuentas?. Hace unos años, por ejemplo, se dio a conocer públicamente que la Secretaría de Educación del Gobierno Federal Mexicano, había gastado alrededor de $32.5 millones de pesos en publicidad en sus redes sociales (Montes 2016), con el objeto de difundir la reforma educativa. Recientemente se han dado a conocer en notas periodísticas que la cantidad empleada en gastos de comunicación social, incluidas las redes sociales, superaron incluso el gasto de capacitación a maestros (Roldán 2018). Todo este gasto se justifica, teóricamente, en que se cumple un objetivo de mantener informada a la sociedad sobre cuestiones de interés público; sin embargo, como consecuencia o beneficio paralelo, se consigue que las cuentas desde las que se difunde la información adquieran más seguidores, lo cual aumenta el poder de difusión de información de una cuenta determinada.

Cabe señalar que los portales de redes sociales son un negocio, y uno de los activos más caros que tienen son precisamente sus usuarios. Por esa misma razón, uno de los mecanismos más costosos de "ganar" adeptos o seguidores es precisamente a través de campañas publicitarias (con las que dichas compañías ganan mucho dinero). La ventaja de ganar usuarios, a pesar del costo, es que la cuenta crece en poder para difundir información y, por lo tanto, en teoría es bueno gastar (o invertir) dinero con ese objetivo. Es claro que las autoridades gubernamentales no buscan lucrar con sus seguidores (al menos en teoría), sino servir a la sociedad a través del cumplimiento de sus obligaciones constitucionales o legales, y en ese sentido, el uso de las redes sociales podría considerarse legítimo para tal fin, incluyendo el gasto de muchos millones de pesos para ello.

Siguiendo con el ejemplo señalado, actualmente la "cuenta oficial" (de acuerdo a la definición de las Políticas Generales del SNT) o bien, la "cuenta pública verificada" en "Twitter" de la Secretaría de Educación Pública (@SEP_mx) tiene alrededor de 784,000 seguidores. No sabemos cuántos tenía hace dos años, ni cuántos ha adquirido a través de sus campañas publicitarias, porque no tenemos acceso a su *"analytics"* que es el servicio que ofrece "Twitter" para poder conocer el crecimiento y actividad de una cuenta, y los resultados derivados de sus "tweets" y campañas publicitarias (lo cual en mi opinión debe ser considerada información pública). Sin embargo, retomando la pregunta con que iniciamos el apartado pasado: ¿Qué hubiera pasado si el treinta de noviembre del dos mil dieciocho el servidor público que la administra o "CM" de dicha cuenta decidiera borrarla totalmente?, ¿Qué pasaría si no entrega las contraseñas de acceso?, ¿Qué pasaría si el gobierno entrante tuviera que abrir una nueva cuenta con cero seguidores? La respuesta es: probablemente no hubiere tenido ninguna consecuencia legal, porque no existe regulación al respecto; y al menos su reactivación no dependería del gobierno, sino de la buena voluntad de un corporativo particular extranjero y transnacional: "Twitter".

II. f. ¿Existen riesgos de violación al artículo 134 constitucional mediante el uso de redes sociales?

Me parece que sí. Por ello, para terminar este capítulo, cerraré con uno de los temas que considero más delicados por la falta de regulación de las redes sociales utilizadas por gobierno, gobernantes y po-

líticos; y es precisamente el referente al empleo de recursos públicos para promocionar o beneficiar la imagen personal de un servidor público.

Debido a la falta de regulación actual, cuando un político asume un cargo público utiliza su "cuenta personal" para difundir las actividades inherentes a dicho cargo. Si uno revisa la "cuenta verificada" de "Twitter", del ex-presidente de México (@EPN), con 7,4 millones de seguidores, descubrirá que dicha cuenta se abrió en el mes de marzo de 2007, es decir, muchos años antes de que fuera presidente del país. En ese sentido, queda claro que es su cuenta personal y, sin embargo, de alguna manera se utilizó como "oficial" o lo más parecido que a ello existe, durante los seis años de su gestión presidencial. Es evidente, que al haberse utilizado de esta manera, dicha cuenta personal obtuvo o "ganó" millones de seguidores en ese mismo periodo. Desconozco cuántos de esos seguidores se obtuvieron producto de alguna campaña publicitaria oficial (es decir, pagada con recursos públicos) pero en mi consideración, es innegable que cualquier seguidor que haya sido obtenido por esa vía, se hizo en contravención con el artículo 134 constitucional.

De igual manera, quienes lo han denunciado públicamente por el uso de "bots" o "peñabots" han argumentado la misma violación al artículo 134 de la Carta Magna, porque dichas supuestas prácticas pudieran haber ayudado a posicionar su imagen (y a ganar seguidores en consecuencia) de manera artificial (no orgánica) inducida por el uso de recursos públicos propiedad de todos.

En Estados Unidos de Norteamérica, por ejemplo, su Presidente actual se negó a utilizar directamente la "cuenta institucional verificada" de la Presidencia de dicho país en "Twitter" (@POTUS), argumentando que la propia (@realDonaldTrump) tenía más de 40 millones de seguidores contra los menos de 14 millones de la "oficial", y que prefería seguir en contacto con ellos a través de su cuenta personal.

En ese sentido vale la pena preguntarnos: ¿Qué tan legal o legítimo es que un funcionario público haga crecer su poder de comunicación personal a través de redes sociales, aprovechando el ejercicio de su cargo público? Es evidente que muchas personas únicamente seguirán esa cuenta por el cargo que ostenta, y también es posible que muchos usuarios dejarán de seguirlo cuando deje de ocupar dicho cargo, pero aún así es altamente probable que no todos -y ni siquiera la mayoría- lo hagan.

Aunque en mi consideración es evidente que cualquier peso destinado a la difusión de alguna cuenta personal de redes sociales de un servidor público, es en detrimento de la prohibición constitucional referida, también es evidente que pueden existir otros mecanismos menos directos de realizar campañas que hagan "ganar" seguidores o adeptos a estos funcionarios en sus cuentas personales, sin que se destinen directamente recursos públicos a la difusión desde sus cuentas. Por ejemplo, si una cuenta institucional crece en número de seguidores gracias al dinero que se le invierte, y aumenta –digamos- de cien mil a diez millones en un breve periodo de tiempo, y después "retwittea" todas las publicaciones de la cuenta personal de un funcionario público (e.g. el titular de la dependencia), es lógico que dicha cuenta personal también "crecerá" en seguidores y se adquirirá mucho mayor alcance o poder de comunicación, beneficiándose indudablemente de los recursos públicos que se emplearon para hacer crecer la cuenta institucional en primer lugar, y proyectándose con mayor facilidad para algún puesto de elección popular u otro puesto de alta jerarquía dentro del gobierno o alguna institución política en detrimento inequitativo de sus hipotéticos rivales.

III. Conclusiones

Concluyo básicamente haciendo referencia al título de este ensayo: Es indispensable legislar sobre el uso de redes sociales por parte de autoridades, funcionarios públicos y políticos (o personas que busquen influir legítima o ilegítimamente en una elección), por los graves daños a la democracia que la falta de regulación puede llegar a tener, según hemos visto en el presente ensayo. Por ello, independientemente del gran avance que las Políticas Generales sobre la materia aprobadas por el Sistema Nacional de Transparencia, considero que sigue siendo indispensable que legislar sobre:

- Definición de "cuenta oficial" de redes sociales.
- Obligaciones de los responsables del manejo de "cuentas oficiales".
- Transparencia sobre el manejo de las "cuentas oficiales", la asignación de recursos para difundirlas y los responsables de su manejo.
- Reglas sobre el tipo y contenido de los mensajes que se pueden difundir.
- Darle calidad de información pública a la que se difunde en redes sociales.
- Establecer las reglas y límites para que un servidor público pueda utilizar su cuenta personal de redes sociales en el ejercicio del encargo.
- Establecer mecanismos de rendición de cuentas y de responsabilidades en el manejo de las redes sociales.
- Establecer los límites para los usuarios de redes sociales sobre el uso de las mismas con fines electorales.
- Generar un registro público de "cuentas oficiales" de redes sociales.

Estoy convencido de que la regulación de estos temas desde leyes generales, federales y/o locales de transparencia y acceso a la información pública (y todas aquellas que sean necesarias) fortalecerá el estado democrático mexicano, por varias razones:

En primer lugar, porque se limitará el uso indebido y el abusivo de las redes sociales por parte de los servidores públicos y los políticos, que actualmente omiten rendir cuentas sobre dicha utilización. En segunda instancia, se fortalecerá el derecho a la información de la población, que tendrá mucha mayor certeza sobre la veracidad de sus fuentes de información pública. Finalmente, se generarán mayores condiciones de equidad democrática, al impedir que se puedan utilizar recursos públicos o capital privado no fiscalizado, para incrementar los seguidores de una persona, o influir en las tendencias electorales, a favor o en contra de una persona o proyecto determinado.

Cabe señalar que las propuestas concretas de reforma ideales, probablemente impliquen un trabajo titánico de redacción, adaptación, adecuación, justificación casuística y localización en cada marco normativo, que posiblemente supere los límites de un trabajo de esta naturaleza, pero ello no debe inhibir a nuestros legisladores a abordar el problema con toda la seriedad y sapiencia posible para lograr fijar los primeros precedentes legislativos en esta materia.

Salvador
Romero Espinosa

Es Abogado por la Universidad de Guadalajara.

Es Doctor en Derecho por el Instituto de Investigaciones y Capacitación electoral, con la tesis doctoral titulada: “Registro Nacional de Compromisos Electorales. Herramienta para fortalecer la Democracia en México.”

Es Maestro en “Derecho Público” por la Universidad Panamericana, y tiene las Especialidades en “Derecho Constitucional y Amparo”, y en “Derecho Fiscal” por la misma universidad.

Tiene además Especialidad en “Derecho Administrativo” por el Instituto Nacional de Administración Pública; así como la Especialidad en “Gestión, Publicación y Protección de la Información” por el Centro de Estudios Superiores de la Información Pública.

Desde agosto del año 2016 es Comisionado Ciudadano del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), y desde el año 2018 es el Director de la Revista “Caja de Cristal” de dicho Instituto.

En 2018 y 2019 fue Coordinador Nacional de la Comisión Jurídica, de Criterios y Resoluciones del Sistema Nacional de Transparencia.

Fue Coordinador de la Sindicatura en el Ayuntamiento de Guadalajara entre 2005 y 2007, y Director del Órgano Técnico de Puntos Constitucionales del Congreso del Estado de Jalisco entre 2007 y 2009.

Entre 2009 y 2011 fue asesor de la Comisión de Puntos Constitucionales, y de la Comisión Bicameral de Seguridad Nacional, en la Cámara de Diputados del Congreso de la Unión.

En el proceso electoral 2012 se desempeñó como Secretario Ejecutivo en el Tribunal Electoral del Poder Judicial de la Federación y en el proceso 2015 como Secretario Relator en el Tribunal Electoral del Estado de Jalisco.

Ha publicado diversos artículos en materia de derecho a la información, protección de datos personales, derecho electoral y derecho municipal, y es autor del Cuaderno de Transparencia denominado: “Las Redes Sociales Digitales: Su relación con el derecho a la información, la libertad de expresión y la privacidad”.

Desde el año 2019 es autor de la columna semanal de divulgación titulada “Hablemos de Derechos”, que se publica en diversos portales digitales.

Hace 18 años, en 2003, ganó el 2do lugar en el Primer Concurso Nacional de Ensayo “México entra en la Era de la Transparencia”, organizado por el entonces Instituto Federal de Acceso a la Información Pública.

Bibliografía

Buentello, Adriana (agosto 08 de 2017). “Los Peñabots: El miedo de Peña Nieto a las redes sociales.” Disponible en: https://actualidad.rt.com/actualidad/246441-penabots-miedo-pena-nieto-redes (consultada el 10 de septiembre de 2018)

ITEI. Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. Disponible en: http://www.itei.org.mx/v3/documentos/art12-11/recursos/2017/resolucion_rr_1441_2017_22112017_testada.pdf (consultada el 11 de septiembre de 2018).

Merriam-Webster. Disponible: es https://www.merriam-webster.com/dictionary/social%20network (consultada el 10 de septiembre de 2018)

Montes, Rafael (diciembre 26 de 2016) “En cuatro años, SEP gastó 32.5 mdp en redes sociales”. Disponible en: http://www.milenio.com/politica/anos-sep-gasto-32-5-mdp-redes-sociales (consultada el 11 de septiembre de 2018).

Nájar, Alberto (marzo 17 de 2015) “¿Cuánto poder tienen los Peñabots, los tuiteros que combaten la crítica en México?”. Disponible en: www.bbc.com/mundo/noticias/2015/03/150317_mexico_internet_poder_penabot_an (consultada el 10 de septiembre de 2018)

Ojeda de la Torre, Ivonne. (agosto 10 de 2018) “EPN gastó 2,758 mdp en la Red, con apenas impacto; ahora su cuenta en Twitter languidece a diario”. Disponible en: http://www.sinembargo.mx/10-08-2018/3455332 (consultada el 11 de septiembre de 2018).

Olaya G. Vicente (junio 14 de 2015). “Un edil de Ahora Madrid se burla en Twitter de los judíos y de Irene Villa.” Disponible en: https://elpais.com/ccaa/2015/06/13/madrid/1434219265_951793.html (consultada el 11 de septiembre de 2018).

Roldán, Nayeli (mayo13 de 2018) “SEP redujo recursos para capacitar docentes al mismo tiempo que multiplicó su gasto en comunicación social”. Disponible en: https://www.animalpolitico.com/2018/05/sep-gasto-reforma-educativa-comunicacion/ (consultada el 11 de septiembre de 2018).

Rosenberg, Matthew; Confessore, Nicholas; y Cadwalladr, Carole. (marzo 17 de 2018) “How Trump Consultants Exploited the Facebook Data of Millions”. Disponible en: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (consultada el 10 de septiembre de 2018)

TWITTER. Términos de servicio. Disponible en: https://twitter.com/es/tos Acerca de las cuentas verificadas. Disponible en: https://help.twitter.com/es/managing-your-account/about-twitter-verified-accounts (consultadas el 11 de septiembre de 2018).

Villanueva, Ernesto. (septiembre 19 de 2016). “Peñabots”: ¿Cuántos son? ¿Cuál es su fundamento legal? (Primera parte). Disponible en: https://aristeguinoticias.com/1909/mexico/penabots-cuantos-son-cual-es-su-fundamento-legal-primera-parte/ (consultada el 10 de septiembre de 2018).

GOBIERNO ABIERTO

Jalisco

gobiernoabiertojalisco.org.mx

SECRETARIADO TÉCNICO DE
Gobierno Abierto
JALISCO

Fotografía: Truth Seeker 08 para Pixabay

La importacia de la debida recepción de los documentos

María del Carmen Silva Ramírez
Actuario en el ITEI

Resumen

El artículo centra su atención en el análisis de las diferentes disposiciones legales en materia archivística, principalmente en el área de la recepción y tratamiento que se le da a la documentación que ingresa a las dependencias públicas para su debida y correcta atención, así como su manejo en las áreas correspondientes que lleva el debido glose de los expedientes y su futuro paso al archivo de concentración o en su caso, el archivo histórico; en el cual se va a poder observar la nula legislación que hay referente a este tema, tratándose de Legislaciones en América Latina (Argentina, Bolivia y México) como en España, si bien es cierto que se cuenta con reglas o leyes, también lo es que no ven como importante el cómo se inicia un expediente o archivo.

También se busca que esta laguna legal, por así llamarla, se pueda legislar para que haya un mejor manejo, desde el inicio de la documentación, como parte del ciclo de vida de un archivo, no se le otorga la debida seriedad y responsabilidad al recibir un documento, puede que sea por la cultura, o las malas praxis de creer que no es indispensable que se encuentren personas calificadas para realizar la debida recepción y derivación de la documentación que se ingresa a las dependencias.

Por lo que, no queda más que empezar esta investigación y futura conclusión, con el fin de que se logre la adecuada tramitología de los archivos en las dependencias públicas y privadas, si estas últimas podrían tener algún valor histórico para el País.

PALABRAS CLAVES:
Legislación Archivística, Recepción de Documento, Digitalización, Leyes Específicas sobre Archivos

Inicio

A causa de la escasa o más bien nula legislación acerca de cómo se debe de llevar el debido control del ingreso de la documentación, es que se sugiere agregar esto… a esta investigación con el fin de dar también vías de solución a esta problemática toda vez que al analizar la Ley General de Archivo, esta no es específica en las funciones que debe de tener el área de correspondencia u oficialía para un ejercicio adecuado para el manejo de la documentación, que son los futuros expedientes que serán archivados, esto para poder contar con una unificación de criterios.

Hay que dejar claro que es diferente el manejo que se pueda llevar en esa área, dependiendo de los organismos ya sea un Ayuntamiento, una Secretaría del Poder Ejecutivo, un organismo autónomo, Poder Judicial, Poder Legislativo por mencionar algunos, sin embargo, se tratará de que pueda ser viable para todos y tratar de unificar criterios.

Para iniciar hay que ser específicos que, debido a la reciente entrada en vigor de la Ley General de Archivo, es que ha tomado mucho interés, sobre todo porque, antes de esta legislación no se encontraban con una norma que regulara a todo el país, por lo que, cada Estado y dependencia hacían con su archivo lo que entendían para poder sobrellevar de manera "organizada" su documentación así como sus expedientes y cumplir con la transparencia y protección de datos personales.

Pero para iniciar hay que determinar que es **Archivo:** *es un conjunto de documentos, servicios de documentación, encargado de reunir y clasificar los materiales de consulta* (Jordán, 1998).

Los archivos son auténticos centros de información, imprescindibles para la administración y esenciales para la cultura. Permiten que la relación entre el Estado y la sociedad sea más dinámica e integral y, por ende, haya un mayor grado de compromiso y solidaridad entre sus miembros. (García, 2001)

También, es necesario saber que son los documentos, expedientes, digitalización, firma electrónica, así como el entender cómo se encuentra la legislación de la gestión documental en otros países; para iniciar definimos **Documento**, que *es la impresión en algún tipo papel la explicación o recopilación de información que da fe pública de un suceso o confirma la realización de una acción.* (Anónimo, 2019)

Al saber que es un documento podemos determinar que un **Expediente** *es el conjunto de los documentos que corresponden a una determinada cuestión. También puede tratarse de la serie de procedimientos de carácter judicial o administrativo que lleva un cierto orden.* (Merino, 2019)

Lo que es digitalización de documentos implica pasar documentación física a formato digital. Son muchas las empresas que almacenan gran cantidad de documentación que ocupa demasiado espacio y es difícil de consultar. Por lo que, pensar en digitalizar sus documentos, es posible que la primera idea que nos venga a la mente sea la cantidad de tiempo que se necesita para escanear a mano múltiples documentos. Pero afortunadamente, este proceso ha cambiado en cuanto a la forma: existen escáneres con una gran potencia que permiten aumentar el número de páginas por minuto, o bien, el proceso se puede subcontratar. (Macías, 2019)

Y para continuar con lo expuesto la Firma Electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca
- Asegurar la integridad del documento firmado, asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación
- Asegurar la integridad del documento firmado, los datos que utiliza el firmante para realizar el firmado son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento.

El uso de la Firma Electrónica[1] surge de la necesidad de las organizaciones de reducir costos e incrementar la seguridad de sus procesos internos, a través del uso de medios electrónicos que permitan agilizar los procesos, reducir los tiempos y evitar el uso de papel, (Varios, 2019)

Retomando el tema, de la digitalización,[2] al empezar a realizarse en todas las dependencias, se estaría salvaguardando a lo mejor lo que en un fututo puede llegar a ser un archivo histórico, del deterioro del paso del tiempo, como es la tierra, el moho, la húmeda, el agua, la destrucción con el paso del tiempo, claro está que los medios para guardar los documentos digitalizados tienen que contar con las medidas necesarias para su correcto archivo.

El inicio de un expediente, como ya fue expuesto es un documento, este comúnmente se ingresa a través de una oficialía de partes, oficialía de correspondencia, o dentro de las oficinas administrativas para iniciar con un proceso o trámite, el cual conlleva el recibir de manera física documentación en papel o medios electrónicos, como son USB, CD, o cualquier otro dispositivo.

Posteriormente este deberá pasar al área correspondiente para su debida integración y tramitación, para lo cual fue dado, en primera vista, se podría considerar que no es de suma importancia, sin embargo, una mala integración o derivación a un área no competente, sería que este documento no tenga la finalidad para lo cual fue ingresado.

Al estar consultando diversas legislaciones en varios países es que me pude percatar que este tema es de nula observancia, no dándole el valor que realmente merece y necesita.

Ejemplo en la Ley General de Archivo, solo lo menciona escuetamente en un artículo, para ser específico el 29, el cual cito a continuación:

> *"Artículo 29. Las áreas de correspondencia son responsables de la **recepción, registro, seguimiento y despacho**[3] de la documentación para la integración de los expedientes de los archivos de trámite.*
>
> *Los responsables de las áreas de correspondencia deben contar con los conocimientos, habilidades, competencias y experiencia acordes con su responsabilidad; y los titulares de las unidades administrativas tienen la obligación de establecer las condiciones que permitan la capacitación de dichos responsables para el buen funcionamiento de los archivos." (SIC)*

Si bien es cierto, el mencionado numeral[4] cita algunas palabras claves como son, recepción, registro, seguimiento y despacho, sin embargo no especifica cómo es que se tiene que realizar. Por lo que, no estaría de más que esta interrogante quedara mejor especificada en la posterior Legislación Estatal en materia de Archivo.

Un claro ejemplo es la Legislación Española, ya que es la que está más completa en materia de archivo, en la cual se podría tomar varias muestras como es el caso de la Orden CUL/1014/2007, del 30 de marzo, por la que se constituye la Comisión Española sobre la digitalización y la accesibilidad en línea del material cultural y la conservación digital.

En la cual, como su solo nombre lo indica habla acerca de la digitalización y accesibilidad de la documentación como cultura así como de la conservación digital.

Parte de esta digitalización, es la modernización de los archivos, podrá entrar una duda, ¿qué va a pasar con aquellos documentos o trámites que se presenten de manera física?, pues es sencillo, se requerirá de que la persona que se encargue de recibirlo, lo digitalice en ese momento y el original se regrese al

[1] Aunque este punto no se profundizará en este artículo.

[2] Tomar en cuenta este punto toda vez que quedará especificado en la conclusión.

[3] Lo subrayado es propio.

[4] Artículo 29 de la Ley General de Archivo.

interesado. Por lo que, el trámite o derivación será de manera digital, ahorrando tiempo y dinero.

¿Por qué se ahorra tiempo? porque al momento de digitalizarlo este se puede enviar al instante, a través de un sistema de derivación, a las áreas competentes, porque también es que quede asentado que no siempre un documento va dirigido a un área sino a diversas, por lo que, es indispensable sacar duplicados de escrito para presentarlos a las mismas, en cambio digitalizado, nada más se envía haciendo este un ahorro en dinero, al no necesitar una copiadora y hojas.

En diversos países principalmente de Europa, sobresaliendo España, ha llevado a cabo una cultura archivística mucho más avanzada que México, no tanto como en América Latina, en la cual se encuentran varios países dando sus primero pasos en esta materia, casi de la mano con nuestro país.

Empecemos con España en el cual su cultura de archivo data desde hace muchos años, como lo relata Miguel Ángel Fernández, en su artículo "Historia de los Archivos en España" como es que se empieza a reorganizar los archivos en el siglo XII, y que los documentos no se conservan en un solo sitio, se conservan en lugares distintos. Los documentos que conocemos son escrituras de propiedad y privilegios. El documento de su organización es el Liber Feodorum Mahior. Es un cartulario en el que se recogen privilegios y escrituras de concesión de feudos. Tiene cerca de 1.000 escrituras recogidas. Se acabó en 1192. (Fernández, 2019)

Su legislación es bastante ya que se conforman de real decreto, acuerdos y leyes, las cuales se conforman de acuerdo al tema de lo que se archiva así como de los Estados.

En una de las tantas legislaciones que cuenta España, la que más nos podría ayudar es la Ley 39/2015[5] cita diversos artículos respecto a las funciones que se cree competentes para llevar a cabo una correcta área de correspondencia (oficina para asistencia en materia de registro), en la cual contempla la citada Ley las siguientes atribuciones: Digitalizar toda la documentación que ingrese a la oficina (oficialía), si este es presentado en papel se deberá de digitalizar y devolverlo al interesado (evitando que no sea necesario su archivo). Llevar un Registro Electrónico General, en el que se hará el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, Organismo público o Entidad vinculado o dependiente a éstos.

Como se puede apreciar menciona lo mínimo necesario para poder realizar de una manera clara y concisa, el realizar una recepción adecuada de la documentación.

Ahora bien, cambiando nos vamos con las legislaciones archivísticas en América Latina, es variada, un ejemplo es la Ley del 23 de enero de 1957, Organización de los Archivos Nacionales de la República de Panamá, en la cual establece una clara diferencia entre las clases de archivos y los divide en estatales y no estatales. Los primeros, son aquellos constituidos por todas las oficinas del Estado, de organismo de gobierno y de instituciones autónomas. Los segundos, corresponden a las instituciones no pertenecientes al Estado, sin embargo, la documentación que custodian forman parte de la historia del país. (García, 2001)

La legislación archivística de Argentina tiene sus cimientos en el período colonial, por cuanto los archivos creados bajo el dominio español en el Virreinato del Río de la Plata, fueron legislados y administrados según lo establecido por la Corona. Posterior a la independencia se continuó rigiendo bajo esas leyes; pero, la abrogación de las estructuras gubernamentales españolas y, en consecuencia, la formación de nuevas instituciones, demandaron la reordenación de los archivos y, por consiguiente, la creación de disposiciones legales para su organización.

[5] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entrada en vigor 02/10/2016.

La legislación archivística boliviana se remonta al siglo XIX, de esta época destaca la ley del 28 de noviembre de 1898 que dio origen al AGN. En la primera mitad del siglo XX merece la atención el decreto del 9 de mayo de 1940, que estableció la Dirección General de Bibliotecas, Archivos y Publicidad. La misión archivística consistió en la conservación del patrimonio documental y contribuir a la reorganización de los archivos de los tres poderes del Estado.

Pero, en materia archivística, nos daremos cuenta que en relación al inicio de un expediente o archivo, no se encuentra establecido bajo qué parámetros se tendrán que recibir y el tratamiento que se le dará al mismo, esto en ninguna legislación; a lo largo de la investigación se puede percatar que casi todas las legislaciones archivísticas son copias casi iguales de varios países de América Latina, es decir, al no encontrarse en una establecida, es motivo por el cual no se encuentra en algún país está clave para llevar a cabo un correcto tratamiento.

En cuanto al aspecto de la legislación archivística en México podemos dividirla en dos etapas. La primera se refiere a las leyes y disposiciones establecidas con la finalidad del resguardo y protección del patrimonio documental. En las últimas décadas observamos una segunda etapa que regula la transparencia y eficacia de la información que genera la administración pública. Las disposiciones sobre los archivos han permitido establecer una normatividad que ha regulado la conservación del patrimonio documental y la organización de un sistema archivístico (redes de centros y órganos consultivos y/o técnicos).

Esta legislación tiene su antecedente en la Real Orden emitida el 28 de abril de 1792 que establecía las Ordenanzas para el Archivo general que ha de establecerse en el Palacio de Chapultepec. Esta disposición archivística señalaba que los documentos que hubiesen sido generados antes de 1760 debían ser remitidos al Archivo General de inmediato y que en lo sucesivo, en cada década, las dependencias de gobierno enviarían los expedientes con antigüedad de treinta años. Cabe señalar que las Ordenanzas seguían los lineamientos establecidos por las Ordenanzas de Indias, publicadas dos años antes. Este proyecto planteaba por primera vez un órgano autónomo dentro de la administración del virreinato de la Nueva España. El virrey Juan Vicente de Güemes Pacheco, segundo conde de Revillagigedo, a su llegada, revisó las oficinas con el fin de establecer un diagnóstico de la administración. En su reporte, el virrey indicó que halló algunos archivos sumamente confusos. (Meizanda M.C Ramírez Aceves, 2011).

El 23 de enero de 2012, Felipe de Jesús Calderón Hinojosa, presidente de los Estados Unidos Mexicanos, promulgó la Ley Federal de Archivos, ésta contiene 56 artículos. Dicha norma prohíbe a los servidores públicos sustraer documentos que estén bajo su custodia y resguardo y los obliga a entregarlos al final de su encargo, establece la estructura organizacional y los instrumentos mínimos necesarios para garantizar la conservación y organización de los archivos gubernamentales, tanto físicos como electrónicos, para conservar la memoria histórica de las instituciones.

El correcto manejo de un buen archivo facilita el buen uso y manejo de la información para una efectiva rendición de cuentas y se propone fortalecer el ejercicio del derecho de acceso a la información. Como México está compuesto por muchos estados, no todos cuentan con una ley de archivo, entre los que sí están Hidalgo, con su Ley de Archivo de Hidalgo, y el Estado de Tabasco, con su Ley de Archivos Públicos de Tabasco. (Aguilar, 2014)

Como se puede observar derivado de lo explicado en las anteriores legislaciones mencionadas en párrafos atrás, son casi nulas en habla de manera clara cómo se tiene que recibir la documentación, solamente se avoca en cómo se debe de manejar un archivo, los sistemas archivísticos, sin embargo, la Legislación Española que es una de las más avanzadas en estos tiempos sí lo establece y podríamos tomar de ahí claros ejemplos para poderlo implementar en nuestra Legislación.

Conclusiones

Finalmente, a continuación se expone la conclusión a la que hemos llegado en relación con el estudio acerca de la falta de legislación en la rama del inicio de un expediente:

Se puede constatar que es nula la legislación acerca de cómo se debe de iniciar, cuál sería el tratamiento que se debe de llevar al momento de recibir un documento, así como su tratamiento de, para la debida integración del expediente, así mismo la digitalización de los documentos para su debida conservación.

Por lo que mi propuesta es la siguiente para mejorar los puntos que se encuentran en laguna legal y así poder dar un mejor tratamiento y unificarlo, claro está que se encuentre en la futura Legislación en materia de Archivo del Estado de Jalisco.

El cual se **propone** que quede estipulado en la Ley de Archivo del Estado de Jalisco de la siguiente manera:

"El área de correspondencia deberá de realizar las siguientes funciones:

1. Recibir y distribuir la correspondencia de entrada;

2. Realizar la digitalización de los documentos;

3. Llevar el registro de la documentación a través de un sistema o base de datos que deberá contar mínimo con la siguiente información:

a) Contar con un número identificador (folio consecutivo de ingreso);

b) El asunto (breve descripción del contenido del documento);

c) Fecha y hora de recepción,

d) Medio por el cual ingreso;

e) Área y receptor del documento (nombre y área administrativa);

4. Ayudar en la iniciación de un procedimiento y facilitar un código de identificación. (De preferencia que sea un código Alfanumérico);

5. El seguimiento y despacho de la documentación pasará a los archivos de trámites para la debida integración de los expedientes;

6. El responsable de recibir la documentación en las áreas administrativas, deberá ser de preferencia el responsable de archivo de trámite, para que este se encuentre en posibilidades de llevar una mejor integración de los expedientes;

7. Si los documentos son remitidos al área de correspondencia a través de medios electrónicos, se tomará en consideración, si es necesario que se haga la impresión de los mismos, o través de un sistema darle entrada y derivarlos por estos medios.

Los responsables del área de correspondencia u oficialía deberán contar con los conocimientos, habilidades, competencias y experiencias acordes con su responsabilidad; y los titulares de las unidades administrativas tienen la obligación de establecer las condiciones que permitan la capacitación de dichos responsables para el buen funcionamiento de los archivos.

María del Carmen Silva Ramírez

Abogado, por la Universidad de Guadalajara y Especialista en Gestión, Publicación y Protección de Información, por el Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales.

Varios diplomados (constancias obtenidas):

- Argumentación Jurídica y Clasificación de la Información.
- Sistemas Anticorrupción, Transparencia y Gobierno Abierto.
- Gestión Documental, Protección de Datos Personales y Seguridad de la Información.
- Transparencia y Protección de Datos Personales en el Ámbito Municipal.

Referencias

Aguilar, A. P. (09 de 05 de 2014). Ley de Archivos y Acceso a la Información en Bolivia. *La Razón, La Gaceta Jurídica,* págs. 1-10.

Anónimo. (20 de 07 de 2019). *Conceptodefinicion.de, Redacción.* Obtenido de Definición de Documento: https://conceptodefinicion.de/documento/

Fernández, M. Á. (12 de 09 de 2019). *Islabahia.com.* Obtenido de Historia de los Archivos en España: http://www.islabahia.com/arenaycal/2009/165_noviembre/miguel_angel_165.asp

García, L. F. (2001). La Leg¡slación Archivística en América Latina. *Diálogos Revista electrónica de historia volumen 2,* 7-10.

Jordán, V. H. (1998). *Diccionario en términos archivísticos.* Buenos Aires: Ediciones del Sur.

Macías, A. (30 de 07 de 2019). *tic. portal.* Obtenido de tic. portal: https://www.ticportal.es/temas/sistema-gestion-documental/digitalizacion-de-documentos

Meizanda M.C Ramírez Aceves. (2011). El devenir histórico de la cultura archivística en México. *Información, cultura y sociedad,* 6-11.

Merino, J. P. (21 de 07 de 2019). *Definicón.de.* Obtenido de Definición.de:: https://definicion.de/expediente/

Varios. (10 de 09 de 2019). *Secretaría de Administración.* Obtenido de Universidad Autonoma del Estado de México: http://web.uaemex.mx/fise/0_1_inciso.html

Lineamientos para la publicación de trabajos en el número doce de la revista Caja de Cristal

Para la obtención del grado de Especialista en Gestión, Publicación y Protección de Información, el egresado deberá entregar un artículo con calidad publicable, de conformidad con lo establecido en los siguientes

LINEAMIENTOS

- Debe ser un artículo original e inédito, producto de una investigación y no podrá estar sometido de manera simultánea a un proceso de dictaminación por parte de alguna otra publicación, o medio de comunicación.
- Se deberán observar las reglas ortográficas, gramaticales y de sintaxis.
- El artículo deberá contener un resumen con una extensión mínima de 250 y máxima de 400 palabras.
- El artículo deberá incluir de cuatro a seis palabras clave sobre el contenido tratado, mismas que deberán ir en seguida del resumen.
- La extensión máxima del artículo es de 30 cuartillas en las cuales se incluya: el resumen, palabras clave, notas a pie y referencias y/o fuentes de consulta.
- El artículo deberá contener Conclusiones, en las cuales se observe el trabajo reflexivo generado por los hallazgos a lo largo de la investigación, y de manera deseable, propuesta(s) para modificar el estado de las cosas en el tema seleccionado.
- Al finalizar el artículo y antes de las Referencias, se deberá incluir una reseña de no más de 150 palabras en que se especifique el perfil curricular que contenga, al menos: nombre completo, institución de pertenencia y/o actividad laboral actual, formación profesional, así como su dirección de correo electrónico. Este apartado se deberá titular: Notas sobre el(la) autor(a)
- El tema tratado en el artículo, deberá apegarse a los temas revisados a lo largo de la Especialidad, mismos que son: Transparencia, Derecho a la Información, Gobierno Abierto, Mecanismos y Sistemas para Impedir la Corrupción, Gestión Documental, Protección de Datos Personales, Ciberseguridad y Big Data. En el caso de los siguientes temas: Participación Ciudadana, Democracia, Comunicación, Vida Pública, así como Vida Privada, deberá relacionarse el contenido de manera coherente con los temas revisados a lo largo de la Especialidad.

Normas de presentación formal y de citado de fuentes

El documento deberá contar con una portada y atender los siguientes requerimientos:

- El título del artículo debe ir centrado, en mayúsculas y en letra estilo Palatino tamaño 26.
- El nombre del autor/a irá todo en mayúsculas, con letra estilo Times New Roman tamaño 16.
- Debajo del nombre, la institución académica Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales (CESIP) en Times New Roman, tamaño 12.
- El cuerpo del artículo irá en fuente Times New Roman tamaño 12.
- El interlineado será a 1.15.
- La separación entre párrafos no irá marcada por un salto de párrafo sino por un espaciado de 6 puntos en la parte posterior de cada párrafo (puede seleccionarlo en Configuración de Párrafo de Word).
- La alineación del texto será Justificado.
- Todas las notas serán a pie (nunca al final del artículo) e irán numeradas correlativamente

con números arábigos, en TNR 10, interlineado sencillo, sin sangría y texto justificado.

- El estilo de citación de las fuentes y materiales consultados deberá ser el señalado por la Norma APA 2018 – 6ta (sexta) edición.

- La información completa sobre las obras consultadas y fuentes de consulta, aparecerá al final del documento, que se titulará "Referencias" y atenderá también a la Norma APA 2018, ya señalada.

DE LA ENTREGA DEL ARTÍCULO

- El trabajo deberá ser enviado a Manuel Rojas Munguía, Director del CESIP, a la dirección de correo manuel.rojas@itei.org.mx a más tardar el día 30 de septiembre del año 2019. El remitente recibirá un correo de confirmación de la recepción, el cual en ningún caso se deberá considerar una confirmación de que el trabajo cumple con los lineamientos ya señalados.

- El artículo debe enviarse en formato Microsoft Word (compatible con Windows y Mac) en dos archivos: el primero contendrá el artículo completo con los datos de identificación del autor(a), en los términos señalados en los lineamientos. El segundo archivo contendrá el artículo anonimizado. Proceso de dictaminación

- Únicamente se someterá a evaluación el artículo que cumpla con los lineamientos aquí presentados.

- Los trabajos aceptados serán dictaminados mediante el sistema Doble Ciego (Double-blind peer review) por un Comité Dictaminador que estará conformado por un miembro de la Junta Académica y por un experto disciplinario externo, que cuente con experiencia académica en el tema elegido por el autor del artículo y que cumpla con lo dispuesto en el Artículo 26 del Reglamento General del CESIP. Los evaluadores recibirán el documento sin nombre del autor(a) y emitirán un dictamen por escrito.

- Los dictaminadores podrán resolver en dos sentidos: aprobado para publicación (pudiendo realizar recomendaciones que se tendrán que atender para aspirar al grado) o no aprobado (y por ende no podrá obtener el grado). En los casos en que se den posiciones encontradas entre los dictaminadores, el Director del CESIP solicitará la intervención de un tercer dictaminador.

Disposiciones y Recomendaciones Generales

- Si bien estos lineamientos se enfocan -principal, aunque no exclusivamente- en la estructura general y presentación que deberá tener el artículo de divulgación con el cual se aspire a obtener el grado, cabe recordar que uno de los propósitos del artículo es transmitir el conocimiento generado y demostrar la capacidad intelectual del sustentante. Por lo tanto, la calidad del documento también depende de una correcta expresión de las ideas e interpretación de los datos.

El fallo del Comité Dictaminador es inapelable

- Cualquier controversia posterior al proceso de dictaminación será resuelta por la Junta Académica, en términos de lo establecido en el Artículo 79 del Reglamento General del CESIP.

- El envío del artículo para obtención de grado, implica la aceptación de lo establecido en este documento, la aceptación de los establecido en el Reglamento General del CESIP, la aceptación de la decisión que tomen en el futuro las autoridades del CESIP para publicar el texto en cualquier medio, en cualquier soporte y en el momento en que lo consideren conveniente.

- Los autores de los artículos que sean publicados no recibirán ninguna retribución económica, únicamente los créditos por autoría intelectual.

- El envío del artículo para obtención de grado, implica también, la aceptación y autorización para el tratamiento de sus datos personales, de conformidad con los Avisos de Privacidad del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco, mismos que pueden ser consultados en el sitio: www.itei.org.mx/v4/index.php/aviso_privacidad

ITEI Informa

01 de noviembre 2020 al 30 de abril del 2021

Caja de Cristal

Publicación Semestral de Transparencia y Acceso a la Información

Consulta los artículos de tu interés en nuestro nuevo portal

www.itei.org.mx/cajacristal

itei

INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE JALISCO

RESOLUCIONES RELEVANTES

CYNTHIA PATRICIA CANTERO PACHECO

Recurso de revisión

Fecha de resolución	Número de recurso
20 de enero del 2021	2425/2020

Sujeto obligado

Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado, SIAPA

Solicitud

"Se me informe lo siguiente vía infomex o a mi correo electrónico, sobre el fenómeno del agua turbia que afecta a colonias de la metrópoli:

1. Qué estudios y/o opiniones técnicas se han generado sobre las causas de este fenómeno, precisando por cada uno:

a). *Cuándo se generó*
b). *Instancia que lo generó*
c). *Costo del documento*
d). *Se me brinde copia electrónica del mismo*

2. Se me informe sobre todas las quejas/reportes recibidos por este fenómeno durante 2019 y 2020, precisando por cada queja/reporte lo siguiente –en archivo Excel como datos abiertos-:

a). *Fecha de recepción*
b). *Colonia donde se dio el caso*
c). *Se informe si ya fue resuelto o aún no*

3. Se me informe si el Órgano Interno de Control (OIC) del SIAPA o de otra instancia ya investiga las presuntas responsabilidades y/o a los funcionarios responsables tras este fenómeno, precisando lo siguiente:

a). *Cuándo inició la investigación, y clave de la misma*
b). *Copia del acuerdo que dé inicio formal a la investigación*
c). *En qué estatus se encuentra la investigación*

4. Se me precise si el SIAPA ya tiene un OIC o aún no, y se precise:

a). *a) Quién lo encabeza*
b). *b) Curriculum del titular*
c). *c) Qué instancia o funcionario lo eligió o designó*
d). *d) Método de elección del titular*

5. Con respecto a los servicios de agua potable del SIAPA, se me informe a cuántas colonias atiende con estos servicios por cada municipio.

6. Por cada municipio de los que son atendidos por el SIAPA con sus servicios de agua potable, se me informe cuántas y qué colonias han presentado este problema del agua turbia –en archivo Excel en datos abiertos." Sic.

¿Qué respondió el sujeto obligado?

El sujeto obligado otorga respuesta a los puntos 3, 4 y 5, de la solicitud de información.

Inconformidad

"Presento este recurso de revisión contra la respuesta del sujeto obligado debido a que la misma está incompleta, en parte debido a que el sujeto obligado condicionó el acceso a la información con requisitos fuera de la ley e innecesarios, por lo cual su resolución impidió que pudiera ejercer satisfactoriamente mi derecho de acceso a la información.

Recurro los siguientes puntos de mi solicitud: 1, 2 y 6.

Sobre el punto 1:

Lo recurro pues el sujeto obligado informa solo sobre posibles tesis explicativas del fenómeno, pero no da cuenta de estudios y/o opiniones de entes o consultores externos o privados, por lo que es posible que también existan estudios externos contratados por el sujeto obligado, mismos que no entregó.

Sobre el punto 2:

Lo recurro pues solicité esta información en archivo Excel como datos abiertos, lo cual evidentemente puede satisfacer sin inconvenientes el sujeto obligado…

Sobre el punto 6:

Lo recurro pues esta información simplemente fue omitida…" Sic.

Resolución del ITEI

Una vez admitido el recurso de revisión y notificado al sujeto obligado, en su informe de ley, se pronunció sobre la totalidad de la información faltante, misma que satisfizo la petición del recurrente.

¿Por qué es relevante esta resolución?

La importancia de la presente resolución se encuentra en el vínculo de dos derechos humanos: el de acceso a la información pública y el del agua.

El Derecho Humano de Acceso a la Información, consagrado en el artículo 6° en la Carta Magna, consiste en garantizar que las personas puedan acceder, buscar, obtener y difundir libremente la información pública generada por la posesión, uso o administración de recursos públicos; buscando constituirse en una herramienta que ayude a fortalecer un estado democrático, a través del principio de la transparencia.

Por lo que respecta al Derecho Humano del Agua, establecido en el artículo 27, de la Constitución Política de México, este no cosiste únicamente a tener el acceso al vital líquido, sino a poder ser utilizado en cantidades suficientes y en condiciones adecuadas para que sus necesidades de vida sean satisfechas de manera digna; de esta manera, cuenta con una dualidad, ser derecho prestacional y, a la vez de protección.

En este sentido, conocer las condiciones del agua (DDHH del Agua) a través un procedimiento de acceso a la información pública (DAI), siendo responsabilidad del Estado poner los medios y las condiciones para que los mismos se puedan ejercer, se vuelven trascendentes para garantizar una vida digna tanto en sentido material como para el desarrollo de todas sus potencialidades, siendo esto la esencia de los derechos humanos.

CYNTHIA PATRICIA CANTERO PACHECO

Recurso de revisión

Fecha de resolución	Número de recurso
16 de diciembre del 2020	1858/2020

Sujeto obligado

Coordinación General Estratégica de Gestión del Territorio

Solicitud

Entregar vía electrónica, en USB que yo llevaré, versión pública de todos los documentos entregables elaborados por parte del contratista SENERMEX INGENIERÍA Y SISTEMAS, S.A. DE C.V., respecto a los siguientes contratos:

- Contrato: SIOP-E-SRP-SER-AD-034-2020; Orden de Trabajo: AD-034-2020; Obra: SERVICIOS DE ASESORÍA TÉCNICA ESPECIALIZADA PARA LA VERIFICACIÓN DE LA CONSTRUCCIÓN DEL TREN ELÉCTRICO URBANO LINEA 3, GUADALAJARA, TLAQUEPAQUE Y ZAPOPAN, PERIODO 2020, PARA SU CERTIFICACIÓN, RECEPCIÓN Y PUESTA EN OPERACIÓN.

- Contrato: SIOP-E-SRP-SER-AD-123-2019; Orden de Trabajo: C-123-2019; Obra: SERVICIOS DE ASESORÍA TÉCNICA ESPECIALIZADA PARA LA CONSTRUCCIÓN DEL TREN ELÉCTRICO URBANO LÍNEA 3, GUADALAJARA, TLAQUEPAQUE Y ZAPOPAN, PERIODO 2019, PARA SU CERTIFICACIÓN Y PUESTA EN OPERACIÓN.

¿Qué respondió el sujeto obligado?

La respuesta es NEGATIVA-RESERVADA bajo los siguientes argumentos:

- Se encuentra aún en proceso de ejecución, ya que el Contratista continúa con los trabajos, y se tiene una prórroga al periodo de tiempo, por lo que aún no se cuenta con el resultado del servicio contratado, por lo que dicha información resulta inexistente.
- Se encuentra imposibilitada de realizar su entrega, incluso en versión pública, puesto que en su totalidad reviste el carácter de información RESERVADA.
- Entregar la información conlleva un riesgo que pudiera comprometer la seguridad pública y poner el riesgo la vida, seguridad o salud de las personas, ya que con ello se obtendría información importante de las instalaciones del Tren Eléctrico Urbano Línea 3; por lo que no se descarta que dicha información se le pueda dar un uso indebido, con el que se puedan planear acciones que dañen las instalaciones, equipo, funcionamiento, operación del sistema de la Línea 3 del Tren Ligero y con ello poner en riesgo a las personas que utilicen dicho transporte público, se encuentren en las instalaciones o laboren ahí.
- El daño o riesgo de perjuicio que se produciría al divulgar la información se podrían realizar actos delictivos como ataques, hackeos, atentados a las instalaciones del medio de transporte mencionado, lo que conllevaría a ocasionar un daño a los particulares que se encuentren en dichas instalaciones
- Se adjuntaron diversas fotografías relativas a diversos ataques sucedidos en otros países al transporte público, entre las cuales se encuentra Londres, España entre otros en los cuales señala que Las notas periodísticas nos rebelan como la delincuencia organizada han realizado actos delictivos en los sistemas de transporte público como lo son; (espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio…)
- Se anexó el acta de RESERVADA a través de la cual se reservó la información.

Inconformidad

- Se peticionó una versión pública de los documentos solicitados, pudiendo testar la información que pudiera poner en riesgo la vida, seguridad o salud de cualquier persona, sin embargo el sujeto obligado decidió reservar la totalidad de información por un plazo de cinco años.

-El argumento principal que sustenta la autoridad es en dar mal uso a la información para cometer ataques terroristas.

Resolución del ITEI

Se ordenó al sujeto obligado a través del Comité de Transparencia llevar a cabo lo siguiente:

1. El análisis de la información contenida en cada uno de los 63 entregables que corresponden al contrato SIOP-E-SRP-SER-AD-123-2019.
2. Sustentada la reserva de los citados documentos, deberá determinar la procedencia de la entrega de la información en versión pública o en caso de que la misma resulte inviable deberá fundar y motivar dicha imposibilidad.
3. Con base en lo anterior, podrá ser procedente la entrega de la información (respecto de cada entregable) mediante informe especifico, el Comité de Transparencia deberá asentar en el mismo mayores datos de identificación, características, naturaleza de la información y cualquier otro elemento que dé certeza de la existencia de la información solicitada y del estado en que esta se encuentra.
4. Respecto de los entregables del contrato SIOP-E-SRP-SER-AD-034-2020, deberá realizar una búsqueda exhaustiva de la información entregando la información o en su caso declare su inexistencia en términos del artículo 86 Bis de la Ley de la materia.

¿Por qué es relevante esta resolución?

La relevancia de esta resolución estriba en la necesidad de hacer cumplir los extremos de las leyes de transparencia, en el sentido de que, aun cuando la información que fue solicitada encuadre en los supuestos que la norma contempla como información protegida, ya sea por tratarse de información reservada o confidencial, sea posible su consulta parcial a través de una versión pública, a fin de garantizar a las personas su derecho de acceso a la información pública.

Además, en una cultura de rendición de cuentas, los sujetos obligados en principio, deben considerar que toda la información en su posesión es pública y solo de manera excepcional proceder a su reserva analizando el caso particular, privilegiando en lo posible la máxima publicidad de la información, y la entrega de esta a través del medio menos restrictivo.

SALVADOR ROMERO ESPINOSA

Recurso de Revisión de Datos Personales

Fecha de resolución	Número de recurso
28 de abril de 2021	506/2021

Sujeto obligado

Ayuntamiento de San Juanito de Escobedo, Jalisco

Solicitud

La solicitud consistía en requerir información respecto a la planeación y reglamentación del municipio; asimismo requirió de Dirección de Seguridad Pública: el monto y partidas presupuestales, así como los recursos ejercidos; el nombre oficial de la Institución Policial; el nombre del titular y su hoja de vida; su estructura orgánica; el número de auto-patrullas, moto patrullas, ciclo patrullas o equinos; chalecos balísticos no caducados; radio comunicadores en funcionamiento; armas largas y cortas (propias y en comodato), así como el nombre de la Institución que proporciona la formación inicial básica a su personal policial; y que le informaran si cuenta con un área de vinculación social.

¿Qué respondió el sujeto obligado?

Así, como respuesta se advierte que se entregó la mayoría de la información solicitada; sin embargo en relación la estructura orgánica, el número de auto-patrullas, moto patrullas, ciclo patrullas o equinos; chalecos balísticos no caducados; radio comunicadores en funcionamiento; armas largas y cortas (propias y en comodato) se señaló que se trataba de información reservada.

Inconformidad

Se inconformó por la clasificación de la información como reservada, ya que el sujeto obligado no explica, justifica, motiva o argumenta la razón de ello.

Resolución del ITEI

El sujeto obligado debía entregar la información cuantitativa, es decir, el número de auto-patrullas, moto patrullas, ciclo patrullas o equinos, el número total de chalecos, de radio comunicadores, de armas de fuego propias y de armas de fuego en comodato; reservando únicamente la información cualitativa, es decir, el número de chalecos balísticos no caducados, radio comunicadores en funcionamiento, y armas cortas y largas, mediante su Comité de Transparencia y conforme a los argumentos señalados.

¿Por qué es relevante esta resolución?

Al determinar procedente la reserva únicamente de la información cualitativa, se protege la capacidad de despliegue y operación, así como el destino final de su propósito (seguridad), en consecuencia, al realizar un análisis de dicha información por parte de los miembros de la delincuencia organizada, el municipio quedaría expuesto, ya que la difusión de dichos datos permiten conocer algunas de las estrategias adoptadas institucionalmente para velar por la seguridad de las y los ciudadanos, así como la de los servidores públicos, por lo que puede ponerse en riesgo su vida, seguridad y salud; por ende, las labores implementadas para el combate a la delincuencia.

El proporcionar la información cuantitativa abona a la rendición de cuentas, pues pone a la luz pública el equipo con el que cuenta el sujeto obligado para la consecución de su labor en materia de seguridad pública, lo que permite advertir que la Policía Municipal está en condiciones operativas de obtener resultados concretos en la labor que le es encomendada, sin poner al descubierto el estado de fuerza.

SALVADOR ROMERO ESPINOSA

Recurso de Revisión de Datos Personales

Fecha de resolución	Número de recurso
17 de marzo del 2021	2528/2020

Sujeto obligado

Contraloría del Estado

Solicitud

Versión publica de la investigación que se abrió por la licitación LPL 001/2018, para arrendamiento de maquinaria.

¿Qué respondió el sujeto obligado?

Al respecto, el sujeto obligado reservó la información mediante su Comité de Transparencia, argumentando medularmente que se trata de procedimientos de responsabilidad que no tienen resolución administrativa o jurisdiccional definitiva, toda vez que si bien ya concluyó la parte de la investigación y con ella, existe una determinación de calificación de las faltas y un informe de presunta responsabilidad, siguen pendientes los procedimientos de responsabilidad administrativa, lo que no permite considerar que la totalidad del proceso ha concluido. Por lo que entregar la información causaría perjuicio grave a las estrategias procesales.

Inconformidad

Se inconformó por la reserva ya que al tratase de actos de corrupción era aplicable la excepción; asimismo señala que no entregan una versión pública, que fue lo que se solicitó; y que no se motivan las razones particulares por las que se actualizan los supuestos de reserva legales señalados.

Resolución del ITEI

Se determinó que si bien ya concluyó la parte de la investigación y con ella, existe una determinación de calificación de las faltas y un informe de presunta responsabilidad, siguen pendientes los procedimientos de responsabilidad administrativa, lo que no permite considerar que la totalidad del proceso ha concluido, por lo que la reserva hecha valer por el sujeto obligado resulta aplicable en alguna medida.

En ese sentido, el sujeto obligado debía proceder a la elaboración de la versión publica de las documentales referidas -determinación de calificación de las faltas y el informe de presunta responsabilidad-, debiendo testarse aquellos datos relacionados con documentación, declaraciones, cargos y nombres de los servidores públicos involucrados, precisamente porque se encontraban sujetos a un procedimiento de responsabilidad para determinar la existencia o inexistencia de las faltas administrativas graves o no graves, así como las sanciones aplicables en su caso, y su divulgación podría afectar el resultado y esencia de dichos procedimientos, por lo que se debía desvincular cualquier dato que permitiera la identificación de los mismos, en tanto no se resolviera de manera definitiva el procedimiento.

Con relación a la manifestación de la parte recurrente en la que refiere la excepción a la reserva por tratarse de actos de corrupción, se le señaló que si bien la determinación de calificación de las faltas y el informe de presunta responsabilidad establecen que efectivamente pudo haber irregularidades -incluso graves- en el actuar de uno o más servidores públicos, también era verdad que ello por sí solo no significa que nos encontramos necesariamente ante actos de corrupción. Ello es así porque no había resoluciones que configuraran o confirmaran dicha situación, ni tampoco obraba en los autos del expediente elementos probatorios para que se acreditara o presumiera su existencia.

¿Por qué es relevante esta resolución?

El proporcionar la versión pública ordenada, permite dar cuenta de manera general del procedimiento de investigación realizado, sus fechas, sus resultados, el cumplimiento de las atribuciones de la Contraloría, entre otras cosas, pero sin obstaculizar la conducción del expediente al dejar al alcance de terceros información que aún debe ser valorada por la autoridad a efecto de adoptar una determinación definitiva sobre presuntas responsabilidades administrativas imputadas a servidores públicos.

PEDRO ANTONIO ROSAS HERNÁNDEZ

Recurso de revisión

Fecha de resolución	Número de recurso
09 de diciembre de 2020	2391/2020

Sujeto obligado

Ayuntamiento Constitucional de Tocolotlán, Jalisco

Solicitud

"…ME INFORME EL CONTENIDO O EVIDENCIA DE LA INSERCIÓN QUE SE PAGÓ A LA EMPRESA PLATAFORMA DE DISEÑO SA DE CV POR CONCEPTO DE SERVICIOS DE PUBLICIDAD MEDIANTE FACTURAS NUMERO 1304 Y 1305..." sic

¿Qué respondió el sujeto obligado?

El sujeto obligado se limitó a informar que la información solicitada podía ser encontrada en un perfil de la red social Facebook, además que se pronunció señalando que no cuenta con la obligación de elaborar documentos ad hoc.

Inconformidad

"…MANIFIESTA QUE LA EVIDENCIA DE LA PUBLICIDAD SOLICITADA ESTA EN LAS PAGINAS DE FACEBOOK, POR LO NO ES POSIBLE IDENTIFICARLAS YA QUE NO TIENE FORMA DE SABER CUALES FUERON LAS PAGADAS A LA EMPRESA PLATAFORMA DE DISEÑO SA DE CV …"sic

Resolución del ITEI

El Pleno de este instituto, determinó que el sujeto obligado debía entregar las evidencias solicitadas, informando específicamente cual de la información publicada en la red social correspondía a la solicitada, o en su defecto entregar copia simple de tales evidencia; lo anterior, de conformidad con el artículo 6, apartado A, fracción I, de nuestra Carta Magna, los sujetos obligados deben documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones.

Ante tal situación, la autoridad recurrida a través de su informe de cumplimiento entregó copia simple de las evidencias solicitadas, garantizando con ello el derecho de acceso a la información del recurrente.

¿Por qué es relevante esta resolución?

Ante tales circunstancias, no se puede perder de vista que la rendición de cuentas es una obligación de toda autoridad y que el acceso a la información es un derecho fundamental de cualquier persona; bajo esa premisa, los ciudadanos en todo momento tienen el derecho de acceder a la información pública y en consecuencia las autoridades deben entregar de forma clara, precisa, puntual y oportuna, aquella información que le es solicitada.

En el mismo orden de ideas, con la resolución emitida por el Pleno de este Instituto, el ciudadano pudo acceder a la información solicitada, es decir, a las evidencias que se generaron por los servicios de un proveedor y por los cuales se erogaron recursos públicos.

PEDRO ANTONIO ROSAS HERNÁNDEZ

Recurso de revisión

Fecha de resolución	Número de recurso
14 de abril de 2021	345/2021

Sujeto obligado

Ayuntamiento Constitucional de San Gabriel, Jalisco

Solicitud

"Desglose de gastos erogados por la Dirección de Cultura del gobierno municipal de San Gabriel, en los años 2019 y 2020.

Especificar el proyecto al que corresponde el gasto y adjuntar facturas correspondientes." (SIC)

¿Qué respondió el sujeto obligado?

El sujeto obligado se limitó a señalar que debido a gran cantidad de información, la misma se ponía a disposición para consulta directa en las oficinas de la Presidencia Municipal.

Inconformidad

"…Agradezco el envío de oficio, pero tomando en cuenta que el sujeto obligado es quien debe entregar la información que resulta existente y no condicionar a la peticionaria acudir de una ciudad a otra para recoger la información tomando en cuenta que la Unidad de Transparencia cuenta con todos los elementos para garantizar el derecho a la información…"

Resolución del ITEI

El Pleno de este Órgano Garante ordenó la entrega electrónica de la información solicitada, lo anterior hasta la capacidad máxima que permite enviar la Plataforma Nacional de Transparencia; señalando además que la entrega de información electrónica no genera gastos al recurrente.

¿Por qué es relevante esta resolución?

Con la resolución emitida por el Pleno del ITEI, por una parte se garantizó el anonimato del solicitante, además, quedó de manifiesto que ningún sujeto obligado debe condicionar la entrega de información de carácter ordinario a la consulta directa de documentos, ya que los ciudadanos no tienen la obligación de trasladarse a ninguna oficina gubernamental o de erogar cantidad alguna para acceder a la información pública en posesión de los sujeto obligados, salvo que el propio solicitante elija la reproducción de documentos con costo.

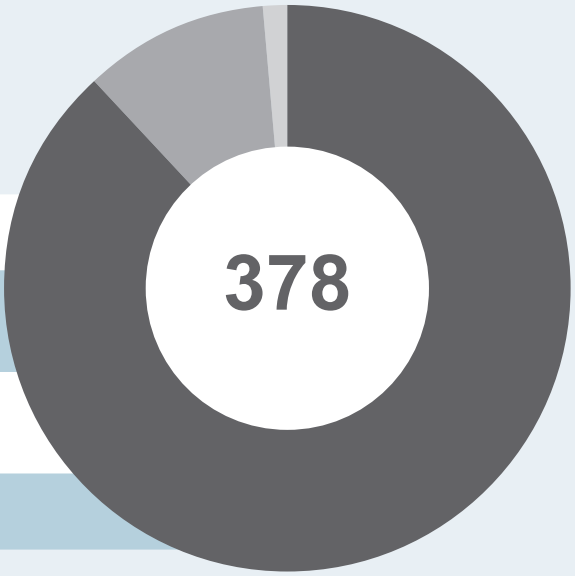
Aunado a lo anterior, de la información que fue requerida el solicitante, cualquier ciudadano puede verificar que los recursos económicos etiquetados para cada proyecto, sean utilizados y ejercidos en el mismo y que en caso contrario, contará con los elementos necesarios para ejercer los derechos que su consideración resulten procedentes; privilegiando como ya se mencionó el anonimato de los solicitantes.

Resoluciones aprobadas por tipo de recurso

Periodo comprendido del 01 de noviembre 2020 al 30 de abril del 2021

Cynthia Patricia Cantero Pacheco

Tipo de recurso	Número total de los recursos resueltos
Recursos de Revisión	333
Recursos de Transparencia	40
Recursos de Revisión de Datos Personales	5
Total	**378**

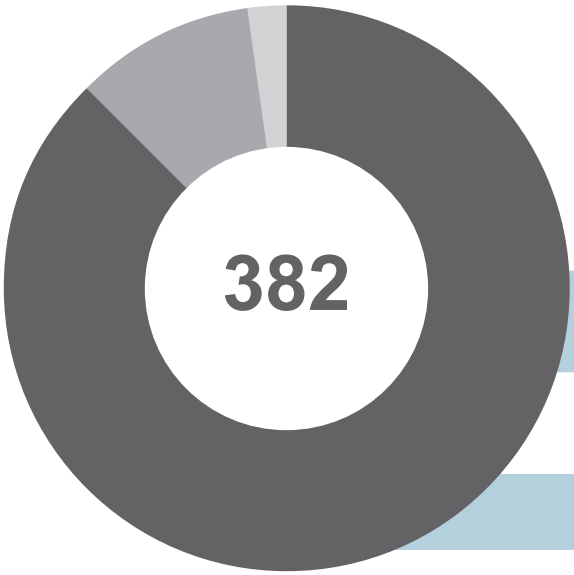


Revisión

Transparencia

Revisión de Datos Personales

Salvador Romero Espinosa



Tipo de recurso	Número total de los recursos resueltos
Recursos de Revisión	335
Recursos de Transparencia	39
Recursos de Revisión de Datos Personales	8
Total	**382**

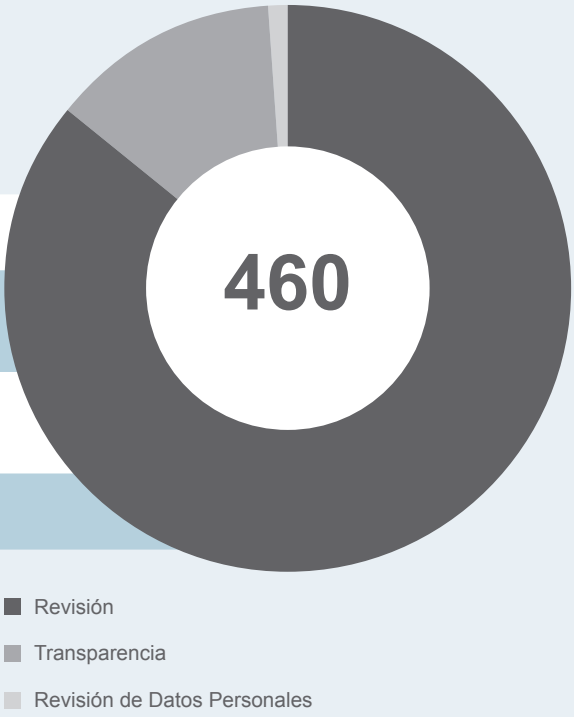
Revisión

Transparencia

Revisión de Datos Personales

Pedro Antonio Rosas Hernández

Tipo de recurso	Número total de los recursos resueltos
Recursos de Revisión	395
Recursos de Transparencia	61
Recursos de Revisión de Datos Personales	4
Total	**460**



Visite nuestro micrositio www.itei.org.mx/cajacristal

Ahora con la nueva
Plataforma Nacional de Transparencia
podrás solicitar información a cualquier
dependencia de Jalisco y de todo México.

Ingresa a
www.plataformadetransparencia.org.mx
¡y ejerce tu derecho!

#TuPlataformaMx

itei | INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE JALISCO