

Caja de Cristal

Publicación Semestral
de Transparencia y Acceso
a la Información

Año 5 - No. 10
Julio - Diciembre 2019

Contenido

Las cuentas de redes sociales abiertas de servidores públicos, son un instrumento para la divulgación de información oficial y/o pública según criterio del Órgano Garante de Jalisco (ITEI), ¿Cuáles son los alcances frente a los derechos de relación?

Miguel Ángel Vázquez Placencia 6

Retos y peligros de vivir sin privacidad en las TIC

Jersain Zadamiq Llamas Covarrubias 13

Libertad de expresión, información y credibilidad: Las fake news en tiempos violentos

Ynerid Yleannis Morales Colmenares 19

El derecho a la información pública, pieza fundamental en el combate a la corrupción

Alejandro Argenis Reynoso Tabares 25

Regulación de la transferencia internacional de datos personales en Latinoamérica. Especial mención al marco regulatorio de Argentina y México

Christian Alejandro Razza Sandoval 29

La transversalidad progresiva de la rectificación y oposición de datos personales para el acceso efectivo al derecho a la identidad jurídica de la población transgénero y transexual

*Rafael Ríos Nuño y
José Benjamín González Mauricio* 35

ITEI Informa

Resoluciones relevantes 47

*Cuadro estadístico:
Resoluciones aprobadas por tipo de recurso* 56



Portada
"Explosión de ideas"
Montaje: Juan Francisco García Gallegos

Revista CAJA DE CRISTAL, Año 5, No. 10, julio - diciembre 2019, 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. Impresa por XXXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX Este número se terminó de imprimir en enero de 2020. Primera edición con un tiraje de XX ejemplares.

Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación y de la Institución.

Queda estrictamente prohibida la reproducción total o parcial de los contenidos e imágenes de la publicación sin previa autorización del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.

Presentación

Desde que asumí la dirección de la revista Caja de Cristal, me propuse como objetivo principal que ésta crezca en difusión y se convierta cada día más en un vínculo entre el Instituto de Transparencia, Información Pública y Protección de Datos Personales del estado de Jalisco (ITEI) y la sociedad. En ese sentido podemos asegurarles que éste ha sido el número más complejo, pues nos propusimos que su contenido se integrara exclusivamente por ensayos de jóvenes interesados en las materias de derecho a la información, rendición de cuentas, protección de datos personales, privacidad y anticorrupción.

El primer gran reto para poder conseguir ese objetivo, fue encontrar la manera de atraer a los jóvenes a voltear a ver estos temas con la debida seriedad, y en ese sentido, se consideró que la mejor manera era proporcionándoles incentivos tangibles tales como premios atractivos (como computadoras y tabletas electrónicas), accesibles a través de la convocatoria a un concurso de ensayo.

El segundo gran reto fue conseguir dichos premios, ya que se tuvieron que tocar muchas puertas, hasta que finalmente el propio ITEI y 3 ayuntamientos de la entidad, por conducto de sus respectivos presidentes municipales, decidieron apoyar este noble concurso, a saber: Zapopan, El Salto y Tonalá, a los cuales hago nuevamente un agradecimiento público por hacer posible este número de la revista Caja de Cristal en los términos en que fue concebido.

El tercer gran reto fue lograr la difusión suficiente para que la mayor cantidad de jóvenes posibles pudieran enterarse —e interesarse— en participar en este concurso de ensayo. Cabe señalar que el ITEI es un organismo constitucional autónomo bastante austero y con presupuesto prácticamente nulo para gastos de comunicación social, lo que evidentemente nos obliga a dar a conocer la gran mayoría de nuestro trabajo a través de conductos gratuitos en redes sociales digitales y la amable cobertura que hacen del mismo los medios de comunicación, por lo que acudimos también a los organismos garantes de transparencia del país para que nos apoyaran con la difusión de la convocatoria a través de sus propias cuentas oficiales de redes sociales.

El último gran reto, después de haber recibido más de dos docenas de ensayos, fue precisamente determinar a los ensayos ganadores, toda vez que me atrevo a asegurar que cualquiera de los 6 ensayos que están publicados en este número de la revista, pudo haber obtenido el primer lugar, por la importancia de los temas que se abordan en cada uno de ellos, y para lo cual agradezco mucho el apoyo de quienes fungieron como jueces para lograr tal objetivo, en especial a mis compañeros comisionados Cynthia Patricia Cantero Pacheco y Pedro Antonio Rosas Hernández, quienes siempre han respaldado los proyectos en los que he requerido de su apoyo, por descabellados o complejos que en un inicio pudieran parecer.

Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco

Cynthia Patricia Cantero Pacheco
Comisionada Presidente del Pleno

Salvador Romero Espinosa
Comisionado Ciudadano

Pedro Antonio Rosas Hernández
Comisionado Ciudadano

Miguel Ángel Hernández Velázquez
Secretario Ejecutivo

Claudia Patricia Arteaga Arróniz
Coordinadora General de Planeación y Proyectos Estratégicos

Juan Carlos Campos Herrera
Coordinador General de Evaluación y Gestión Documental

Rocío Hernández Guerrero
Directora Jurídica

Olga Navarro Benavides
Directora de Vinculación y Difusión

Gricelda Pérez Nuño
Directora de Administración

Manuel Rojas Munguía
Director del Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales

Ricardo Alfonso De Alba Moreno
Director de Protección de Datos Personales

Revista Caja de Cristal

Salvador Romero Espinosa
Director

Elizabeth Velasco Aragón
Encargada de Edición

Juan Francisco García Gallegos
Diseño Editorial

Comité Dictaminador

Pedro Antonio Rosas Hernández
Manuel Rojas Munguía
Olga Navarro Benavides
Rocío Hernández Guerrero
Francisco Eduardo Arriola Aranda

Consejo Editorial

Augusto Chacón Benavides
Jesús Gómez Fregoso
Gabriel Torres Espinoza
Luis Miguel González
Ricardo Duarte Méndez

Así las cosas, lo que encontrarán en las páginas de este número, son una colección de 6 ensayos, que plasman la visión de dichos jóvenes en los temas que el ITEI está llamado a acercar a la sociedad, pero con un enfoque fresco y apartado de la visión tradicional de quienes integramos este Instituto y las autoridades gubernamentales. En ese tenor, considero que su contenido se trata de un muestreo, cuyo lectura nos permitirá generar una mayor consciencia de las preocupaciones y los intereses de la juventud en general, respecto a temas tales como el uso de las redes sociales digitales, los peligros de las llamadas “fake news”, los riesgos de la privacidad en el marco de las tecnologías de la información y la comunicación, y la importancia del combate a la corrupción en una democracia moderna, entre varios otros.

Hace alrededor de 2,400 años Platón señaló que el precio del desinterés social por la política es que gobiernen las peores personas y, por ello, considero que uno de los grandes retos que tenemos todos aquellos interesados en un mejor futuro global y nacional, consiste en acercar a los jóvenes a la política, lo cual por supuesto no significa pretender que todos los jóvenes se dediquen a la política, sino simplemente para que independientemente de la rama técnica, profesional y/o laboral a la que se dediquen, no pierdan el interés en ella, ni dejen de vigilar el actuar de sus gobernantes y de sus representantes, exigiendo que les rindan cuentas a través de las múltiples herramientas con las que cuentan actualmente.

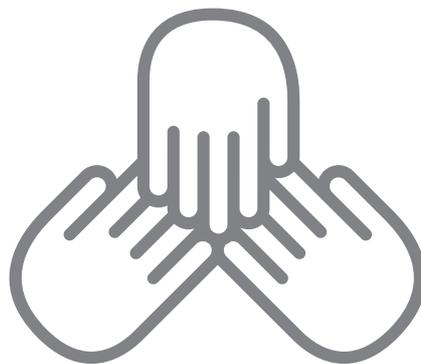
En conclusión, este espacio pretende ser una aportación, quizás minúscula pero cierta, a ese gran reto que tenemos los organismos garantes de transparencia del país para promover y fomentar la cultura de la transparencia y de la privacidad en la sociedad, como premisas para el fortalecimiento de la democracia de nuestra nación, ante un panorama político en el cual no existen señales claras de promover el fortalecimiento o preservación del Sistema Nacional de Transparencia, Información Pública y Protección de Datos Personales, cuya existencia es producto de muchas décadas de trabajo de la sociedad civil, los periodistas, los académicos y los políticos comprometidos con la rendición de cuentas y la democracia.

Muchas felicidades a los ganadores, espero y deseo que sigan siempre interesados en estos temas, y que este premio los anime a seguir escribiendo y trabajando por un México mejor. Hace alrededor de 17 años yo tuve la oportunidad de participar en la categoría juvenil del Primer Concurso Nacional de Ensayo organizado por el entonces flamante Instituto Federal de Acceso a la Información Pública (IFAI), obteniendo el segundo lugar y, desde entonces, no he dejado de interesarme y de seguir participando en este tipo de temas, pues estoy convencido que por muchos defectos que tenga, no existe otra forma de gobierno que promueva y garantice más el respeto a los derechos humanos que la democracia.

Mtro. Salvador Romero Espinosa

Comisionado Ciudadano del ITEI





#ITEISomosTodos

itei |

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



Las cuentas de redes sociales abiertas de servidores públicos, son un instrumento para la divulgación de información oficial y/o pública según criterio del Órgano Garante de Jalisco (ITEI), ¿Cuáles son los alcances frente a los derechos de relación?

Miguel Ángel Vázquez Placencia

*Titular de la Unidad de Transparencia
de Contraloría del Estado*

Resumen

El acceso a la información sobre las redes sociales de personas que, por su condición de servidores públicos, deben realizar acciones tendientes a garantizar la transparencia y la rendición de cuentas por estas vías de comunicación, al margen de la protección de su privacidad en cuanto a sus propias comunicaciones.

Las resoluciones que otorgan las bases sobre este criterio, no son determinantes para obtener los límites o ponderaciones que deben realizar los sujetos obligados, por ello, el cuestionamiento sobre ¿Cuáles son los alcances frente a los derechos de relación?, en ese sentido es la búsqueda de encontrar respuesta a la interrogante mediante la ponderación entre los derechos.

PALABRAS CLAVES:

Redes Sociales,
Privacidad, Alcances
Servidores Públicos,
Acceso a la Información

Introducción

Las cuentas de redes sociales hoy en día son canales de comunicación sumamente importantes, haciendo de éstas, una de las herramientas de enlace más relevante de nuestros tiempos, acotando las fronteras entre las personas, con una característica esencial, como lo es, una gran concentración de información, mismas, que han sido de vital aporte para el desarrollo de los Gobiernos y la sociedad.

Los diferentes actores políticos, hoy en día, pueden impactar a muchas más personas por esta vía, que, recorriendo casa por casa, sin embargo, hasta qué punto podríamos delinear en confección los derechos intervencionales, como lo son, la libertad de expresión, el acceso a la información y la privacidad.

Ante ello, existen criterios judiciales y en fecha reciente, el criterio que sostuvo el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), en los que, se determina a las redes sociales de servidores públicos, como instrumentos de divulgación de información oficial y/o pública.

Es bajo la existencia de dichas determinaciones que se busca analizar, cuales son las situaciones de aplicación y en qué lógica podría imperar una ponderación y garantía sobre aquellos derechos que participan en su ejecución o en un punto específico, sin con esto, estamos regulando la condición de extraterritorialidad de una red social. Las resoluciones que otorgan las bases sobre este criterio, no son determinantes para obtener los límites o ponderaciones que deben realizar los sujetos obligados, por ello, el cuestionamiento sobre ¿Cuáles son los alcances frente a los derechos de relación?

El Criterio 03/2018:

“...Las cuentas de redes sociales abiertas de servidores públicos, son un instrumento para la divulgación de información oficial y/o pública.

Época Segunda.

Año de emisión :2018

Materia: Acceso a la información.

Tema: Cuentas públicas de redes sociales.

Tipo de criterio: Reiterado

Las cuentas de redes sociales abiertas al público administradas por personal de los Sujetos Obligados o por un tercero autorizado, así como las de servidores públicos, que se utilicen para difundir información derivada de sus atribuciones y obligaciones, se constituyen como información pública en los términos de la Ley de Transparencia y Acceso a La Información Pública del Estado de Jalisco y sus municipios...”¹

(Lo subrayado es propio)

En ese sentido, podemos tomar como punto de partida que dicho criterio sienta sus bases en la reiteración de solicitudes de información resueltas por el órgano garante como precedentes, solicitudes que demandan contar con las redes sociales oficiales de funcionarios.

Bajo ese orden de ideas y desarticulando los posicionamientos de dicha interpretación para vincular la propiedad de una red social a la garantía de (Consultado el 12 de Octubre de 2018) determinarle como información pública, es que podríamos esquematizarlo de la siguiente forma:

RED SOCIAL----PROPIEDAD----ADMINISTRACIÓN

¿QUÉ SE PUBLICA? ---- INFORMACIÓN DERIVADA DE SUS ATRIBUCIONES

= TODO ESTO BAJO LOS TERMINOS DE LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE JALISCO Y SUS MUNICIPIOS.

Una interpretación bastante amplia para regular una plataforma a la cual se accede mediante la aceptación de un convenio de adhesión por más figura pública que pueda representarse, a la que en estricto sentido una norma

¹ ACUERDO GENERAL DEL PLENO DEL INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE JALISCO, MEDIANTE EL CUAL SE APRUEBA EL CRITERIO DE INTERPRETACIÓN 003/2018. http://www.itei.org.mx/v3/documentos/art12-14/criterios/2018/acuerdo_criterio_de_interpretacion_03-2018..pdf

de carácter estatal no podría regular, por un asunto de competencias determinada.

Plataformas que se encuentran en el mundo del internet, llamado ciberespacio que examinado por KOEPSSELL² o COHEN³, primero como una utopía, a saber, como un espacio separado; luego como isotopía, es decir, como un espacio que continua el espacio existente; y finalmente como heterotopía, en el sentido de un espacio donde las reglas ordinarias de comportamiento o conducta son suspendidas o transformadas. La heterotopía conserva su aspecto relacional que, con respecto al ciberespacio, se refiere a la conexión con el espacio físico.

Espacio que representa libertades y respetos ape- gados a derecho, como lo es el artículo 16 constitucio- nal, párrafo décimo segundo que contempla el secreto o inviolabilidad de telecomunicaciones⁴, de tal modo que cada usuario final en nuestro país según refiere le Ley Federal de Telecomunicaciones y Radiodifusión en su artículo 3, es la persona física o moral que utiliza el servi- cio de telecomunicaciones como destinatario final, sobre aquellos servicios que se prestan en internet, conceptua- lizada en el mismo numeral fracción XXXII:

“...Artículo 3. Para efectos de la presente ley se entenderá:

...XXXII. Internet: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporcióna diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto

componen Internet funcionen como una red lógica única; ...”

Empero de lo anterior, coexiste lo declarado, en el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos, que señala que:

“... Artículo 6.

...I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo 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 en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información...”

El principio de máxima publicidad que refiere el numeral transcrito, según la siguiente interpretación publicada en el Semanario Judicial de la Federación:

Época: Décima Época

Registro: 2002944

Instancia: Tribunales Colegiados de Circuito

Tipo de Tesis: Aislada

Fuente: Semanario Judicial de la Federación y su Gaceta

Libro XVIII, marzo de 2013, Tomo 3

Materia(s): Constitucional

Tesis: I.4o.A.40 A (10a.)

Página: 1899

ACCESO A LA INFORMACIÓN. IMPLICACIÓN DEL PRINCIPIO DE MÁXIMA PUBLICIDAD EN EL DERECHO FUNDAMENTAL RELATIVO.

² KOEPSSELL, David: The ontology of cyberspace: law, philosophy, and the future of intellectual property. Editorial Open Court, Illinois, 2003.

³ CHOEN, Julie: “Cyberspace as/and space”, en Columbia Law Review, Vol. 107, 2007.

⁴ “Artículo 16...
...Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley...”

Se refiere a una doble dimensión, en sentido individual y por otro social, consecuentemente entonces, la vía individual representa un respeto a las libertades tanto de recibir como de externar expresiones, que dan origen a la segunda, que es la de permitir que, con ello, el desarrollo en lo social tanto del individuo, como de la sociedad frente a sus autoridades.

La posesión de información pública, supone la acción de entregar y acceder a la misma sin necesidad de prebendas, pero en qué punto específico, contar con Facebook o Twitter, es requisito para ingresar al servicio público, por ello, la necesidad de encontrar una ponderación sólida o bien determinar la existencia oficial de aquellos entes y servidores que lo determinen.



La ponderación es la base

Las directrices por las cuales es suscrito el criterio de mérito, son tan amplias que, sin duda alguna, permiten que el objeto del presente comentario se fije sobre el balance que pudiera existir.

Los derechos que confluyen en esta determinación, en un punto representan puntos opuestos y la línea delgada sobre la cual transitan no debe estimarse con ligereza, por ende, entendiendo el derecho de acceso a la información como aquel que no solo permite acceder o reproducir, sino la generación de información como bien lo señala el objeto de la Ley General de Transparencia y Acceso a la Información Pública, otorgando razones suficientes para concatenar las disyuntivas existentes con la privacidad o el ejercicio de libertad de expresión.

Sobre el punto específico, la Suprema Corte de la Nación, en la resolución del Amparo Directo 3/2011. Caso “Los demonios del Edén”, para establecer lo denominado como “doctrina específica de los derechos en conflicto” (información y vida privada), refirió que:

- a) La presencia de un interés público en la difusión de la información relativa a la vida privada de una persona elimina el carácter de ilícito o antijurídico de una intromisión a un derecho de personalidad, como lo es la vida privada;

- b) En atención al llamado sistema dual de protección, las personas denominadas figuras públicas tienen menor resistencia que los particulares ante intromisiones en sus derechos de personalidad;
- c) De la adopción del sistema dual se desprende el criterio de “malicia efectiva” para determinar la responsabilidad. En todo caso, la “malicia efectiva” dependerá de un ámbito de proyección de cada persona (será menor en personas con proyección pública);
- d) Al determinar la invasión a la intimidad, también resulta importante analizar si la vida privada había o no sido divulgada con anterioridad. La divulgación previa es un factor que disminuye la intensidad de violaciones similares en el futuro.

La presencia de una red social abierta en el criterio resuelto por el ITEI, como elemento supremo, obliga a la consideración de una red social como información pública, basándonos en un concepto de “red” para las ciencias sociales como el grupo de personas u organizaciones que interactúa y se interrelaciona de alguna manera; por otro lado, contemplamos el concepto que señala el reporte sobre la libertad en la conectividad y libertad de expresión elaborado por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), que refiere que una red social es el servicio

que prevé herramientas para construir vínculos entre personas, en el que cada usuario puede tener su propio perfil y generar vínculos con otros usuarios, estableciendo nodos homogéneos de sus actores; en años recientes, las redes han sido conceptualizadas o definidas de tres maneras: como estructuras, como procesos relacionales o como herramientas o instrumentos de gestión utilizados en la administración pública (Ramírez, E. 2016, pág. 36), la consideración de apertura en esa construcción racional, trae a colación, la privacidad de las personas como un derecho que puede contraponer los argumentos que se sostienen y que no son en menoscabo de la libertad de expresión, a decir de los hechos, la protección de este derecho ha ocupado sendas discusiones sobre cómo lograr su mayor y más eficiente tutela; y no es para menos, pues en una sociedad informatizada y ampliamente dependiente de las nuevas tecnologías de la información y la comunicación, es indefectible brindar las mayores garantías de protección para quienes forman parte de ella.

Con el advenimiento de las nuevas tecnologías surgió un gran problema: el hecho de que éstas podrían ser intrusivas en la vida privada de las personas. Mundialmente, la protección del uso de datos personales, vinculado estrechamente con la privacidad de las personas, ha venido en aumento por ciertos mecanismos legales de normas generales o específicas, convencionales o constitutivas, que de una u otra manera establecen reglas mínimas para el tratamiento de datos y para la habilitación de los mismos en las bases de datos, así como en la protección de los derechos de quienes están registrados en dichas bases de datos.

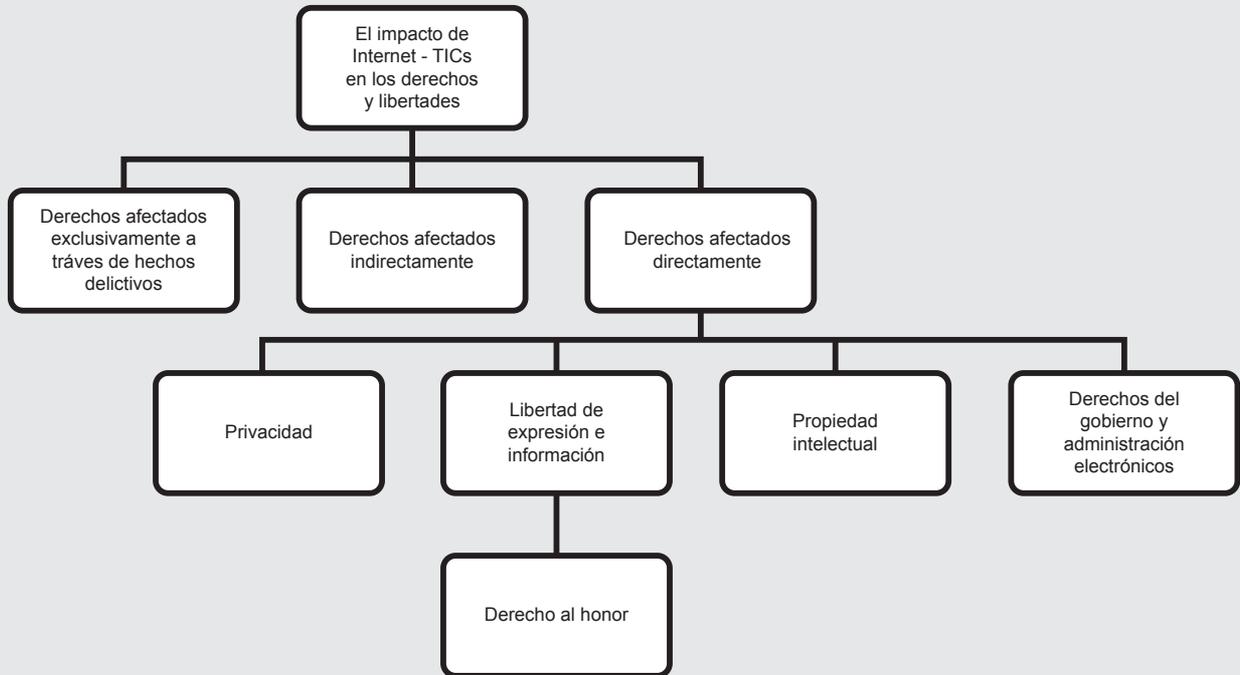
Si bien desde el punto de vista filosófico se hace la distinción entre lo íntimo y lo privado, desde el punto de vista jurídico, se habla del derecho a la intimidad para aludir al derecho a la reserva de la vida privada (Delpiazzo, 2012, pág. 5). Este derecho se encuentra consagrado en diversos instrumentos jurídicos internacionales, y teniendo como antecedente principal a la Declaración Universal de los Derechos Humanos de 1948, la cual, establece en su artículo 12, que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Como parte de las respuestas jurídicas a los nuevos fenómenos sociales que se han presentado en la sociedad, como la irrupción de las nuevas tecnologías, se han configurado marcos de referencia en cuanto a individualizar a las personas en su entorno digital y sobre el cómo son contemplados los alcances de su privacidad, un ejemplo claro es la llamada neutralidad de la red.



El impacto sobre los derechos y libertades sobre la persona como lo vemos en el siguiente cuadro:

Figura 1. El impacto de Internet y las TICs sobre los derechos y libertades



Fuente: García, P. (2014), *Derechos y libertades, internet y tics* (pág. 21) España: Tirant lo Blanch.

Es bajo ese impacto, que debemos buscar algo más que la simple determinación de sujetos obligados, puesto que, en ninguna ley se dota de atribuciones específicas para contar con una vía de comunicación frente a la sociedad a través de redes sociales.

Al analizar este criterio y las resoluciones que llevaron al órgano garante a estimar una red social como “abierta”, fija pautas para una ponderación más efectiva sobre la aplicación, ya que la preocupación sobre la privacidad desde otro punto de vista, es inherente en mayoría, al jurista o legislador, puesto que los individuos ya han cambiado la concepción a una privacidad en sentido social, como ese derecho de estar con amigos virtuales, venciendo barreras territoriales, adheridos a las redes sociales mediante convenios genéricos de voluntad.

Fijar como regla general que las redes sociales de servidores públicos sean abiertas, no permite la distinción entre condicionantes que revisten la función pública frente a la privacidad o bien, la libertad de expresión versus el honor de cada uno de los individuos en esa vida virtual, que por demás está recordar, la existencia sobre el olvido a que se tiene derecho.

Conclusión

Ya nada volverá a ser como antes. La irrupción de las nuevas tecnologías de la información y la comunicación han moldeado nuestra realidad a tal grado, que ha sido necesario adecuar nuestro entorno para que su recepción sea venidera. Desde la industria, hasta la política, pasando por la ciencia y las relaciones personales, prácticamente todo. Mientras tanto, el Derecho se ha visto en

la imperiosa necesidad de adoptar estas nuevas tecnologías, útiles tanto en la impartición como en la administración de la justicia.

Hemos atestiguado que las nuevas tecnologías, si bien son neutras, de cómo se utilicen dependerá si son benignas o malignas para nuestro desarrollo. Sin que se convierta en la discusión principal, podríamos señalar a tecnologías disruptivas como la inteligencia artificial fuerte, la cual estará próximamente equipada en diversos equipos tecnológicos y que los dotará de autonomía de decisión, sin necesidad de que ningún humano intervenga. La inteligencia artificial fuerte, bien puede ser de gran utilidad a la humanidad; sin embargo, también podría significar su destrucción, por más que parezca sacado de un libro de ciencia ficción, el aniquilamiento de la humanidad podría estar en manos de equipos tecnológicos dotados de inteligencia artificial fuerte, tales como los drones y robots.

Como prioritario resulta entender que se requiere claridad en la regulación, pero más aún, una adaptación a los nuevos anales de la vida pública en esta vida virtual, para acceder con mayor efectividad y certeza a contenidos y acelerar la comunicación entre los servidores públicos y la sociedad.

En esta era de la información, no todo lo privado debe ser público, ni todo lo público puede ser privado, sin que medie un estudio para ser reservado o bien considerado un archivo histórico con todos sus elementos para ser consultado como fuente de acceso público.

Gran reto de la Reforma de Transparencia, que por fin establece en todas sus vertientes pisos y condiciones iguales en todos los sujetos obligados.

Fuentes de referencia

Constitución Política de los Estados Unidos Mexicanos, disponible en: <http://www.diputados.gob.mx/LeyesBiblio/index.htm>

Delpiazzo, C. (2012). Relaciones entre Privacidad y Transparencia. En G. Tenorio Cueto, Los Datos Personales en México, perspectivas y retos de su manejo en posesión de particulares (pág. 258). México: Porrúa.

García, P. (2014). Derechos y libertades, internet y tics (pág. 21) España: Tirant lo Blanch.

Gordillo, A. (2013). Teoría General del Derecho Administrativo, Tomo XIII.

Buenos Aires: Fundación de Derecho Administrativo.

Hamelink, C. (2015). La ética del ciberespacio. México: Siglo XXI.

López Azpitarte, E. (1990). Ética y vida. Madrid: Paulinas.

Ley Federal de Telecomunicaciones y Radiodifusión, disponible en: <http://www.diputados.gob.mx/LeyesBiblio/index.htm>

Ley General de Transparencia y Acceso a la Información Pública, disponible en: <http://www.diputados.gob.mx/LeyesBiblio/index.htm>

Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus municipios, disponible en: <https://www.itei.org.mx/v4/index.php/normatividad>

Ramírez, E. (2016). Segunda dimensión: Conceptualización del fenómeno, en Análisis de redes sociales para el estudio de la gobernanza y políticas públicas (pág. 36). México: CIDE.

Recio, M. (2015). La protección de datos en el ámbito de las telecomunicaciones e internet (39). México: INFODF.

Téllez Valdés, J. A. (2009). Derecho Informático. México: McGrawHill.



Miguel Ángel Vázquez Placencia

Licenciado en Derecho por la Universidad de Guadalajara, a lo largo de su vida profesional, se ha desempeñado en diversos cargos, tales como: Titular de la Unidad de Transparencia de Contraloría del Estado, Director de Protección de Datos Personales del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco; Jefe de Protección de Datos Personales del Consejo de la Judicatura del Estado de Jalisco, Consultor en Protección de Datos Personales y Normas ISO, además de Profesor en la Universidad de Guadalajara.



Retos y peligros de vivir sin privacidad en las TIC

Jersain Zadamiq Llamas Covarrubias

*Co-fundador del movimiento
internacional Legal Hackers*

Resumen

PALABRAS CLAVES:

Datos Personales,
Privacidad, Internet,
Acceso No Autorizado,
Ciberalfabetización,
Ciberhigiene

Con el presente ensayo se pretende abordar una concepción general sobre lo que es la privacidad, así mismo se realiza un análisis de los retos y peligros de vivir sin privacidad y la importancia de la protección de datos ante el rompimiento de paradigmas tradicionales por las nuevas tecnologías disruptivas, concluyendo en que la ciberalfabetización y ciberhigiene son pilares fundamentales para combatir las amenazas, revelaciones, riesgos y vulnerabilidades que pudieran convertirse en incidentes de seguridad que atenten contra la injerencia arbitraria de la vida privada.

Introducción

En las sociedades contemporáneas, las TIC son la espina dorsal del desarrollo. La información se convierte en conocimiento y poder, los datos personales son tan importantes que transmutan la forma en la que percibimos el mundo y se convierten en el petróleo del siglo XXI. Pero esto no termina aquí, ya que con la llegada del Machine Learning, Deep Learning e Inteligencia Artificial en armonía con el Big Data todo se mueve tan deprisa en “Velocidad, Variedad, Volumen, Valor y Veracidad” (Martínez, 2018: 262-263), acorralando al sector público, privado y sociedad civil organizada, a tomar decisiones precipitadas y en ocasiones no del todo estudiadas, pues gracias a la celeridad con la que se mueve el mundo digital, pareciera que es humanamente imposible mitigar los incidentes de seguridad o tomar un breve espacio para hacer conciencia sobre los datos personales y la privacidad.

En el informe del Foro Económico Mundial (2019: 18), titulado The Global Risks Report 2019 14th Edition, específicamente en la encuesta de percepción de riesgos mundiales, coloca los ciberataques: robo de datos/dinero en el cuarto lugar con un 82%. Así mismo en el informe Cost of a Data Breach Report 2019, elaborado por IBM Security y Ponemon Institute (2019: 3), cada registro perdido o robado con información sensible o confidencial tiene un precio de \$150 dólares por registro y el promedio mundial de registros expuestos por cada incidente de seguridad es de 25,575.

Por su parte, la empresa internacional LLOYD'S (2018a: 20), en su Informe de riesgos emergentes 2018, relacionado con la Tecnología, ha comunicado que a nivel mundial, se estima que el cibercrimen le cuesta a las empresas \$400 mil millones al año, lo que significa que los riesgos cibernéticos son uno de los principales problemas que las empresas deben tener en cuenta cuando se trata de su capacidad de recuperación y planificación de continuidad. En el mismo orden de ideas, el “2017 fue uno de los años más costosos para las catástrofes naturales en la última década. Nuevas amenazas como la cibernética plantean diferentes riesgos para el crecimiento económico mundial” (LLOYD'S 2018b: 46). Pudiendo deducir que un ataque cibernético es más costoso que un desastre natural.

Privacidad

Definir la privacidad es algo complejo, pues existen diversos enfoques, perspectivas y encuadres epistemológicos, pero lo cierto es que este concepto pese a que se defina directa o indirectamente, todo concluye en que es un pilar insustituible de la dignidad humana y por ende de los derechos humanos.

En la doctrina se encuentran diversos conceptos de privacidad, no obstante, a mi consideración son dos definiciones las que marcan el preámbulo teleológico, la primera que es la más primigenia y posiblemente el arquetipo es el “derecho a que nos dejen en paz” (Warren & Brandeis, 1890). La segunda es el derecho a controlar el uso que otros hacen de las informaciones que nos afectan (Westin, 1968).

Una definición ecléctica de privacidad, es la que define la Comisión Interamericana de Derechos Humanos (2017) donde señala que:

El derecho a la privacidad protege al menos cuatro bienes jurídicos, a saber: a) el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas; b) el derecho a gobernarse por reglas propias según el proyecto individual de vida de cada uno; c) el derecho al secreto respecto de lo que se produzcan en ese espacio reservado con la consiguiente prohibición de divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona; y d) el derecho a la propia imagen (p. 78).

En resumen, se ha definido la privacidad desde diversos encuadres epistemológicos, y es necesario demostrar dos enfoques respecto a la privacidad y datos personales. Pues así, como en el mundo existe el lenguaje binario representado en 1 y 0, en verdadero o falso, también podremos encontrar diversos enfoques en la privacidad. Tal es el caso de David Cuartielles (2019), el fundador de Arduino, que dice que la “gente está muy equivocada

da pensando que sus datos son super valiosos... que la privacidad de los datos personales está sobrevalorada... porque cuanto más gente los tenga menos valen para quienes los quieren para su beneficio”, mientras que desde otra perspectiva Bruce Schneier (2006) un reconocido criptógrafo, dice que “la privacidad es un derecho humano inherente y un requisito para mantener la condición humana con dignidad y respeto... la privacidad nos protege de los abusos de quienes están en el poder, incluso si no estamos haciendo nada malo en el momento de la vigilancia”.

Aunque hemos abordado conceptos y enfoques de privacidad, sin dejar por un lado la práctica y facticidad, la realidad es que se puede inferir que no hay derechos absolutos, pero a mi percepción esto no es del todo cierto, ya que en un sentido lógico la vida y la libertad son derechos absolutos universales, pero también lo es la intimidad. De manera más puntual, la Real Academia Española (RAE) da luz respecto a una separación entre privacidad e intimidad, donde la intimidad es la “zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia” y cómo privacidad al “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”, esto es que no existe ninguna regla, locución sentenciadora o garantía para poder violar la intimidad, incluso ni con excepciones constitucionales o mandamientos escritos, en pocas palabras la intimidad es un derecho inviolable inmutable absoluto universal y la privacidad pese a que es un derecho fundamental, está sujeta a cada caso en concreto.

Además, en este mundo tan hiperconectado y con tantas violaciones de datos, pese a que en un primer plano pudieran colisionar la libertad de expresión y la privacidad, también la privacidad entra en conflicto con la seguridad nacional, y es aquí donde emerge un ciudadano que lucha por su privacidad, con ideologías de Cypherpunk, Lex Cryptographica o Dataísmo, con técnicas de cifrado o anonimato, ya sea utilizando algún seudónimo, software como TOR (The Onion Router), o incluso una VPN Virtual Private Network, en español red privada virtual.

Retos y peligros de privacidad en el siglo XXI

En un primer plano contamos con el Internet; un espacio sin color, nacionalidad, política o religión, que puede ser una herramienta pero a la vez un arma. Un ejemplo es la suplantación o robo de identidad como el riesgo más común, ya que pueden realizarse actos ilícitos con diferentes niveles de dificultad, desde crear un perfil falso y hacerse pasar por alguien más, ingeniería social o hasta utilizar métodos técnicos para lograr un acceso no autorizado. También existen métodos no tan especializados como doxing, acoso, sexting, sextorsion o incluso comentarios de odio, que dañan indirectamente a la privacidad, protegiendo los derechos a la propia imagen, reputación y al honor, creando un menoscabo e injerencia arbitraria en la vida privada.

Otro reto que deberá abatir nuestra sociedad del conocimiento, es el uso de drones, pues pese a que en México y otros países ya exista su regulación especial, requiriendo una licencia para aquellos que dispongan de ciertas características, en la práctica pueden ser utilizados de manera ruin, para vigilar sin el consentimiento de las personas, y es claro que por las características fisonómicas del humano es imposible mitigarlos de manera natural.

Además, otro reto fundamental es el reconocimiento facial, un claro ejemplo es Facebook, donde una Corte Federal de Apelaciones de Estados Unidos dio la razón a un grupo de denunciantes que señalaron que el reconocimiento facial de esta empresa, viola el acta de privacidad de información biométrica (BIPA) del Estado de Illinois (Patel vs Facebook), que prohíbe la recolección de datos biométricos incluida esta tecnología, claramente sin autorización ni consentimiento informado. Es así que Facebook el 03 de Septiembre del 2019 emitió un comunicado donde expresaba que todas las características de reconocimiento facial, incluyendo etiquetado, estarán apagadas por defecto para usuarios nuevos, para los usuarios ya registrados posterior a este comunicado deberían desactivarlo manualmente. (R3D.mx, 2019).

De igual modo, respecto al reconocimiento facial, cuando se une con el Internet de las Cosas, con su comunicación de persona a persona (P2P), persona a máquina (P2M), e inclusive de máquina a máquina (M2M), transforman la manera en la que percibimos el mundo. En primer término, tenemos las cámaras de vigilancia, que su utilización de manera desmedida y no apegada a derecho con la tecnología innovadora de reconocimiento facial, pueden convertir a las naciones en el Gran Hermano de George Orwell. No obstante, ante esta situación desde el ámbito de la moda han diseñado prendas y accesorios personales para evitar ser captados y reconocidos por esta tecnología (Esage, 2019).

Siguiendo con el Internet de las Cosas, que son dispositivos interrelacionados con identificadores únicos y capacidad de transferir datos, llegan los asistentes de voz, que en este pleno año 2019 diversas empresas como Amazon, Google y Apple reconocieron que almacenaban y enviaban las conversaciones a trabajadores que escuchaban lo que dicen los usuarios para mejorar el servicio (elmundo.es, 2019).

Pero esto no concluye aquí, pues si mezclamos Internet, Big Data e Internet de las Cosas, es evidente que tenemos información en dispositivos y sensores conectados que incluso pueden comunicarse de máquina a máquina sin intervención humana, y estos dispositivos son vulnerables a acceso no autorizado u otros ciberdelitos, ya que en ocasiones su software se encuentra desactualizado, vulnerable o desde su fabricación contienen contraseñas genéricas. Si bien podemos encontrarnos con datos identificativos; de origen; ideológicos; sobre la salud; laborales; patrimoniales; sobre procedimientos administrativos y/o jurisdiccionales; académicos y de tránsito y movimiento migratorios, lo cierto es que con las TIC, nacen nuevas formas de información concerniente a personas físicas identificadas o identificables, incluso cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, aún si se puede “singularizar, vincular o inferir la información relativa a una persona” (Grupo de Trabajo Artículo 29, 2019: 3).

Dicho lo anterior, independientemente de la jurisdicción, pese a que ya se encuentra una homologación a que existen datos personales en identificadores en línea como Cookies; Web Beacons; Metadatos y direcciones IP (en algunos casos), entre otros. A pasos agigantados el mundo virtual trasciende al material, y con todos estos sensores del Internet de las Cosas nacen nuevos retos, pudiendo hacer identificables “la forma de oprimir un teclado y la forma de caminar” (INAI, 2018: 10-11), o también algo que pareciera de ciencia ficción; el pentágono tiene un láser que puede identificar a las personas a distancia, por el latido de su corazón, captando una firma cardiaca única a 200 metros de distancia, incluso a través de la ropa (Hambling, 2019).

En el mismo sentido, si ya se abordó el utilizar la tecnología como un objeto y un medio, ahora surge una nueva forma de vivir la tecnología, utilizándola como fin, y es cuando el ser humano quiere trascender en sus capacidades o suplir déficits, emergiendo nuevas ideologías de transhumanismo y posthumanismo, especialmente con el fenómeno de los cyborgs (ser de materia orgánica y dispositivos tecnológicos). Un caso es Steve Mann (2012), que fue agredido por empleados de Mcdonald's en Francia, por utilizar un EyeTap (pantalla incrustada en la cabeza que se coloca delante del ojo con funciones de cámara y pantalla) con el argumento de proteger el derecho a la privacidad del personal y clientes. Ahora imaginemos a otros cyborgs, como Neil Harbisson con su antena para escuchar los colores, o Rob Spence con su Eyeborg con su ojo biónico con cámara. ¿Esto podría violar la privacidad?



Conclusiones

Después de abordar de manera exhaustiva la definición, riesgos y retos de la privacidad, es necesario concluir que lo más importante y la solución a la mayoría de los problemas de violación de datos son las personas. Ya que sería muy sencillo decir que todo se resolverá gracias a una tecnología disruptiva, por mencionar algunas de la industria 4.0 como: los Sistemas de integración; máquinas y sistemas autónomos (robots); Internet de las cosas (IoT); Manufactura aditiva; Big data y análisis de grandes datos; Computación en la nube; Simulación de entornos virtuales; Inteligencia Artificial; Ciberseguridad; y Realidad Aumentada (Basco, Beliz, Coatz & Garnero, 2018: 26-29), así como Blockchain o conocida como la Cadena de Bloques.

Lo anterior lo sustentó con un sencillo ejemplo, que fue el de las elecciones para la presidencia de México del año 2018, donde algunos ciudadanos subieron su foto con el pulgar demostrando que ya habían votado, sin embargo, expertos afirmaron que al realizar esta acción era posible que un ciberdelincuente pudiera extraer la huella dactilar y utilizarla para cometer algún delito, fraude cibernético o acceder a un sistema privado (Meza, 2018). Dicho lo anterior se comprueba que el eslabón más débil y a la vez el más fuerte son las personas, pues todo radica en la educación digital. La Unión Europea en su Reglamento sobre ciberseguridad 2019, menciona dos conceptos clave que deberán forjarse como pilares fundamentales en las sociedades de la información, los cuales son ciberhigiene y ciberalfabetización.

Las formas, métodos y sistemas del pasado fracasaron porque nunca consideraron la privacidad como un pilar fundamental para proteger el futuro. Y es necesario tener presente que “ninguna generación puede atar con sus leyes a las generaciones futuras” (Rodotà, 2014: 30), y si en el pasado la privacidad ha sido derrotada y olvidada, es menester luchar por el derecho de la misma.

Debemos abandonar la idea de que la privacidad ha muerto y que debemos olvidar, que existen otros principios que deben trascender ante nuestros derechos originarios. Pues la privacidad es sinónimo de sociedad libre, es el aliento hacia un plan de prosperidad, aspira a un

mundo donde cada quien sea dueño de sus datos. Es necesario entender, que la libertad se basa en la privacidad, que los derechos humanos y su dignidad humana deben encontrar su mejor aliado en este principio.

Debemos recordar y reforzar el asunto del derecho a la propiedad de los datos, donde realmente le pertenezcan a las personas, donde la gente pueda controlar sus propios datos, obtener el derecho de decidir sobre su identidad digital, qué compartir y qué no, respetar y evitar las injerencias arbitrarias a la vida privada, conviviendo con sistemas descentralizados y distribuidos como pilares de una sociedad abierta, libre y anónima, expresándonos de manera respetuosa sin miedo a represalias, pues únicamente de esta manera se construirá una sociedad libre, donde de manera corpórea e incorpórea, individual y colectiva, todos podrán controlar sus propias vidas. Vale la pena forjar un camino donde podamos elegir controlar nuestro destino y lo que somos, a nosotros mismos, somos datos e información. En equilibrio la privacidad y legalidad, se convierten en una lucha por el derecho.



Referencias

- Basco A., Beliz G., Coatz D. & Garnero P. (2018). Evolución de las Revoluciones Industriales. Banco Interamericano de Desarrollo. Recuperado de: <https://bit.ly/33mYiOy>
- Comisión Interamericana de Derechos Humanos CIDH. (2017). Estándares para una Internet Libre, Abierta e Incluyente. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Recuperado de: <https://bit.ly/2pOJrOz>
- Cuartielles, D. (2019, 02 de noviembre). David Cuartielles: “La privacidad de los datos como concepto ético es muy flexible”. Elpais España. Recuperada de: <https://bit.ly/2Ct1Cfz>
- Esage, A. (2019). 8 métodos para esquivar cámaras y software de reconocimiento facial. Recuperado de: <https://bit.ly/2qpUxtn>
- Elmundo.es (2019). Apple, Google y Amazon escuchan: ¿es seguro hablar con un asistente de voz?. Recuperado de: <https://bit.ly/36GZjU2>
- Foro Económico Mundial. (2019). The Global Risks Report 2019 14th Edition. Recuperado de: <https://bit.ly/33mzjLx>
- Grupo de Trabajo Artículo 29. (2014). Dictamen 05/2014 sobre técnicas de anonimización. Recuperado de: <https://bit.ly/33pEz0Q>
- Hambling, D. (2019). The Pentagon has a laser that can identify people from a distance—by their heartbeat. Recuperado de: <https://bit.ly/2qo5fR0>
- IBM Security & Ponemon Institute (2019). Cost of a Data Breach Report 2019. Recuperado de: <https://ibm.co/2NNMRct>
- INAI. GUÍA para el Tratamiento de Datos Biométricos. Recuperado de: <https://bit.ly/2rapZMn>
- LLoyd's. (2018a). Emerging Risk Report 2018 Technology. New realities Risks in the virtual world, Recuperado de: <https://bit.ly/32mdQB4>
- LLoyd's. (2018b). A world at risk Closing the insurance gap, Recuperado de: <https://bit.ly/32nx8pw>
- Mann, S. (2012). Augmediated* Reality and “McVeillance”. Recuperado de: <https://bit.ly/2PMOSrX>
- Martínez, R. (2018). Capítulo 11 Inteligencia Artificial, Derecho y Derechos Fundamentales. M. Barrios & J. Torregrosa (Ed.), Sociedad Digital y Derecho. (pp. 262-263). Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. Madrid. Recuperado de: <https://bit.ly/2WKmpED>
- Meza, E. (2018). Compartir fotos del voto con tu huella puede vulnerar tu seguridad. Recuperado de: <https://bit.ly/2PXyNiW>
- R3d.mx (2019). facebook desactiva por defecto el reconocimiento facial para usuarios nuevos. Recuperado de: <https://bit.ly/2PXnCqR>
- Rodotà, S. (2014). El derecho a tener derechos. Editorial Trotta.
- Schneier, B. (2006). The Eternal Value of Privacy. Recuperado de: <https://bit.ly/2rjDrOf>
- Warren S., Brandeis L. (1890). The Right to Privacy. Harvard Law Review Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220 (28 pages). Recuperado de: <https://bit.ly/36CTnel>
- Westin, A. (1968). Privacy And Freedom, Washington and Lee Law Review. Recuperado de: <https://bit.ly/2Njx3z4>



Jersain Zadamig Llamas Covarrubias

Es Abogado por la Universidad de Guadalajara y Maestrante en Derecho Constitucional y Administrativo por la misma. Especialidad en derecho y nuevas tecnologías de la información.

Publicaciones: libro “Internet ¿Arma o Herramienta?” (2018) UdG, revista ciencia de la legislación de la Universidad del Salvador en Argentina, Revista Informática Jurídica en España, y en el Congreso del Estado de Oaxaca.

Es un activista y pionero en derecho y nuevas tecnologías de la información en Latinoamérica, publicando en diversos medios en Perú, Venezuela, Uruguay y Chile. Es co-fundador del movimiento internacional Legal Hackers en la ciudad de Guadalajara.



Libertad de expresión, información y credibilidad: Las fake news en tiempos violentos

Ylnerid Yleannis Morales Colmenares

*Estudiante de Comunicación y medios digitales de
la Universidad del Valle de México*

Resumen

PALABRAS CLAVES:

Fake News, Libertad
de Expresión,
Seguridad, Medios de
Comunicación

En la actualidad existen diferentes tecnologías, como las redes sociales, que han sustituido los medios de comunicación tradicionales, impidiendo la verificación de la información y provocando revuelo en la población por los problemas que dice existen en la sociedad. Este tipo de incertidumbre lleva a las personas a actuar por instinto sin verificar la información, provocando que la libertad de expresión, por primera vez, sea un problema para la seguridad.

I. Introducción

Dentro de la influencia recíproca humana existe un proceso que se lleva a cabo para poder interactuar con la información; en la actualidad muchas de estas formas se han modificado en el mundo.

De acuerdo con Bateson y Ruesch (1986), el concepto de comunicación incluye todos los procesos mediante los cuales las personas se influyen mutuamente. Todas las acciones y los eventos se convierten en aspectos comunicativos tan pronto como son percibidos por el ser humano; implicando, que tal percepción modifica la información que una persona poseía y, por tanto, influye en ella.

A partir de estas interacciones, los seres humanos crean habilidades y realizan acciones que están principalmente influenciadas por los medios que consumen, ya sea de manera tradicional o aquellos que forman parte de la primera era del periodismo, las redes sociales y páginas web.

Esta nueva era ha permitido que la información sea accesible para todos y a su vez cambió, de manera importante, el proceso de comunicación actual. La producción de material tan extenso permite que los individuos creen un estándar de lo que es aceptable y lo que no, volviéndose más exigente con el tiempo y reclamando contenido de calidad, que cumpla con el derecho de libertad de expresión.

Los medios de comunicación tradicionales (prensa, radio y televisión) ya no poseen la relevancia de antes, ni inspiran la confianza suficiente en la sociedad, por lo tanto, las redes sociales han tomado relevancia en cuanto a la comunicación de noticias oficiales o situaciones que los diarios o televisoras no quieren cubrir, razón por la cual, se ha ganado confianza la credibilidad en estos medios permitiendo que sean fuentes confiables.

Si bien estas redes sociales ofrecen información al momento y que, a veces, no se publica en otros medios, también pueden tener consecuencias mortales que afectan la seguridad y privacidad de estos, refiriéndose a las noticias que se generan para causar un impacto en la sociedad y no se tomen en cuenta otros problemas más grandes en la misma, como la pobreza, la delincuencia, la corrupción y el acceso a la educación, pudiéndose revelar la información confidencial que en la actualidad es la causante de muchos problemas a nivel económico y político.

Tomando en cuenta que las redes sociales en México respetan el derecho a la libertad de expresión, es necesario destacar que también existe una falta de regulación en cuanto a las fuentes de la información que se difunde, situación que dificulta y confunde a los receptores porque en vez de corroborar la noticia solo se conforman con recibirla, provocando caos que pueden llegar a ser mortales.

II. Desarrollo

El caos y la “desestabilización” de la sociedad por culpa de Fake News es un problema usual en el Siglo XXI, en especial por la aparición de las redes sociales que hacen más sencilla su difusión y acercamiento a los individuos,

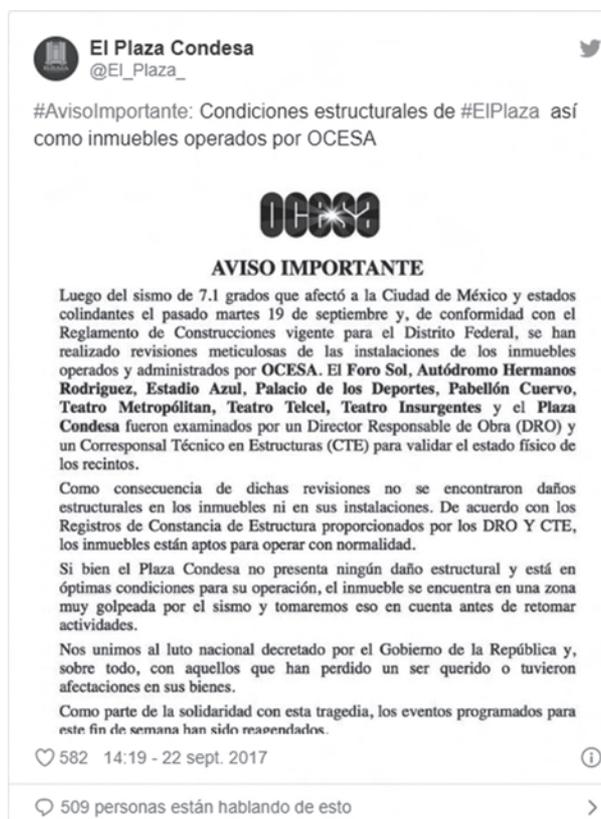
que ha llevado a consecuencias fatales en algunos casos, como:

1. Caso Condesa

A consecuencia del terremoto de 7.1 grados el 19 de septiembre del año próximo pasado, en Ciudad de México, se comunicó por medio de la red social Twitter sobre el posible colapso de El Plaza Condesa (entre América y División del Norte) en Coyoacán que tenía problemas de estructura y posibilidad de derrumbe.

Debido a la conmoción, la información se esparció por otros medios sin esperar la confirmación de la compañía dueña del establecimiento y provocó que las personas dejaran de visitar la plaza, pidiendo de igual manera por Twitter un reembolso por los boletos a los eventos que se celebrarían ahí.

Luego de tanta especulación, la cuenta oficial de El Plaza Condesa decidió aclarar los rumores y asegurar que el espacio era seguro, así como confirmar que los eventos planificados seguían en pie (Ver Imagen 1.0).



El Plaza Condesa
@El_Plaza_

#AvisoImportante: Condiciones estructurales de #ElPlaza así como inmuebles operados por OCESA

OCESA

AVISO IMPORTANTE

Luego del sismo de 7.1 grados que afectó a la Ciudad de México y estados colindantes el pasado martes 19 de septiembre y, de conformidad con el Reglamento de Construcciones vigente para el Distrito Federal, se han realizado revisiones meticulosas de las instalaciones de los inmuebles operados y administrados por OCESA. El Foro Sol, Autódromo Hermanos Rodríguez, Estadio Azul, Palacio de los Deportes, Pabellón Cuervo, Teatro Metropolitano, Teatro Telcel, Teatro Insurgentes y el Plaza Condesa fueron examinados por un Director Responsable de Obra (DRO) y un Corresponsal Técnico en Estructuras (CTE) para validar el estado físico de los recintos.

Como consecuencia de dichas revisiones no se encontraron daños estructurales en los inmuebles ni en sus instalaciones. De acuerdo con los Registros de Constancia de Estructura proporcionados por los DRO Y CTE, los inmuebles están aptos para operar con normalidad.

Si bien el Plaza Condesa no presenta ningún daño estructural y está en óptimas condiciones para su operación, el inmueble se encuentra en una zona muy golpeada por el sismo y tomaremos eso en cuenta antes de retomar actividades.

Nos unimos al luto nacional decretado por el Gobierno de la República y, sobre todo, con aquellos que han perdido un ser querido o tuvieron afectaciones en sus bienes.

Como parte de la solidaridad con esta tragedia, los eventos programados para este fin de semana han sido reprogramados.

582 14:19 - 22 sept. 2017

509 personas están hablando de esto

2. Caso de Acatlán de Osorio

Después de la difusión, principalmente, de una cadena de WhatsApp entre los pobladores de Acatlán de Osorio en Puebla fueron linchados un joven estudiante de 22 años, Ricardo Flores Rodríguez, y su tío de 43 años, Alberto Flores Morales, que era albañil y trabajaba en la siembra de su parcela.

Uno de los mensajes difundidos decía: “Comunicado importante: si tiene hijos en la escuela me pidieron de favor que yo informara, vaya por ellos, mande por ellos, pida por favor, de paso, se los traigan por ahí, hay que prevenir si ven algo sospechoso suban a las redes para apoyarnos, de preferencia en las áreas más marginadas se puede prestar esto de robo, secuestro y hasta para comercializar sus órganos de antemano gracias cuidemos de nuestros hijos y a nuestra sociedad, donde vivimos, gracias su amigo tecuanito en vivacho cuídense”.

El caso se difundió luego de que los hombres fueran detenidos por uniformados municipales y llevados a la comisaría, donde fueron encerrados y luego sacados por los lugareños acusándolos de intentar robarse a dos niños.

Gracias a videos tomados durante el acto por medio de la red social Facebook, se reconoce que el primer ataque hacia los acusados fue por medio de golpes y luego procedieron a prender en fuego a los dos hombres.

Luego de minutos en fuego, se capturó el momento en el que Don Alberto se trata de reincorporar y sentarse, pero un lugareño le lanzó gasolina para avivar las llamas.

Este caso causó gran revuelo en la población mexicana debido a la seriedad de sus consecuencias, donde los actos difundidos por un mensaje llevaron a las personas a asesinar a dos miembros de la comunidad por miedo a la seguridad de sus hijos, donde si ellos no cuidan de sí mismos nadie lo hará, mostrando la desconfianza en los cuerpos policiales y procesos de investigación de estos.

3. Caso de Guanajuato

Siguiendo los casos de desabasto de gasolina en varias regiones del país, se difundió la noticia sobre una presunta falta de combustible en la ciudad de León, en donde el gobernador de Guanajuato, Diego Sinhue Rodríguez Vallejo, desmintió la noticia por medio de la red social Twitter (Ver imagen 2.0).



La noticia se esparció por el estado cuando trascendió una nota en la que se informa que Petróleos Mexicanos había suspendido el ducto Salamanca-León como estrategia contra el huachicol.

La consecuencia más grave se obtuvo cuando un hombre que esperaba comprar gasolina intentó meterse en la fila, molestando a otro que provocó que sacara un arma de fuego y le disparó.

Después del percance, la Procuraduría Federal del Consumidor (Profeco) por medio de la cuenta oficial de Twitter asegurando que “en Guanajuato no hay desabasto de gasolina. Hace unos momentos hablé con Javier González, director de logística de Pemex y me asegura que hay suministro normal. No hay razón para hacer filas, sí hay gasolina” (Ver imagen 3.0, próxima página).

#ProfecoInforma No hay desabasto de gasolina en León, Guanajuato.

Desde el mes de junio, el gasoducto Salamanca-León se cierra hasta por un día para reparar daños causados por huachicoleros y ese corte se suple con pipas.

No hagas caso ni compartas información falsa.

#ProfecoInforma

En León, Guanajuato no hay desabasto de gasolina.

No compartas información falsa, ni realices compras de pánico.

PROFECO

261 18:52 - 23 oct. 2019

295 personas están hablando de esto

III. Conclusión

Si bien es cierto que los medios de comunicación forman parte de la vida diaria y son una base de la libertad de expresión y de información, ya que por medio de estas la sociedad comprende los problemas que pasan en su comunidad y en el mundo, de igual manera permiten obtener una visión crítica de las situaciones y tomar decisiones que se encuentren fundamentadas.

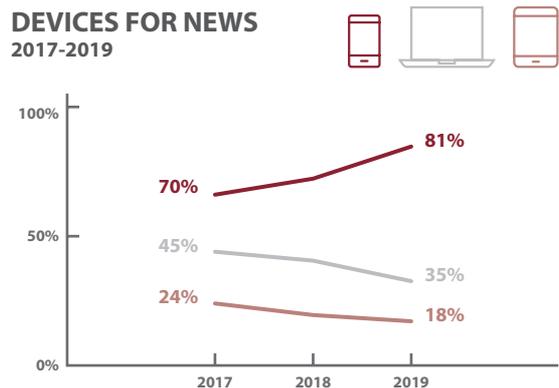
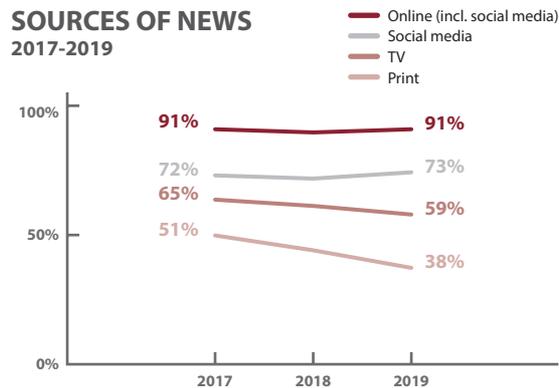
De acuerdo con las situaciones que se ven actualmente en el día a día, es necesario respetar el derecho que tienen las personas de compartir la información que desean para que se tenga un acceso equitativo a la información y conocimiento, sin importar que se traten de sistemas de información libres, independientes y pluralistas.

Las redes sociales forman un mundo dentro del cual es imposible controlar todo lo que pasa o se crea en ellos, debido a que si se llegase a establecer una ley

para evitar la difusión de Fake News se estaría violando por completo la libertad de expresión y derechos humanos, violando las garantías individuales y dando paso al espionaje digital autorizado.

Las propias plataformas han intentado establecer reglas para evitar problemas como los anteriormente ejemplificados, como la creación de cláusulas y filtros en las redes sociales para difundir una noticia, no obstante ninguna de estas cláusulas se cumple realmente para poder ofrecer a los usuarios un lugar seguro, pero si ni las plataformas ni los gobiernos pueden tomar acciones contra el problema ¿cómo se supone que la situación va a mejorar? ¿quién se va a encargar de regular la información y desmentir noticias antes de que tengan consecuencias fatales?

De acuerdo con investigaciones de la Agencia de Noticias Reuters, México confía más en las noticias proporcionadas por medios en línea, con 91 %, y en las redes sociales, con 73%. Así como también tiene preferencias por leer las noticias en un teléfono móvil, con 81%, seguido del uso de las computadoras, con 35% (Imagen siguiente).



Sin ofender o violar los derechos de libertad de cada ser humano, todos los medios de comunicación que han surgido en el último siglo deberían colocar dentro del reglamento cancelar contenido que pongan en riesgo físico o económico a las personas, intimidación por medio de discursos de odio, o ganancia de dinero por medio de engaños, tal y como actualizó sus políticas de seguridad la red social Facebook, que desde el cambio han removido 652 páginas que las violaban.

La regulación de las redes sociales es importante para detener la difusión de noticias que pongan en riesgo la seguridad de los individuos, si bien en ciertas formas afecta el derecho a la libertad de expresión es necesario tener requerimientos para publicar información delicada y de esa manera evitar la desestabilización de la población.

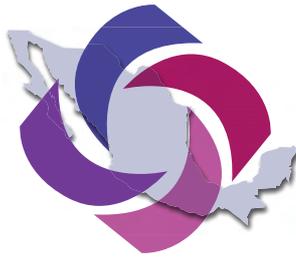
IV. Referencias

- Ávila, E. (2019). Fake News: Falso desabasto de gasolina deja un muerto en Guanajuato. Noticias Énfasis. 03/11/2019. Recuperado de: <https://noticiasenfasis.com.mx/fake-news-falso-desabasto-de-gasolina-deja-un-muerto-en-guanajuato>
- Bateson, G. y Ruesch, J. (1986) Comunicación: La matriz social de la psiquiatría. (Versión PDF). Doi: 10.2307/40183202
- El Sol de León. (2019). Causa pánico falsa información de desabasto de gasolina en León. El Sol de León, Local. 03/11/2019. Recuperado de: <https://www.elsoldeleon.com.mx/local/video-causa-panico-falsa-informacion-de-desabasto-de-gasolina-en-leon-4358034.html>
- Gobierno del Estado de Jalisco. Instituto de Transparencia e Información Pública de Jalisco (ITEI). Jalisco. 03/11/2019. Recuperado de: <https://www.jalisco.gob.mx/en/gobierno/organismos/7811>
- Gómez, F. (2019). Falso desabasto de gasolina causa escenas de pánico y deja un muerto en Guanajuato. Heraldo de México. 05/11/2019. Recuperado de: <https://heraldodemexico.com.mx/estados/guanajuato-desabasto-gasolina-un-muerto-largas-filas-compras-de-panico-caos/>
- Gómez, P. (2019). A un año, permanece impune el doble linchamiento en Acatlán. (En línea). El Sol de Puebla. 03/11/2019. Recuperado de: <https://www.elsoldepuebla.com.mx/local/estado/a-un-ano-permanece-impune-el-doble-linchamiento-en-acatlan-4106090.html>
- Hernández, D. (2018). En Acatlán, linchamiento difundido en tiempo real. Proceso. 03/11/2019. Recuperado de: <https://www.proceso.com.mx/551515/en-acatlan-linchamiento-difundido-en-tiempo-real>
- Hernández, M. (2017). Cuidado con las noticias falsas ante el sismo, no las difundas. Forbes México. 03/11/2019. Recuperado de: <https://www.forbes.com.mx/cuidado-con-las-noticias-falsas-ante-el-sismo-no-las-difundas/>
- Pérez, H. (2008). Comunicación y sociedad: Hacia una semiótica de la comunicación. 05/11/2019. (Versión PDF). Nueva época, núm. 9, pp. 35-57
- Notimex. (2018). Fiscalía de Puebla investiga caso de Acatlán de Osorio; señalan omisión de protocolo. 24 horas. 03/11/2019. Recuperado de: <https://www.24-horas.mx/2018/08/29/fiscalia-de-puebla-investiga-caso-de-acatlan-de-osorio-senalan-omision-de-protocolo/>
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (3-11-2019). Alfabetización mediática e informacional. UNESCO, Comunicación e Información. 03/11/2019. Recuperado de: <http://www.unesco.org/new/es/communication-and-information/media-development/media-literacy/mil-as-composite-concept/>
- Reuters Institute. Reuters Institute Digital News Report 2019. 05/11/2019. (Versión PDF). Universidad de Oxford.
- Ruiz, J. (2019). Desabasto de gasolina en Guanajuato es falso: Sinhue. Milenio. 03/11/2019. Recuperado de: <https://www.milenio.com/politica/comunidad/desabasto-de-gasolina-en-guanajuato-es-falso-sinhue>
- Vázquez, R. (2018). Regulación de las redes sociales y libre expresión. Forbes México. 03/11/2019. Recuperado de: <https://www.forbes.com.mx/regulacion-de-las-redes-sociales-y-libre-expresion/>
- Weidenslauffer, C. (2019). La regulación de las “fake news” en el derecho comparado. (Versión PDF). Biblioteca del Congreso Nacional de Chile, Asesoría Técnica Parlamentaria.
- Yuste, B. (2019). Las nuevas formas de consumir información de los jóvenes. Injuve. 05/11/2019. (Versión PDF). Revista 108-14, nuevas formas de consumir información.



Ylnerid Yleannis Morales Colmenares

Nacida en Valencia, Venezuela. Es estudiante de Comunicación y medios digitales por la UVM, con una gran pasión e interés por el diseño web y la publicidad.



**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



El derecho a la información pública, pieza fundamental en el combate a la corrupción

Alejandro Argenis Reynoso Tabares

Estudiante de la licenciatura en Estudios Políticos y

Gobierno de la Universidad de Guadalajara

Resumen

PALABRAS CLAVES:

Corrupción, Sociedad Democrática, Transparencia, Órganos Garantes de Transparencia

Este trabajo aborda la importancia del derecho a la información pública en el combate a la corrupción, así como la relevancia de tal derecho para una sociedad que se dice ser democrática. Además, habla del involucramiento de los ciudadanos y las asociaciones civiles en la difusión de este derecho, la relación del mismo con la transparencia, y el valor que tienen los órganos que garantizan el derecho a la información pública en el combate a la corrupción.

La corrupción es, indudablemente, uno de los problemas más graves que aqueja a la nación mexicana. De hecho, según el índice de percepción de corrupción, realizado por Transparencia Internacional en el año 2018, México ocupa el lugar 138 de 180 países.¹ Lo anterior no sólo demuestra la magnitud del problema, sino que obliga a la búsqueda inmediata de mecanismos que puedan ayudar en el combate contra la corrupción. Estrategias con tal propósito hay muchas, por ejemplo: la rendición de cuentas, el derecho a la información, la cooperación interinstitucional, entre otros. Sin embargo, el derecho a la información es una pieza clave si lo que se busca es dar el primer paso para combatir la corrupción. Por lo que en este trabajo se buscará defender la afirmación planteada anteriormente.

¹ Forbes Staff. (2019). México cae aún más en el ranking de corrupción y llega al lugar 138 de 180. Ciudad de México, México. Forbes México. Recuperado de: <https://www.forbes.com.mx/mexico-cae-aun-mas-en-ranking-de-corrupcion-y-llega-al-lugar-138-de-180/>

En primer lugar, se debe definir la corrupción.

El concepto de la corrupción, como muchos otros de la ciencia política, no es único, y, debido a esto, es importante aclarar el concepto a utilizar durante este trabajo. Una de las definiciones más conocidas en la ciencia política, y la que será utilizada aquí, es la dada por el politólogo Samuel Huntington, el cual conceptualiza a la corrupción como: “el comportamiento de los funcionarios públicos que se desvían de las normas establecidas para obtener un fin privado”.² En México existen una infinidad de casos recientes de corrupción que empatan perfectamente con la definición previamente dada. Por ejemplo: El caso de la ex secretaria de estado Rosario Robles, la cual, presuntamente, participó en el caso de corrupción conocido como “la estafa maestra”, en el que el gobierno mexicano habría desviado millones de dólares entregados a universidades para que éstas, a su vez, entregaran este dinero a empresas fantasmas para que simularan los servicios contratados.³ Dado tal concepto sobre corrupción y una ejemplificación del mismo, es posible continuar con el siguiente punto.

En segundo lugar, se debe establecer la importancia que tiene el derecho a la información pública en el combate a la corrupción.

Según José Sosa: “en la medida en que existen medios para conocer los desajustes de la acción gubernamental, se hace más tangible la idea de un mejor gobierno, de una democracia más efectiva y de unos derechos individuales más vigentes”.⁴ Debido a lo anterior, el derecho a la información pública, entendido como el derecho que tienen las personas de solicitar información a las dependencias gubernamentales, parece ser fundamental para aspirar a tener un mejor gobierno, entonces, ¿qué tan importante es este derecho en relación con el combate a la corrupción? La respuesta, claro está, es que tal derecho es de suma importancia, pues no sólo permite a los ciudadanos el cuestionar a las autoridades, sino que,

también, hace que las autoridades tengan la obligación dar dicha información.

En tercer lugar, se debe determinar la relación existente entre el derecho a la información pública y la transparencia.

Para Jonathan Fox: “la transparencia se refiere a la existencia o no de información -y de sistemas que la producen- sobre lo que son, hacen, utilizan y producen las dependencias del gobierno o, incluso, sobre actos o productos de actores privados”. Esta definición de transparencia y el derecho a la información pública tienen una similitud tremenda, pues ambas abordan la cuestión de la información de las dependencias gubernamentales. Pero, mientras que la transparencia parece hacer alusión al llenado de un baúl con información sobre tales dependencias, el derecho a la información pública parece ser quien nos otorga la llave para abrir dicho baúl.

En cuarto lugar, es de suma importancia aclarar que, según José Sosa, existen dos tipos de transparencia.

El primer tipo es la “transparencia opaca”. Este tipo ocurre cuando la información que otorgan las dependencias no encaja con la realidad. En otras palabras, la información dada por las dependencias sólo sirve, como se dice coloquialmente, para “taparle el ojo al macho”. El segundo tipo es la “transparencia clara”. Este tipo hace alusión a que, no sólo la información dada es confiable, sino que se sabe el destino final de los fondos públicos. Ya dados los dos tipos de transparencia, es claro que la transparencia deseada por México debería de ser la “clara”, pues los mexicanos ya estamos hartos de simulaciones.

Antes de continuar con el siguiente punto, se debe aclarar que la transparencia es una obligación gubernamental y no debe glorificarse a ningún político que la utilice como un medio para ganar simpatizantes. Esto no quiere decir que los políticos no deban buscar ser lo más transparente posible, sino que nosotros, los ciudadanos, no veamos en esto algo que merezca ser aplaudido, pues a ellos les corresponde ser así.

² Huntington, S. (1973). *Political Order in Changing Societies*. Estados Unidos de América: The Colonial Press Inc., Clinton, Mass.

³ Arturo Angel. (2019). Encarcelar a Rosario Robles no es hacer justicia. Ciudad de México, México. *The New York Times*. Recuperado de: <https://www.nytimes.com/es/2019/08/18/espanol/opinion/rosario-robles-prision-amlo.html>

⁴ Sosa, J. (2011). *Transparencia y rendición de cuentas: Un ensayo introductorio*. México: Siglo XXI.

El quinto punto a tratar es la relevancia del derecho a la información pública para la democracia.

La democracia no puede existir sin transparencia. Esto debido a que en una democracia se tiene el supuesto de que los funcionarios públicos gobiernan para los ciudadanos y no para sus intereses personales. Obviamente, el derecho a la información pública sólo existe y es importante en un gobierno democrático. Por ejemplo: en un gobierno totalitario o autoritario este derecho, tan fundamental para una democracia, es inexistente. Además, en una democracia, vista desde una perspectiva “liberal”, las instituciones (Procuraduría General de la República, Congreso, etc.) son parte vital de ésta, y si no existe el derecho a la información no existe transparencia, lo que genera desconfianza en las instituciones y, en consecuencia, daña la credibilidad pública. Por lo tanto, ningún gobierno en el mundo puede ser llamado democrático si durante tal no existe el derecho a la información pública.

En sexto lugar, los ciudadanos no sólo debemos aspirar a tener el derecho a la información pública, sino que debemos ejercerlo.

Es difícil pensar que, en un país como México, con tantos problemas socio-económicos, entre muchos otros, los ciudadanos busquen ejercer este derecho tan esencial, pues es entendible que existen un sinnúmero de prioridades para estos. A pesar de ello, los ciudadanos debemos entender que entre más nos involucremos en los asuntos públicos, y, por consecuencia, ejerzamos el derecho a la información pública, podremos aspirar a tener mejores funcionarios públicos. Además, una ciudadanía activa y participativa podría ser un remedio para atacar el problema de la corrupción. Evidentemente, para poder ejercer este derecho, los ciudadanos debemos conocerlo y sería muy increíble de nuestra parte el pensar que el gobierno haría difusión del mismo. En consecuencia, las personas que conocemos este derecho y su enorme importancia, asociaciones civiles con fines de transparencia, entre otros, deberíamos organizar campañas de difusión de tal derecho en nuestras colonias o vecindarios y, de igual manera, utilizar esos grandes medios de difusión gratuitos que tenemos en la actualidad, conocidos como redes sociales (Facebook, Twitter, WhatsApp, etc.).

En séptimo lugar, abordaré la importancia que tienen los órganos que garantizan el derecho a la información pública en el combate a la corrupción.

Antes de comenzar es importante saber cuáles son los órganos que garantizan tal derecho en México. Según el INFODF (Instituto de Transparencia, Acceso a La Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México) “la Constitución Política reconoce la existencia de 33 órganos de transparencia especializados, imparciales y autónomos que garantizan el derecho de acceso a la información, integrados en 31 órganos estatales, el INFODF y el INAI”⁵. Tales órganos son fundamentales, pues su tarea es vigilar a las organizaciones públicas y privadas que reciben dinero público, e intervenir cuando una persona solicite información a tales organizaciones y éstas no cumplan con su deber de informar. Es decir, se encargan de que los ciudadanos podamos saber en dónde termina el dinero de nuestros impuestos. Además, su no dependencia de ninguno de los tres poderes del estado (Ejecutivo, Legislativo y Judicial) ayuda a garantizar la imparcialidad de estos órganos garantes de transparencia.

Para finalizar, durante este trabajo se ha establecido la trascendencia del derecho a la información pública en el combate a la corrupción y en la existencia de la democracia. Además, se ha mencionado la influencia de los órganos garantes de la transparencia en el cumplimiento y respeto de este derecho, como la importancia de su difusión por parte de ciudadanos y asociaciones civiles. Por lo tanto, el derecho a la información pública es, sin duda alguna, una pieza clave en el rompecabezas de cualquier sociedad democrática.



⁵ INFODF. S.F. Órganos garantes. Ciudad de México, México. INFODF. Recuperado de: <http://www.infodf.org.mx/index.php/transparencia-en-m%C3%A9xico/%C3%B3rganos-garantes.html>

Referencias bibliográficas

Huntington, S. (1973). Political Order in Changing Societies. Estados Unidos de América: The Colonial Press Inc., Clinton, Mass.

Sosa, J. (2011). Transparencia y rendición de cuentas: Un ensayo introductorio. México: Siglo XXI.

Referencias Web:

Forbes Staff. (2019). México cae aún más en el ranking de corrupción y llega al lugar 138 de 180. Ciudad de México, México. Forbes México. Recuperado de: <https://www.forbes.com.mx/mexico-cae-aun-mas-en-ranking-de-corrupcion-y-llega-al-lugar-138-de-180/>

Arturo Angel. (2019). Encarcelar a Rosario Robles no es hacer justicia. Ciudad de México, México. The New York Times. Recuperado de: <https://www.nytimes.com/es/2019/08/18/espanol/opinion/rosario-robles-prision-amlo.html>

INFODF. S.F. Órganos garantes. Ciudad de México, México. INFODF. Recuperado de: <http://www.infodf.org.mx/index.php/transparencia-en-m%C3%A9xico/%C3%B3rganos-garantes.html>



Alejandro Argenis Reynoso Tabares

Estudiante de la licenciatura en Estudios Políticos y Gobierno de la Universidad de Guadalajara, formo parte del Observatorio Electoral de la UdeG como asistente de investigación y beneficiario del PEES (Programa de Estímulos a Estudiantes Sobresalientes).





Regulación de la transferencia internacional de datos personales en Latinoamérica. Especial mención al marco regulatorio de Argentina y México

Christian Alejandro Razza Sandoval

Abogado de los Tribunales y Juzgados de la República por la Universidad de las Américas sede Quito, Ecuador

Resumen

PALABRAS CLAVES:
Dato Personal, Protección de Datos Personales, Transferencia Internacional de Datos Personales, Redes Sociales, Estándar de Protección

Los datos personales se han vuelto a nivel internacional un activo intangible que permite la productividad y competitividad. Razón por la cual se ha visto necesario regular adecuadamente su tratamiento por una serie de mecanismos, derechos y principios que garanticen el derecho a la protección de datos personales. En la actualidad este derecho se lo concibe como un derecho autónomo, complejo e instrumental. En Latinoamérica se ha marcado la tendencia de reconocer este derecho constitucionalmente, sin embargo, hasta ahora no se ha brindado las garantías suficientes para efectivizar su protección, especialmente en la transferencia internacional de datos personales (TIDP).

Introducción

La época actual se caracteriza por una actividad social, cultural, económica, jurídica y política que constantemente rebasa fronteras. Los avances tecnológicos se han fundido con nuestro diario vivir y prácticamente todas las áreas de nuestra sociedad se ven afectadas por la tecnología. El avance tecnológico ha permitido que el tráfico de información se realice rápidamente y en grandes cantidades, lo cual, en ocasiones, se constituye como una herramienta para facilitar el desarrollo de las sociedades, y otras veces, un riesgo para los derechos de las personas (Rebollo y Serrano, 2017, pp. 21-23).

Históricamente algunas legislaciones han mostrado una preocupación mayor por la protección de datos personales, como es el caso de la Unión Europea (UE) que, en el 2016, con el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) estableció un conjunto de mecanismos para regular el tratamiento de datos personales (TOP) y la TIDP. Siguiendo esta línea, con el presente trabajo se pretende mostrar que en Latinoamérica no existe una adecuada regulación respecto a la TIDP, por lo cual si los datos personales de una persona son objeto de una de estas transferencias se encontrarían en un total estado de desprotección.

1. Estándares de protección para la transferencia internacional de datos personales

Por las disparidades existentes entre las legislaciones nacionales sobre protección de datos la TIDP puede poner en riesgo los derechos de las personas. Sin embargo, como señala Castellanos (2017, p. 6) sin la TIDP difícilmente se podría dar el comercio mundial. Así pues, para evitar los posibles perjuicios que a la privacidad de las personas podría causar una TIDP y poder garantizar la libre circulación de datos personales, los Estados, así como las Uniones geopolíticas (UE) han establecido estándares de protección o convenios para regular la TIDP.

En Estados Unidos el derecho a la protección de datos personales tiene como antecedente principal, el derecho a la privacidad o Right to Privacy. Esta doctrina

construida por Louis Brandeis y Samuel Warren en 1890 aportó con una reinterpretación de los precedentes en la materia ya que comenzó a proteger a la privacidad fuera del derecho a la propiedad. No obstante, el sistema de protección de datos norteamericano “no reconoce la protección de la privacidad mediante una legislación específica, sino que ello se efectúa a través de normativas sectoriales que, mediante la complementación de reglamentaciones y códigos de adhesión, propician un marco regulador singular” (Castellanos, 2017, p. 14).

En Estados Unidos en el siglo XX se dictaron tres leyes que establecen los principios rectores que configuran el derecho a la privacidad en este país: la Freedom of Information Act (FOIA) de 1966, la Privacy Act de 1974 y la Right to Financial Privacy Act (RFPA) de 1978. En el siglo XXI aparecieron el Safe Harbor de 2000 y posteriormente el Privacy Shield de 2016 para regular la TIDP con Europa, la California Consumer Privacy Act (CCPA) de 2018 que entrará en vigor en 2020.

Del Safe Harbour al Privacy Shield

Tanto el Safe Harbour como el Privacy Shield se concibieron como mecanismos para solucionar la ausencia de regulación en Estados Unidos sobre el TOP y permitir la TIDP con la UE. Estos marcos regulatorios son su estándar de protección para realizar la TIDP con la UE. No obstante, el Safe Harbour que fue el marco regulatorio que más tiempo estuvo vigente, aunque fue acogido por miles de empresas americanas, no era de carácter obligatorio, no estaba en igual rango que otras leyes americanas y se encontraba desactualizado, lo cual dificultaba su aplicación y, por ende, tuvo que ser sustituido. El Privacy Shield si bien entró a cubrir los vacíos de su antecesor sigue cayendo en los mismos problemas, no es un marco regulatorio obligatorio y no implica que Estados Unidos sea un país con un nivel adecuado de protección de datos personales.

La regulación sobre protección de datos personales en la UE ha venido desarrollándose a lo largo del tiempo con gran interés debido a que, por la evolución de las tecnologías de la información y comunicación (TICs) se ha podido realizar un intercambio inmediato de informa-

ción sin límites físicos. En la UE desde el Convenio 108 de 1981 se ha emitido varias normas comunitarias que regulan la protección de datos personales, requiriendo una “protección equivalente” entre los países partes, y buscando una cooperación internacional a través de las autoridades locales de cada país.

Una de las normativas más importantes fue la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al TDP y a la libre circulación de estos datos. Los Estados miembros de la UE, a efectos de cumplir con las obligaciones que imponía esta Directiva, fueron elevando progresivamente el nivel de protección de los datos personales, produciéndose “un efecto homogeneizador de los medios de protección y de los mecanismos para la eficacia de los derechos” (Rebollo, 2008, p. 105). Como resultado de este proceso, con la expedición del GDPR la normativa de la UE en el campo de la protección de los datos se ha constituido como la más exigente del planeta (Guasch, 2012, p. 22).

Reglamento General de Protección de Datos

En Europa el 27 de abril de 2016 se adoptó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, con el que se derogó la Directiva 95/46/CE a fin de reformar la normativa ya existente sobre protección de datos personales y adaptarla al nuevo contexto mundial que después del caso de Cambridge Analytica cambió notablemente. Con el GDPR la UE estableció todo un sistema de protección de datos personales, que modificó reglas ya existentes, desarrolló aquellas que eran muy básicas y creó otras que eran necesarias. Esta novedad se orienta a una transición hacia una economía centralizada en los datos y la creación de un mercado único digital (Moritz y Gibello, 2017, p. 116).

Respecto a la TIDP con el GDPR en la UE se estableció un conjunto de mecanismos para transferir datos a terceros países: decisiones de adecuación, normas contractuales estándar, normas corporativas vinculantes, mecanismos de certificación y códigos de conducta. En la UE con el GDPR para realizar una TIDP se requiere un nivel adecuado de protección. Razón por la que Estados

Unidos debió implementar el Privacy Shield, y Latinoamérica se encuentra en proceso de adopción y aplicación de estándares internacionales para la protección de datos personales.

En el GDPR existen 3 niveles de protección a efectos de autorizar una TIDP a un tercer país u organización internacional. La regla general es cumplir con un nivel adecuado de protección, que es el nivel más riguroso, después viene el nivel de ofrecer garantías adecuadas; y el establecimiento de normas corporativas vinculantes o certificaciones. Además, existen casos excepcionales para realizar una TIDP.

2. Regulación de la protección de datos personales en América Latina

En América Latina la regulación del derecho a la protección de datos personales sigue un ritmo propio y tiene ciertas características que ameritan analizarse. Recientemente en las constituciones latinoamericanas se incorporó como derecho autónomo a la protección de datos personales frente a la necesidad de dar respuesta al proceso de evolución tecnológica (Ordóñez, 2017, p. 85).

República de Argentina

En el Art. 43 de la Constitución de la República de Argentina se encuentra consagrado el derecho a la protección de datos personales. En este artículo se deriva la obligación de los organismos públicos de garantizar el acceso a la información, confidencialidad, supresión y rectificación de los datos personales. Pero, es en la Ley 25.336 promulgada el 4 de octubre del año 2000 donde se encuentra reglamentada la protección de datos personales. En el Art. 2 de la mencionada Ley se regula la protección de datos personales sin hacer una distinción entre el ámbito público y privado.

En el capítulo 2 de la Ley 25.326 se establece los principios generales en materia de protección de datos personales y TOP. Destacándose, el principio de licitud para la formación de archivos de datos. El principio de calidad de datos que se traduce en que la recolección

de datos no puede hacerse por medios desleales y que dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular.

En Argentina conforme el Art. 29 el órgano de control que gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del ministerio de justicia y Derechos Humanos de la Nación es la Agencia de Acceso a la Información Pública, la cual es la encargada de supervisar que se cumplan las disposiciones contenidas en la Ley 25.326. Respecto a la TIDP se sigue el modelo europeo toda vez que en el Art. 12 se exige para autorizar una TIDP que el Estado receptor de los datos cuente con un nivel adecuado de protección.

Estados Unidos Mexicanos

El caso mexicano es particular, recién con las reformas constitucionales del año 2007 y 2009 es que se protege constitucionalmente a los datos personales, se consagra explícitamente el derecho a la protección de los datos personales y se establecen los derechos ARCO como núcleo fundamental de dicho derecho (Cunha, 2011, p.323). Posteriormente, en el año 2010 se adopta la Ley Federal de Protección de Datos en Posesión de Particulares, teniendo un ámbito de aplicación únicamente privado. Dada la redacción de esta Ley es evidente que se basa en el marco normativo europeo apuntando hacia la tendencia mundial de regulación jurídica de los datos personales para garantizar el derecho a la vida privada de los individuos, con respecto al TOP.

En la mencionada Ley se establece una serie de principios para la protección de datos personales, como son: el de información, licitud, consentimiento, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En el capítulo VI establece las competencias de la Autoridad reguladora, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). En capítulo V se desarrolla la TIDP, pero, no se exige un nivel adecuado de protección, tan solo exige consentimiento del titular de los datos y enumera ciertos supuestos que no requieren consentimiento, además no desarrolla las transferencias ulteriores.

El 26 de enero de 2017, se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados con el fin de regular el ámbito público del TDP. Son sujetos obligados conforme el Art. 1 en el ámbito federal, estatal y municipal: “cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.”. Los particulares, sean personas naturales o jurídicas, no le son aplicables esta Ley sino la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En el capítulo 1 del Título segundo de la Ley aplicable a sujetos obligados, en relación con la Ley aplicable a privados se aumenta y se desarrolla un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales, como son los: principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad demostrada en el TOP. De la autoridad de protección de datos personales señala que sigue siendo el INAI. En lo que se refiere a la TIDP en el Art. 68 de la Ley aplicable a los sujetos obligados se señala que:

“El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obliguen a proteger los datos personales conforme a los principios y deberes que establece la presente Ley.”

De esta norma se evidencia que para autorizar una TIDP se exige el cumplimiento de garantías adecuadas, además de necesitar el responsable del TDP el consentimiento del titular de los datos y deberá comunicar al receptor de los datos personales las finalidades conforme a las cuales se tratan los datos personales frente al titular. No obstante, no se requiere un nivel adecuado de protección como en la UE con el GDPR.

Comparación entre las regulaciones

Del estudio realizado se evidenció que el derecho a la protección de datos personales se tutela de una manera diferente a nivel mundial, aunque con una tendencia a dirigirse al modelo europeo. Además, debido a los riesgos de la TIDP, se ha marcado una predisposición de los Estados y las organizaciones internacionales de exigir un nivel adecuado de protección de datos personales para autorizar una TIDP. Así pues, a partir del análisis realizado sobre la regulación de la protección de datos personales, corresponde efectuar una comparación centrada en los temas que son objeto de este trabajo.

Tabla 1. Comparación con respecto a la protección de datos personales

	Latinoamérica		Europa		OCDE
	Argentina	México	GDPR	EE.UU.	
Norma constitucional sobre la protección de datos	•	•	NA	X	NA
Legislación general sobre protección de datos personales	•	•	•	X	•
Normativa sectorial en cuanto al TDP	•	•	NA	•	NA
TDP especial para datos personales sensibles	•	•	•	X	•
Autoridad autónoma competente	•	•	•	X	•
Recursos administrativos y acciones judiciales	•	•	•	•	•
Obligaciones a los responsables y encargados de los TDP	•	•	•	X	•
Principios para el TDP y la TIDP	•	•	•	X	•
Derechos ARCO	•	•	•	X	•
Sanciones	•	•	•	•	•
Regulación sobre la TIDP	•	•	•	•	•

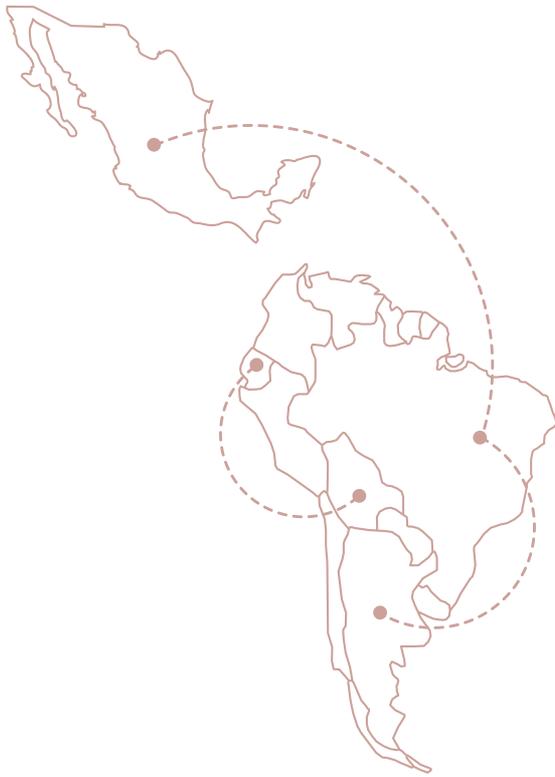
Nota: NA - no aplica

Tabla 2. Comparación general respecto a la TIDP

	Argentina	México	GDPR	Privacy Shield	OCDE
Definición sobre la TIDP	X	X	X	X	X
Desarrollo de las TIDP ulteriores	X	X	•	•	•
Exigencia de un nivel adecuado para la TIDP	•	X	•	•	•
Garantías adecuadas para la TIDP	X	•	•	X	•
Normas corporativas vinculantes para la TIDP	X	•	•	•	•
Casos excepcionales para la TIDP	•	•	•	•	•

Nota: Comparación de los niveles de protección para realizar una TIDP.

Como se puede notar Estados Unidos con el Privacy Shield, Latinoamérica y los organismos internacionales se alinean al estándar de protección de datos personales que establece la UE con el GDPR. Se resalta la necesidad de contar con autoridades de control autónomas como la AEPD en España o la CNIL en Francia para un correcto desarrollo de la protección de datos. En cuanto a la TIDP de igual manera se sigue la tendencia europea de establecer niveles de protección adecuados que permitan proteger a los titulares de los datos.



Conclusiones

Desde la incorporación y posterior desarrollo de las nuevas tecnologías, Latinoamérica ha pasado por una revolución en el manejo de la información. La combinación de estas herramientas tecnológicas con el fenómeno de la globalización trajo consigo múltiples ventajas, como: el desarrollo del comercio electrónico, la implementación de un gobierno en línea, y la virtualización de las relaciones de los ciudadanos, proveedores, consumidores y autoridades. Todas estas actividades requieren de la TIDP, por ello la necesidad de buscar armonizar las legislaciones en cuanto a la protección de datos personales.

En Latinoamérica, si bien son varios los países que regulan la protección de datos personales para proteger los derechos de sus ciudadanos, y desarrollar el comercio internacional y electrónico, aun existen ciertas falencias en la regulación. Por ejemplo, contar con una autoridad de control independiente, regular adecuadamente la TIDP, poder sancionar a los infractores con multas que puedan causar un grado de responsabilidad y actualizar las legislaciones sobre protección de datos. Falta todavía mucho para lograr la protección que brinda el GDPR, pero un paso importante es comenzar a tener una cultura de protección de nuestros datos personales.

Referencias bibliográficas

- Castellanos, A. (2017). El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield. /CPS Working Papers, 350. Recuperado el 15 de octubre de 2019 de <https://www.icps.cat/archivos/Workingpapers/wp350.pdf?noga=1>
- Cunha, T. D. (2011). Las recientes reformas en materia de protección de datos personales en México. Anuario Jurídico y Económico Escurialense. Recuperado el 29 de octubre de 2019 de <https://webcache.googleusercontent.com/search?q=cache:QvIznE2P Z80J:https://dialnet.unirioja.es/descarga/articulo/3625376.pdf+&cd=1&hl=es&ct=clink&l=ec>
- Eur-Lex. (s.f.). Decisión de ejecución, Privacy Shield UE-EE. UU 201611250de Ja Comisión Europea de 12 de julio de 2016. Recuperado el 2 de septiembre de 2019 de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:3201601250&qid=1542660556803&from=EN>
- Eur-Lex. (s.f.). Decisión de Ja Comisión 20001520/CE, Safe Harbor Privacy Principies de la Comisión Europea de 26 de julio de 2000. Recuperado el 2 de octubre de 2019 de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=en>
- Eur-Lex. (s.f.). Reglamento General de Protección de datos del Parlamento Europeo y del Consejo UE 20161679(GDPR) de 2016. Recuperado el 15 de octubre de 2019 de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>
- Gibello, V. y Moritz, M. (2017). El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro. Foro, 27. Recuperado el 25 de octubre de 2019 de <http://repositorio.uasb.edu.ec/bitstream/10644/5948/1/08-TC-Moritz-Gibello.pdf>
- Guasch Portas, V. (2012). La transferencia internacional de datos de carácter personal. RDUNED, 11. Recuperado el 20 de octubre de 2019 de <http://revistas.uned.es/index.php/RDUNED/article/view/11139/10667>
- Honorable Cámara de Diputados. (s.f.). Ley Federal de Protección de Datos Personales en Posesión de /os Particulares de México de 2010. Recuperado el 30 de septiembre de 2019 de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- Honorable Cámara de Diputados. (s.f.). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México de 2017. Recuperado el 14 de septiembre de 2019 de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPSO.pdf>
- Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. Foro, 27. Recuperado el 14 de octubre de 2019 de <http://repositorio.uasb.edu.ec/bitstream/10644/5947/1/07-TC-Ordo%C3%B1ez.pdf>
- Organización de Estados Americanos. (s.f.). Ley de Protección de Datos Personales de Argentina, Nro. 25.326 de 2000. Recuperado el 25 de septiembre de 2019 de https://www.oas.org/juridico/PDFs/arg_ley25326.pdf
- Rebollo, L. (2008). Vida privada y protección de datos en la Unión Europea. Madrid: Dykinson.
- Rebollo, L. y Serrano, M. M. (2017). Manual de Protección de Datos (2a. ed.). Madrid: Dykinson.
- Zaballos, E. (2013). La Protección de Datos Personales en España: Evolución Normativa y Criterios de Aplicación (Tesis Doctoral). Recuperado el 18 de octubre de 2019 de <https://eprints.ucm.es/22849/1/T34733.pdf>



Christian Alejandro Razza Sandoval

Abogado de los Tribunales y Juzgados de la República por la Universidad de las Américas sede Quito, Ecuador. Experiencia laboral en el ámbito público como privado en temas laborales, societarios y de niñez y familia. Actualmente es asesor legal del Hospital Vozandes en el área de propiedad intelectual y Abogado Jr. En Fabara & Compañía Abogados en el área laboral y de telecomunicaciones. Ha participado en varios proyectos de vinculación con la comunidad, como combatir la violencia intrafamiliar, también participo en la creación de una ley de protección de datos personales para el Ecuador.



La transversalidad progresiva de la rectificación y oposición de datos personales para el acceso efectivo al derecho a la identidad jurídica de la población transgénero y transexual

Rafael Ríos Nuño

Instituto Autónomo de Occidente/Centro de Derecho Corporativo, Derechos Humanos y Paz

José Benjamín González Mauricio

Comisión Estatal de Derechos Humanos Jalisco

Resumen

En el presente estudio se reflexionará el empoderamiento de la población trans¹ abocando su derecho a la protección de sus datos personales, como es la identidad jurídica a través de la interpretación evolutiva de los derechos humanos suscritos y ratificados por el Estado mexicano ante la comunidad internacional; situación que a la fecha son transgredidos dentro de la legislación doméstica al existir normas restrictivas y omisas en garantizar los derechos básicos e indispensables de esta población.

PALABRAS CLAVES:

Derechos Humanos,
Población Trans,
Privacidad, Protección de
Datos Personales

¹ Asimismo, a la población transgénero y transexual se les considere con el acrónimo general trans que refiere «del otro lado».

Derecho a la identidad jurídica de la población transgénero y transexual

Al referirse de manera específica al concepto de persona física, Kelsen (2003) manifestaba que persona era el «portador» de derechos y obligaciones. De esta manera se interpretará que el derecho al reconocimiento de la personalidad jurídica se refiere a la facultad de ejercer y gozar de sus derechos, la capacidad de asumir obligaciones, y la capacidad de actuar.

Bajo la misma línea argumentativa, la Convención Americana sobre Derechos Humanos (CADH), advierte en su artículo 1.2 que «para los efectos de esta Convención, persona es todo ser humano»; por lo que en este sentido se desprende la vinculación directa que persona es cualquier ser humano, incluida la población transgénero y transexual (población trans) que se desarrolla y se es sujeto a derechos como obligaciones.

Para lograr identificar las características elementales que diferencian a la población trans, la Comisión Nacional de los Derechos Humanos (CNDH), ha advertido textualmente lo siguiente:

Transgénero: Utilizado para describir las diferentes variantes de la identidad de género (incluyendo travestis, transexuales, entre otras), cuyo denominador común es que el sexo asignado al nacer no concuerda con la identidad de género de la persona. Las personas transgénero construyen su identidad de género independientemente de intervenciones quirúrgicas o tratamientos médicos. Cabe resaltar que la identidad de género no la determinan las transformaciones corporales, las intervenciones quirúrgicas o los tratamientos médicos; sin embargo, éstas pueden ser necesarias para la construcción de la identidad de género de algunas personas trans (CNDH, 2017, pp. 9 y 10).

Transexual: Se refiere a las personas que se sienten y se conciben a sí mismas como pertenecientes a un género diferente al

que social y culturalmente se asigna a su sexo biológico y que optan por unas intervenciones médicas hormonales, quirúrgicas o ambas para adecuar su apariencia física biológica a su realidad psíquica, espiritual y social (CNDH, 2017, p. 10).

Sin embargo, dentro de la legislación interna aún no se ha logrado balancear la titularidad de derechos humanos de esta población, orillando al exilio a estas personas con calidad de sujetos indocumentados al no poder coincidir su imagen al estatuto social asignado en los patrones de ser una mujer o el ser un hombre.

Por ello, bajo una perspectiva de derechos humanos a través de sus mecanismos interpretativos que descansan en la Convención de Viena sobre el Derecho de los Tratados (CV), en su numeral 31 (Reglas de la Interpretación) y 32 (medios complementarios de la interpretación); y de acuerdo a la CADH, en sus numerales 26 (Desarrollo progresivo), 29 (Normas de interpretación) y 31 (Reconocimiento de Otros Derechos) en relación con los artículos 1.1, 1.2 (Obligación de Respetar los Derechos) y 2 (Deber de Adoptar Disposiciones de Derecho Interno), que sustraen los efectos holísticos, evolutivos, sistemáticos, teleológicos y hermenéuticos que encarnan la justiciabilidad directa y positiva del reconocimiento de nuevos derechos que emergen acorde a los cambios y exigencias sociales, económicas y culturales que detona una sociedad inclusiva, como en este sentido el reconocimiento y reivindicación del derecho a la identidad de género como atributo de la personalidad jurídica que se encuentra protegida en el artículo 3 (Derecho al Reconocimiento de la Personalidad Jurídica) de referida CADH en favor de las personas trans.

Lo anterior robustecido en el más reciente estándar latinoamericano en favor de los derechos humanos de la población trans que se afianzó en la Corte Interamericana de Derechos Humanos (Corte IDH) a través de la Opinión Consultiva 24 (OC-24/17)². En su decisión, la

² Corte IDH. Identidad de género, e igualdad y no discriminación a parejas del mismo sexo. Obligaciones estatales en relación con el cambio de nombre, la identidad de género, y los derechos derivados de un vínculo entre parejas del mismo sexo (interpretación y alcance de los artículos 1.1, 3, 7, 11.2, 13, 17, 18 y 24, en relación con el artículo 1 de la Convención Americana sobre Derechos Humanos). Opinión consultiva OC-24/17, del 24 de noviembre de 2017. Serie A, núm. 24.

Corte IDH reiteró su jurisprudencia constante en el sentido de que la orientación sexual, y la identidad de género son categorías protegidas por la CADH. Por ello está proscrita cualquier norma, acto o práctica discriminatoria basada en estas características de la persona. Reiterando que la falta de consenso interno en algunos países sobre el respeto pleno por los derechos de ciertos grupos o personas que se distinguen por su orientación sexual, su identidad de género o su expresión de género, reales o percibidas, no puede ser considerado como un argumento válido para negarles o restringirles sus derechos humanos o para perpetuar y reproducir la discriminación histórica y estructural que estos grupos o personas han sufrido.

Ahora bien, en México, diversas entidades de la república mexicana han logrado articular este derecho a las personas trans a través del levantamiento de acta por reasignación para la concordancia sexo-genérica, como la Ciudad de México, así como Michoacán, Nayarit y Sinaloa, en donde se otorga una nueva acta de nacimiento para el reconocimiento de la identidad de género. Asimismo, establecen que, al momento de contar con la nueva acta, la persona no pierde los derechos u obligaciones contraídas con la identidad anterior.

Por lo anterior, y de acuerdo a la plataforma normativa sobre la atención del derecho a la identidad de género de la población trans, robustece la obligatoriedad constitucional y convencional de promover, respetar, proteger y garantizar los derechos humanos por parte de todas las autoridades públicas, de conformidad con el artículo 1° y 133 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), y 4° de la Constitución Política del Estado de Jalisco, que exhibe el estándar mínimo jurídico de atención para esta población, dando como resultado integral la reivindicación de este derecho primordial para tener los efectos catalizadores con los diversos derechos indivisibles e interdependientes que infieren en el entorno vivencial de una persona, como la privacidad y la autodeterminación.

Alcances del derecho a la privacidad, protección de datos personales y autodeterminación informativa

Gregorio (2004, p. 303), de su obra titulada «Protección de Datos Personales: Europa vs Estados Unidos, todo un dilema para América Latina», diferencia de forma sencilla los conceptos de público y privado, definiendo al primero como la necesidad de dejar determinado documento accesible al público con la finalidad del control ciudadano de los actos de gobierno; lo privado, para él es toda decisión personal en la que el Estado no puede intervenir. Por lo cual, la población trans tiene el derecho a que su privacidad sea protegida, respetada y garantizada por el Estado, que sus decisiones personales no salgan al escrutinio público para evitar actos de discriminación o ataques de odio.

Por su parte, Escalante (2004, p. 186), afirma que el límite que se refiere a la privacidad, se justifica debido a la dignidad humana que implica el poder elegir en libertad; dicho de otra manera, se trata de elegir el propio plan de vida.

Por otro lado, Garzón (1998, p. 227), en su estudio «Privacidad y Publicidad», señala que la privacidad es el ámbito donde imperan exclusivamente los deseos y preferencias individuales; es condición necesaria del ejercicio de la libertad individual. Asimismo, dice que lo público está caracterizado por la libre accesibilidad de los comportamientos y decisiones de las personas en sociedad.

México reconoce en el artículo 6° y 16 de la CPEUM, el derecho a la información y como sus límites, el derecho a la privacidad y a la protección de datos personales, al acceso, rectificación, cancelación y oposición de los mismos.

La Suprema Corte de Justicia de la Nación en México (SCJN) y la Corte Interamericana de Derechos Humanos (Corte IDH), han destacado la vinculación de la privacidad con un amplio abanico de otros derechos, como la inviolabilidad de la correspondencia y de las comunicaciones en general, la inviolabilidad del domicilio, las garantías respecto de los registros personales y corporales, las relaciones con la recopilación y registro de

información personal en bancos de datos y otros dispositivos; el derecho a una vivienda adecuada, a la salud, y a la igualdad; los derechos reproductivos, o la protección en caso de desalojos forzados.

Además, las citadas Cortes sostienen que las personas tienen derecho a gozar de un ámbito de protección de su existencia que quede reservado de la invasión y la mirada de los demás, que les concierna sólo a ellos y les provea de condiciones adecuadas para el despliegue de su individualidad –para el desarrollo de su autonomía y libertad–. La misma idea puede describirse apelando al derecho de las personas a mantener fuera del conocimiento de los demás ciertas manifestaciones o dimensiones de su existencia que los demás no las invadan sin su consentimiento.

Por lo tanto, la vida privada implica poder conducir parte de la vida de uno, protegido de la mirada y las injerencias de los demás, y guardar conexiones de variado tipo con pretensiones más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos: el derecho de poder tomar libremente ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular.

En otro orden de ideas, Martínez (2007, p. 51) define el derecho a la protección de datos personales como aquel que «garantiza la facultad del individuo de decidir básicamente por sí mismo sobre la difusión y la utilización de sus datos personales».

Aunado a lo anterior, la SCJN sostiene que el derecho a la protección de datos personales está íntimamente ligado con el derecho a la autodeterminación de la información:

« (...) es el derecho a poseer la intimidad a efecto de disponer del control sobre la publicidad de la información tanto de la persona como de su familia; lo que se traduce en el derecho de la autodeterminación de la información que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede utilizar esa información. En este contexto, el derecho a la intimidad impone a los poderes públicos, como a los particulares, diversas obligaciones, a saber: no difundir información de carácter personal entre los que se encuentran los datos personales, confidenciales, el secreto bancario e industrial y en general en no entrometerse en la vida privada de las personas; asimismo, el Estado a través de sus órganos debe adoptar todas las medidas tendentes a hacer efectiva la protección de este derecho»³.

Derivado de lo anterior, es evidente que la población trans tiene el derecho a tomar las decisiones concernientes a su propio plan de vida, a elegir con libertad respecto a la forma como se identifican y ejercer válidamente su derecho a la autodeterminación. Además, tienen la prerrogativa a ejercer su derecho a la rectificación y oposición de sus datos personales, cuando estos han dejado de cumplir las finalidades para los cuales fueron entregados –independientemente que el tratamiento en un principio haya sido lícito–, cuando exista un tratamiento desproporcionado que le cause un perjuicio a la persona –ataques de odio y de discriminación por la falta de homologación de sus documentos con su identidad–, cuando dichos datos ya no están actualizados o no coinciden con la identidad con la cual se identifican. Por lo tanto, las autoridades –particularmente las de los registros civiles–, no pueden dejar de garantizar sus derechos a la rectificación y oposición de sus datos personales, alegando la falta de legislación interna –Ley de Identidad de Géne-

³ Suprema Corte de Justicia de la Nación. Tesis: I.3o.C.695 C. Amparo en revisión 73/2008. 6 de Mayo de 2008. [En línea]. Consultado el 28 de octubre de 2019. Disponible en: <https://bit.ly/2S4Wffz>

ro-, sino que, como lo dijo la Corte IDH en la OC-24/17, la falta de legislación especializada o la falta de consenso interno, no es argumento válido para no respetar, proteger o garantizar los derechos.

En virtud de lo anterior, cuando una persona de la población trans necesite realizar el cambio de nombre, género y sexo ante las autoridades del registro civil, éstas no pueden argumentar la falta de legislación especializada, sino que deberán ir más allá para brindar una protección amplia a la persona, tomando especial atención de que se trata de un grupo históricamente discriminado y en situación de vulnerabilidad.

La autoridad registral, deberá realizar una interpretación progresiva como le obliga los artículos 1° y 133 de la CPEUM, bastará con revisar el derecho de rectificación consagrado en el artículo 16, segundo párrafo y bajo los principios rectores de la protección de datos personales –recogidos en las leyes de protección de datos personales–, es decir, el principio de calidad, finalidad, proporcionalidad y responsabilidad, hacer el levantamiento de una nueva acta de nacimiento. Hecho lo anterior, observando el derecho de oposición de datos personales, reconocido en el mismo numeral 16 antes citado y bajo los mismos principios rectores en la materia, deberá hacer el resguardo integral del acta primigenia para limitar el tratamiento por personas no autorizados, de esa forma se protegerá la privacidad y la dignidad de la persona.

Conclusiones

A lo largo de esta reseña se ha dimensionado la situación actual que rige en México dentro del entorno de la población trans, reflexionando las últimas reformas constitucionales en materia de derechos humanos que vinculan la exigibilidad y justiciabilidad del derecho a la identidad de género a través de los principios rectores e interpretaciones latinoamericanas que establecen la protección amplia del derecho a la identidad, y el debido reconocimiento de los derechos de rectificación y oposición de los datos personales sensibles; lamentando con profunda preocupación el contexto que se enfrentan en nuestro país, deduciendo ser personas indocumentadas que carecen de documentación acorde a su identificación

genérica en su propio país de origen.

Recordando que, en la mayoría de las entidades de la república mexicana, y en particular en Jalisco, el reconocimiento del derecho a la identidad de género de la población trans no está garantizada en su legislación, lo que implica que ante la negativa derivada de dicha circunstancia, cualquier persona que pretenda llevar a cabo un trámite de esa naturaleza debe trasladarse a Ciudad de México o a otro estado que sí la considere, con la expectativa de obtener una nueva acta de nacimiento, sin alterar datos fundamentales como la fecha y lugar de nacimiento y apellidos.

Dicho trámite resulta costoso, sin olvidar que no todas las personas pueden hacerlo; por ello, se ven forzados a ser revictimizados y obligados a no conseguir los documentos oficiales que amparen su nueva identidad, y, por excluidos de ejercer el libre desarrollo de su personalidad. Por lo que, dichos actos se consideran barreras institucionales, culturales, económicas, lingüísticas, legislativas y de género, lo que se podría traducir en graves violaciones a los derechos humanos de un grupo históricamente discriminado y en situación de vulnerabilidad.

El hecho de que las personas trans no tengan una identidad jurídica coherente con su identidad de género es el inicio de una cadena de sucesos que vulneran sus derechos, generando prácticas tan cotidianas que ayudan a reforzar los estereotipos y los patrones de comportamiento, expresión, pensamiento entre hombres y mujeres, llamada transfobia. Por lo que, en cierta parte de la sociedad e instituciones públicas, aún dentro de sus actividades cotidianas, se reproducen estereotipos que impactan de lo que es normal y castigan cualquier desvío de lo ya establecido, como es el basarse estrictamente en los genitales y las características físicas y cualquier situación que salga de lo que se tiene ya normalizado.

Finalmente, la propuesta de este estudio descansa en que, con independencia de que se cuente con una Ley de Identidad de Género, las autoridades de los registros civiles tienen la obligación de acatar los derechos constitucionales de rectificación y oposición de datos personales, así como de los principios y deberes rectores de las leyes en la materia, para realizar el levantamiento de una nueva acta de nacimiento y resguardar la primigenia.

Bibliografía

Cuervo, J. (2014). Autodeterminación informativa. [En línea] Consultado el 10 de enero de 2019 en: http://www.informatica-juridica.com/trabajos/autodeterminacion_informativa.asp#1.4.2.

Comisión Nacional de los Derechos Humanos (2017). Los derechos humanos de las personas transgénero, transexuales y travestis, Primera Visitaduría General, Programa Especial de VIH/Sida y Derechos Humanos.

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

Garzón, V. (1998). Privacidad y publicidad, Revista Doxa, número 21, Cuadernos de filosofía del Derecho, Centro de Estudios políticos y Constitucionales, Alicante, España, pp. 223-244.

Gregorio, C. (2004). Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina. Transparentar al Estado: la experiencia mexicana de acceso a la información. México: Instituto de Investigaciones Jurídicas de la UNAM.

Hans, K. 2003. Teoría pura del derecho, traducción de Roberto J. Vernengo, México. Porrúa.

Troncoso, A. (2010). La protección de datos personales. En busca del equilibrio. España: Tirant lo Blanch.



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.

Participación en diversos foros y ha sido amicus curiae de la Corte Interamericana de Derechos Humanos.



José Benjamín González Mauricio

Abogado por la Universidad de Guadalajara y doble Máster de Derecho Internacional y Derechos Humanos por el Instituto Europeo de Derechos Humanos de Compostela España.

Cuenta con reconocimientos internacionales, ha colaborado en la Comisión Ejecutiva de Atención a Víctimas del Estado de Jalisco, y preside el Grupo Especializado en Diversidad Sexual de la Comisión Estatal de Derechos Humanos Jalisco (CEDHJ) y es consejero suplente del primer Consejo Consultivo para la Protección de Personas Defensoras de Derechos Humanos y Periodistas en Jalisco y ha sido amicus curiae de la Corte Interamericana de Derechos Humanos.

Lineamientos para la publicación de trabajos en el décimo número de la revista Caja de Cristal

La revista “Caja de Cristal” del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI), con el propósito de promover la cultura de la transparencia, el derecho a la información, la rendición de cuentas y el derecho a la protección de datos personales y a la privacidad:

SE CONVOCÓ AL CERTAMEN JUVENIL DE ENSAYO EN MATERIA DE DERECHO A LA INFORMACIÓN Y A LA PROTECCIÓN DE DATOS PERSONALES

BASES

I. Dirigido a:

Podrán participar jóvenes entre los 18 y hasta 30 años de edad cumplidos al día 30 de septiembre del 2019. No podrán concursar personas que presten sus servicios en el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI).

II. Temas:

- El derecho a la información pública.
 - Su importancia en el contexto de un estado democrático.
 - El impacto de los organismos garantes de transparencia en su preservación.
 - Los riesgos de la opacidad en los poderes públicos.
 - Su relación con en el combate a la corrupción.
 - Análisis de casos y experiencias relevantes en el ejercicio de este derecho.

- El derecho a la protección de datos personales.
 - El valor de nuestros datos personales.
 - Los peligros de vivir sin privacidad.
 - Los daños que representa el acceso no autorizado a nuestros datos personales.
 - Los datos personales en la era del Internet y las redes sociales.
 - Análisis de casos y experiencias relevantes en el ejercicio de este derecho.

III. Los ensayos participantes deberán cumplir con los siguientes requisitos:

- Cada interesado tendrá derecho a remitir tantos trabajos como deseen, en los cuales se podrá comentar o reflexionar sobre una o más de las problemáticas planteadas, siempre y cuando estén íntimamente relacionadas en cuanto a la temática de fondo.
- Un mismo ensayo podrá ser escrito hasta por dos autores bajo un mismo pseudónimo.
- Los trabajos deberán ser inéditos y originales, y no estar simultáneamente sometidos a un proceso de dictaminación por parte de otra revista o medio de publicación.
- Se deberá incluir un resumen del contenido del trabajo con una extensión máxima de 100 palabras (siete u ocho líneas), así como entre cuatro y seis palabras clave.
- Los participantes entregarán el ensayo firmado con un pseudónimo.
- Las colaboraciones se acompañarán, por separado, de una breve referencia del autor que contenga: nombre(s) completo(s), institución de pertenencia y correo electrónico.
- Deberá anexarse también una síntesis curricular (hoja de vida) de cada autor, no mayor a 100 palabras, una fotografía del mismo en formato .jpg y una copia de su credencial de elector, pasaporte o licencia de conducir.

- Deberá anexarse una carta de cesión de derechos a favor de la Caja de Cristal debidamente firmada (escaneada en formato .pdf o .jpg).
- Los textos se entregarán en formato electrónico (.txt, .doc o .docx), con una extensión mínima de 1,500 y máxima de 3,000 palabras (incluyendo título, apartados bibliográficos y notas).
- El tipo y tamaño de fuente deberá ser Arial, en 12 puntos. En caso de que el artículo contenga imágenes o gráficas, deben enviarse por separado en archivo JPG, así como el archivo en donde se generó la imagen o gráfica, en su caso (Excel, ArcMap, SPSS, etc.)
- Las notas y referencias deberán ajustarse a la norma APA en su versión seis. Se incluirá un apartado final con las referencias utilizadas. (https://www.ubu.es/sites/default/files/portal_page/files/guia_estilo_apa.pdf)
- Si se incluyen citas textuales, éstas deberán seguir las siguientes modalidades: si ocupan cinco líneas o menos irán precedidas de dos puntos y entrecorilladas; si son de mayor extensión se ubicarán en párrafo aparte, con sangría, sin entrecorillar y a un espacio.
- Cuando por primera vez aparezca una sigla o acrónimo debe escribirse su significado extenso, con la sigla o acrónimo entre paréntesis.
- Los gráficos que aparezcan en el documento deberán ser enumerados e intitolados, estableciendo en la parte final del gráfico la información correspondiente al pseudónimo del autor.
- No utilizar mayúsculas para destacar o enfatizar alguna palabra; para ese fin, se utilizan las itálicas o cursivas. También las palabras que se refieran a otro idioma deberán usarse en la misma tipología.
- Las itálicas se aplican a los párrafos o palabras que pretenda enfatizar el autor.

IV. Entrega de Trabajos

Toda la información solicitada deberá entregarse dentro del plazo establecido por la presente convocatoria, junto con el Formato de Inscripción debidamente llenado, en la oficialía de partes del ITEI (Av. Vallarta 1312, Col. Americana, Guadalajara, Jalisco) en un horario de 9:00 a 17:00 hrs. en un sobre cerrado con el nombre del pseudónimo en la parte frontal. O por correo electrónico a cajadecristal@itei.org.mx anexando el formato de inscripción llenado y escaneado. La confirmación de la recepción de todos los trabajos se hará de manera electrónica, al correo que el participante indique en su Formato de Inscripción.

V. Plazos

La recepción de los trabajos quedará abierta a partir del día lunes 10 de septiembre del 2019 y se cerrará a las 23:59 horas del lunes 08 noviembre del año en curso 2019. Para los trabajos enviados por correo electrónico o servicio de mensajería, se tomará como fecha de entrega el día en que se reciba el sobre con el ensayo en las oficinas del ITEI. La confirmación de la recepción de todos los trabajos se hará de manera electrónica, al correo que el participante indique en su Formato de Inscripción.

La evaluación de los ensayos se realizará del 11 al 15 de noviembre del 2019 y los resultados se darán a conocer durante el mes de diciembre también del presente año.

VI. Jurado

El Jurado estará conformado por al menos 5 especialistas en materia de transparencia, derecho a la información y protección de datos personales, cuyos integrantes se darán a conocer junto con los resultados del certamen.

Las decisiones del Jurado serán inapelables.

Cualquier caso no considerado en las bases de la presente convocatoria será resuelto a criterio del Jurado y los organizadores.

La participación en este concurso implica la aceptación total de las normas fijadas para esta convocatoria.

VII. Criterios de evaluación

- 10% Ortografía y sintaxis. No tiene errores ortográficos ni de sintaxis.
- 15% Redacción, articulación y claridad. Está bien redactado, la información ordenada y clara.
- 15% Congruencia y consistencia. No hay contradicciones y las conclusiones están fundamentadas.
- 20% Análisis. Hace comparaciones, saca conclusiones, ofrece soluciones, etc.
- 10% Argumentación. Proporciona datos que sustentan los argumentos presentados.
- 15% Cobertura. Cubre los temas requeridos en la convocatoria.
- 15% Investigación. Ofrece fuentes de información bibliográfica o de cualquier otra índole.

Total: 100%

Comité Dictaminador

Pedro Antonio Rosas Hernández

Comisionado Ciudadano del ITEI

Rocío Hernández Guerrero

Director Jurídico y Unidad de Transparencia

Manuel Rojas Munguía

Director del Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales.

Olga Navarro Benavides

Directora de Vinculación y Difusión

Francisco Eduardo Arriola Aranda

Coordinador de Ponencias

ITEI Informa

01 de mayo al 31 de octubre de 2019

Caja de Cristal

Publicación Semestral de Transparencia y Acceso a la Información



Descarga este número y los anteriores desde nuestro micrositio

www.itei.org.mx/cajacristal

itei

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

CYNTHIA PATRICIA CANTERO PACHECO

Recurso de revisión

Fecha de resolución	Número de recurso
31 de julio de 2019	732/2019
Sujeto obligado	
Secretaría Ejecutiva del Sistema Estatal Anticorrupción	
Solicitud	
<i>Listado de ciudadanos que se postularon para ocupar las plazas de Director de Coordinación Institucional, Director de Desarrollo de Capacidades y Director de Inteligencia de Datos, señalando:</i>	
<ul style="list-style-type: none">• Nombre• Grado Académico• Dirección a la que se postula.	
¿Qué respondió el sujeto obligado?	
Por su parte, el sujeto obligado respondió que la petición de información se resuelve en sentido afirmativo parcial, por tratarse de información confidencial, entregando en su lugar una tabla que contiene información estadística, sobre el número de aspirantes de cada una de las direcciones sobre las cuales solicita información y su grado académico.	
Inconformidad	
<i>Por la indebida clasificación de la información solicitada como información confidencial.</i>	

Resolución del ITEI

El sujeto obligado indebidamente clasificó una parte de la información solicitada como confidencial aludiendo a que solo contaba con el consentimiento de 11 aspirantes, omitiendo la información de los 20 restantes en razón de no contar con su consentimiento para dar a conocer la información requerida.

Sin embargo el pleno consideró que la información solicitada, alude a un procedimiento de reclutamiento y/o selección realizado por el sujeto obligado para ocupar diversos cargos públicos.

En este sentido, independientemente de si cuenta o no, con el consentimiento de los aspirantes para proporcionar dicha información, al tratarse de documentos que posee el sujeto obligado y toda vez que se encuentran relacionados con un proceso de selección para la designación de diversos funcionarios públicos, la misma reviste el carácter de información pública que debe darse a conocer.

Razón por lo cual se requirió al sujeto obligado para que proporcione el nombre del resto de los aspirantes, así como el cargo por el cual participó y en cuanto al grado académico y si cumplían o no con el grado académico requerido.

¿Por qué es relevante esta resolución?

Es de interés de la sociedad el transparentar los procesos de selección de los aspirantes a cargos públicos.



CYNTHIA PATRICIA CANTERO PACHECO

Recurso de revisión

Fecha de resolución	Número de recurso
17 de junio de 2019	905/2019
Sujeto obligado	
Sistema de Tren Eléctrico Urbano	
Solicitud	
<i>Fotografías y nombres completos de todas y todos los operadores (choferes) de las rutas denominadas SITREN o SITRAN de la Línea 1, Línea 1-B, Línea 2, Línea 3, y Línea 4.</i>	
¿Qué respondió el sujeto obligado?	
Entregó la información relativa a los nombres de los choferes de las líneas referidas en la solicitud.	
Inconformidad	
<i>El sujeto obligado entrega información incompleta toda vez que no entregó las fotografías solicitadas.</i>	

Resolución del ITEI
El sujeto obligado clasificó las fotografías solicitadas como información confidencial.
El Pleno determinó que:
Quando los usuarios del servicio de transporte público realizan el pago del pasaje correspondiente, se encuentran en contacto visual con el operador de la ruta, por lo que es del dominio público que cualquier persona que tenga acceso al servicio de transporte público puede relacionar la prestación de dicho servicio con la imagen del operador que se encuentra brindándolo.
El artículo 65 de la Ley de Movilidad y Transporte del Estado de Jalisco, establece la obligación de los conductores y operadores de vehículos del servicio público de portar la vista durante sus actividades, un gafete con fotografía y demás elementos que permitan su identificación.
Los usuarios del transporte público tienen derecho a trasladarse de una forma segura, lo que conlleva que la identificación del chofer sea necesaria para tener la certeza de que el chofer que conduce el vehículo fue acreditado por la autoridad competente, situación que puede ser corroborada observando el gafete con fotografía que es emitido por la autoridad competente y que el conductor se encuentra obligado a portar.
Los vehículos a través de los cuales se brinda el servicio público son pagados con recursos públicos, por lo que la información que derive de dicho servicio es generada y administrada por el sujeto obligado como consecuencia del cumplimiento de sus obligaciones, misma que lleva el carácter de información pública.
En consecuencia se ordenó requerir al sujeto obligado a efecto de que entregue las fotografías de los choferes que fueron solicitados.
¿Por qué es relevante esta resolución?
Es relevante para la sociedad identificar a los conductores y operadores del servicio público a través de su fotografía para que hagan uso del servicio de forma más segura.



SALVADOR ROMERO ESPINOSA

Recurso de revisión

Fecha de resolución	Número de recurso
14 de agosto de 2019	1614/2018
Sujeto obligado	
Ayuntamiento de Arandas, Jalisco	
Solicitud	
<i>Información sobre la "Feria de Arandas 2019"</i>	
¿Qué respondió el sujeto obligado?	
El sujeto obligado señaló que la información era inexistente, en virtud de que la "feria de Arandas 2019" fue concesionada mediante el debido proceso, a una empresa, quien fue la que llevó a cabo toda la organización, y en ese sentido se trataba de información del ámbito privado.	
Inconformidad	
<i>Señala que se utilizaron recursos propios del ayuntamiento para la realización de la misma.</i>	

Resolución del ITEI

Atendiendo a la naturaleza que dio origen al vínculo entre el Ayuntamiento y la empresa que organiza la feria, se determinó que las actividades e ingresos relacionadas con la "feria de Arandas" derivan de la explotación de un bien de dominio público, intangible, de carácter patrimonial, en razón de pertenecer a todos los habitantes del municipio e incluso de la entidad, aunado a que se trata de un festival cultural tradicional.

Así, ante la presencia del ejercicio de recursos públicos -entrega de un bien público intangible-, se tiene que rendir cuentas a la sociedad de cómo se explota el bien que reciben en concesión, debiendo haber un pronunciamiento por parte de la empresa concesionaria, persona jurídica denominada "Contenidos Culturales de los Altos S.A. de C.V."; de manera indirecta a través del sujeto obligado que le otorgó la concesión.

¿Por qué es relevante esta resolución?

La información que se genera ya sea derivada de concesiones de servicios o bienes a cargo del Estado, resultan de interés público y social, con independencia de que la misma no se encuentre propiamente dentro de los archivos del sujeto obligado, sino derivado de la relación jurídica entre éste y un particular.

Es importante precisar, que el cumplimiento de obligaciones de transparencia, en estos casos se limitará a hacer pública toda la información relacionada tanto con la recepción y el ejercicio de los recursos públicos que le son concesionados, como aquella relacionada con sus funciones equiparables a actos de autoridad.

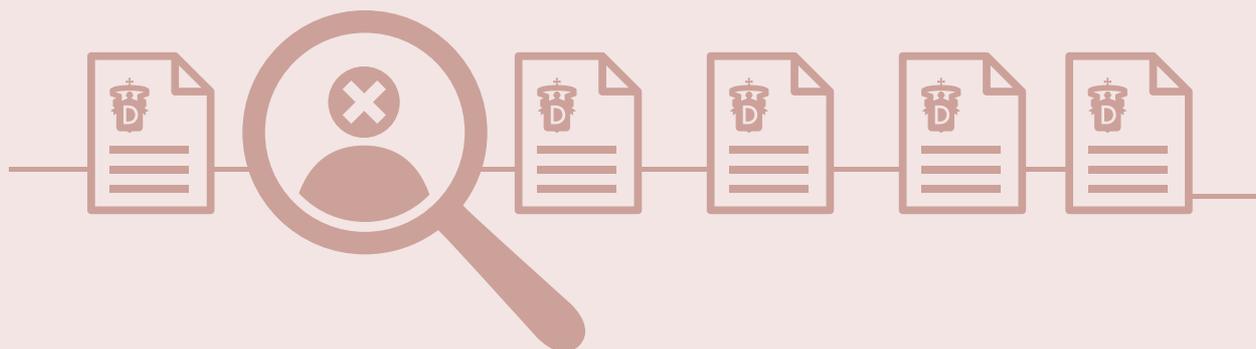


SALVADOR ROMERO ESPINOSA

Recurso de revisión

Fecha de resolución	Número de recurso
14 de octubre de 2019	2279/2019
Sujeto obligado	
Universidad de Guadalajara	
Solicitud	
Se solicitaron las versiones públicas de todas las recomendaciones emitidas por la Defensoría de los Derechos Universitarios.	
¿Qué respondió el sujeto obligado?	
En ese sentido, el sujeto obligado entregó el link del que se desprendía la información en versión pública.	
Inconformidad	
Se negó el acceso a información pública clasificada indebidamente como confidencial, ya que aparecen testados datos personales, entre los cuales no es posible conocer los nombres de los servidores públicos o funcionarios de la Universidad de Guadalajara, que de acuerdo con la propia Defensoría de los Derechos Universitarios, son responsables de alguna violación a los derechos humanos de los universitarios.	

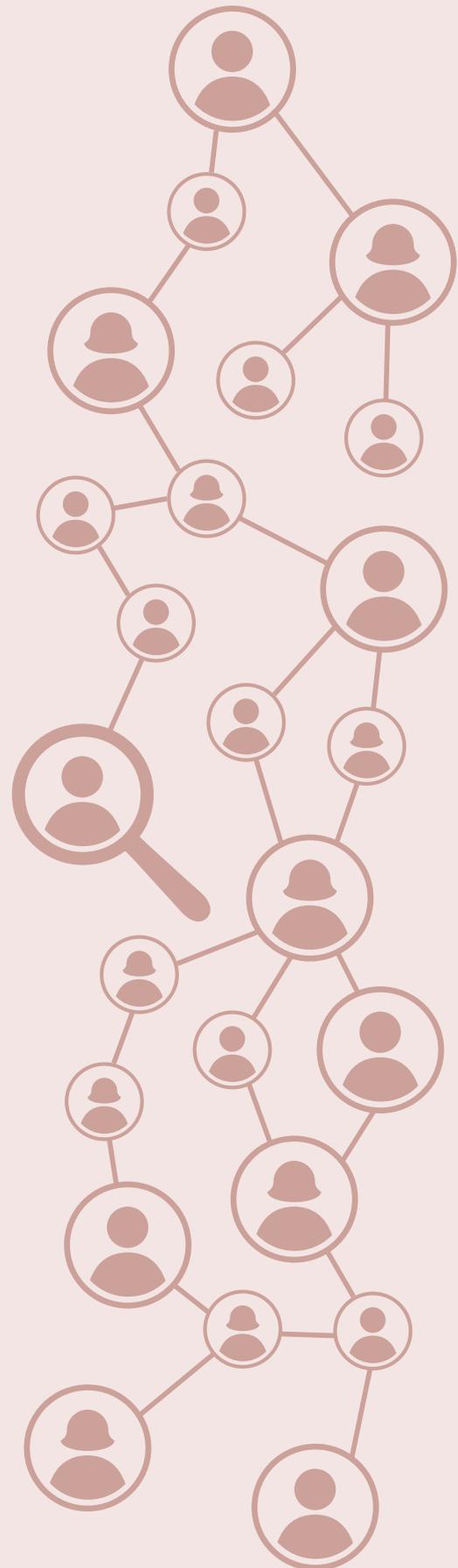
Resolución del ITEI
<p>Se determinó que en el caso concreto, prima el interés público de dar a conocer el nombre del servidor público, integrante de la comunidad universitaria o autoridad universitaria a quien se le imputa la violación de un derecho universitario o la comisión de un acto de violencia en agravio de quien forma parte de la comunidad universitaria, por sobre el derecho a la privacidad o interés particular del mismo, de mantener clasificada dicha información por argumentar que es dato personal al tratarse de su nombre, con base en los elementos de idoneidad, necesidad y proporcionalidad.</p> <p>Lo anterior, ya que la Defensoría de Derechos Universitarios, fue creada para proteger los derechos humanos de la comunidad universitaria, y en ese sentido, sus resoluciones y recomendaciones guardan una semejanza directa con aquellas emitidas por los organismos internacionales, nacionales o estatales en materia de protección de derechos humanos que cumplen con esa misma función en el ámbito de sus respectivas competencias.</p> <p>En ese sentido, es evidente que tanto para el Legislador Nacional como para el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, existe una causa superior de interés público de que se den a conocer los nombres de aquellos servidores públicos sobre los que exista una presunción de violación a derechos humanos, debidamente consolidada en una resolución emitida por una instancia especializada en su protección.</p>
¿Por qué es relevante esta resolución?
<p>Garantizar una ciudadanía informada, se vuelve un elemento fundamental para el funcionamiento de una sociedad democrática, cumpliendo con ello el objetivo de la Ley, que es permitir que los miembros de la sociedad tengan acceso en la mayor medida posible a la información en posesión de dependencias públicas en forma compatible con el interés público y el derecho de privacidad, y en el caso que nos ocupa, existen todos los elementos mínimos necesarios para ordenar la desclasificación de información confidencial que de origen debe protegerse.</p>



PEDRO ANTONIO ROSAS HERNÁNDEZ

Recurso de revisión

Fecha de resolución	Número de recurso
28 de agosto de 2019	1824/2019
Sujeto obligado	Consejo de la Judicatura
Solicitud	<p>“Se me informe por este mismo medio:</p> <ol style="list-style-type: none">1. El nombre y una versión pública del curriculum de todos los visitantes en funciones del Consejo.2. Los resultados de las visitas de inspección que se realizaron a todos los juzgados de primera instancia incluyendo la actuación de los jueces de control y de enjuiciamiento, correspondientes a los años 2017 y 2018, con desglose de los elementos previstos en los artículos 173 y 175 de la Ley Orgánica del Poder Judicial del estado de Jalisco.3. Nombre de los visitantes y quienes tienen relación de parentesco por afinidad dentro del segundo grado o consanguinidad dentro del cuarto grado, con magistrados del Supremo Tribunal de Justicia, consejeros del consejo de la judicatura o jueces de primera instancia del Estado de Jalisco; ya sea que estén en funciones, en retiro, removidos o separados de su encargo.4. Nombre de jueces o juezas y quienes tienen relación de parentesco por afinidad dentro del segundo grado o consanguinidad dentro del cuarto grado, con magistrados del Supremo Tribunal de Justicia, consejeros del consejo de la judicatura, o jueces de primera instancia del Estado de Jalisco; ya sea que estén en funciones, en retiro, removidos o separados de su encargo.5. El resultado de las evaluaciones de los jueces que fueron designados en los últimos 4 años y quienes formaron parte del jurado que los evaluó.”
¿Qué respondió el sujeto obligado?	El sujeto obligado no entregó la información referente al parentesco existente entre los servidores públicos de dicho sujeto obligado.



Inconformidad

“(…)

NO me ha proporcionado el nombre y una versión pública del curriculum de todos los visitantes en funciones del Consejo.

NO me ha proporcionado el nombre de los visitantes y quienes tienen relación de parentesco por afinidad dentro del segundo grado consanguinidad dentro del cuarto grado, con magistrados del Supremo Tribunal de Justicia, consejeros del consejo de la judicatura o jueces de primera instancia del Estado de Jalisco; ya sea que estén en funciones, en retiro, removidos o separados de su encargo.

NO me ha proporcionado el nombre de los jueces o juezas y quienes tienen relación de parentesco por afinidad dentro del segundo grado consanguinidad dentro del cuarto grado, con magistrados del Supremo Tribunal de Justicia, consejeros del consejo de la judicatura o jueces de primera instancia del Estado de Jalisco; ya sea que estén en funciones, en retiro, removidos o separados de su encargo.

NO me ha proporcionado el resultado de las evaluaciones de los jueces que fueron designados en los últimos 4 años y quienes formaron parte del jurado que los evaluó...”

...la información solicitada no se trata de información clasificada como reservada o confidencial o de información inexistente por no estar dentro de la competencia del sujeto obligado, por lo que debe proporcionar la información en los términos de ley y en su caso generarla y focalizarla en la forma solicitada, pues de ello depende el que se pueda conocer con exactitud si existen conflictos de interés...(SIC)

Resolución del ITEI

A pesar de que el parentesco constituye un dato personal que por ende es información pública protegida de acceso restringido; al tratarse de servidores públicos, se considera un dato de interés general, por lo que dicha protección disminuye, en razón de lo cual se puede decir que el parentesco existente entre servidores públicos que laboran en una misma dependencia, adquiere especial importancia.

En ese orden de ideas, aunque no es un requisito de ingreso que las áreas de recursos humanos pidan a los servidores públicos por la información relativa a si guardan alguna relación familiar o de parentesco con otro servidor público que labora en su misma dependencia, sí es factible que dicha área requiera a su personal para que lo manifieste; esto, como se sostiene particularmente en el punto Tercero dictaminado en la Consulta Jurídica 16/15 emitida por el Pleno de este Órgano Garante.

En ese orden de ideas, se requirió al sujeto obligado para que a través del área de Recursos Humanos, realizara la gestión interna correspondiente con los visitantes y jueces, a fin de que manifestaran de manera categórica si tienen relación familiar o de parentesco con los servidores públicos aludidos, con el objeto de que se proporcione el listado de aquellos que se encuentren en ese supuesto.

¿Por qué es relevante esta resolución?

El solicitante tuvo acceso a la información solicitada, de la cual pudo conocer el parentesco que existe entre los servidores públicos del sujeto obligado recurrido.



PEDRO ANTONIO ROSAS HERNÁNDEZ

Recurso de revisión

Fecha de resolución	Número de recurso
31 de julio de 2019	1513/2018
Sujeto obligado	Coordinación General Estratégica de Gestión del Territorio
Solicitud	<p>“...Solicito se me entregue un informe detallado acompañado del soporte documental que lo acredite sobre lo siguiente:</p> <ol style="list-style-type: none">1. Listado de solicitudes ingresadas por el operador del relleno sanitario “Los Laureles” para ampliar la superficie de disposición final (debiendo incluir la totalidad de los intentos; tanto los resolutivos positivos como los desechamientos), a partir del año 2014.2. Listado de solicitudes ingresadas por el operador del relleno sanitario “Los Laureles” para modificar su autorización (debiendo incluir la totalidad de los intentos; tanto los resolutivos positivos como los desechamientos), a partir del año 2014.3. Listado de avisos de modificaciones de infraestructura de etapa de manejo tramitados por el operador del Relleno Sanitario “Los Laureles” (debiendo incluir la totalidad de los intentos; tanto los resolutivos positivos como los desechamientos), a partir del año 20144. Reproducción electrónica (sin costo) de toda la documentación derivada de mis peticiones....”sic
¿Qué respondió el sujeto obligado?	El sujeto obligado dejó a disposición del entonces solicitante la información solicitada previo pago de \$4,634.00
Inconformidad	<p>“...El sujeto obligado en su respuesta dice:</p> <p>“..En respuesta a la solicitud antes mencionada la Dirección Ejecutiva de Protección y Gestión Ambiental, emitió el oficio SEMADET DGPGA/DEIA/ No. 353/1287/2016, donde se niega la autorización en materia de impacto ambiental. Se emite prevención y apercibimiento del proyecto de Integración y Regularización del predio rústico Los Pinos al relleno sanitario Los Laureles.</p>

Es importante destacar que, en materia de evaluación de impacto ambiental, se cuenta únicamente con una solicitud ingresada desde el año 2014 a la fecha.

Así mismo, se informa que la reproducción electrónica de la documentación en términos del artículo 38 fracción IV inciso e) y g) de la Ley de Ingresos del Estado de Jalisco para el Ejercicio Fiscal 2019 y sus anexos se pone a disposición la copia electrónica a través de un disco compacto de documentos señalados con su debida protección de datos, esto previo a la exhibición del recibo de pago de derechos correspondiente por la emisión de 351 copias escaneadas de las cuales la primera (sic) 20 se pones (sic) a disposición de manera gratuita más un disco compacto, donde la cantidad a erogar es de \$4,634.00 (cuatro mil seiscientos treinta y cuatro pesos 00/100 M.N.) y \$24.00 (veinticuatro pesos 00/100 M.N.)”

Pretendiendo que el usuario erogue un monto de \$4,634.00 (cuatro mil seiscientos treinta y cuatro pesos 00/100 M.N.) por la reproducción de documentación que expresamente solicitó en versión digital sin costo; fundamentando la Autoridad su respuesta en “.. la reproducción electrónica conlleva el escaneo de los documentos solicitados, por lo que en términos del 38 fracción IX inciso g) de la citada ley..” ; fundamentación que resulta totalmente errónea y discrecional, al determinar por propia voluntad que la generación de la versión pública y digital implica el escaneo de la documentación ingresada por el particular, siendo que tal información debiera existir ya en tal modalidad dentro de sus archivos.

Aunado a lo anterior, la Autoridad pretende justificar la erogación del particular fundamentando su interpretación unilateral en el numeral ..”38 fracción IX inciso g) de la citada ley..”, esto, refiriéndose a la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, cuyo artículo se cita para mayor ilustración:

“..Artículo 38. Instituto - Remuneraciones. 1. La remuneración bruta anual de los servidores públicos

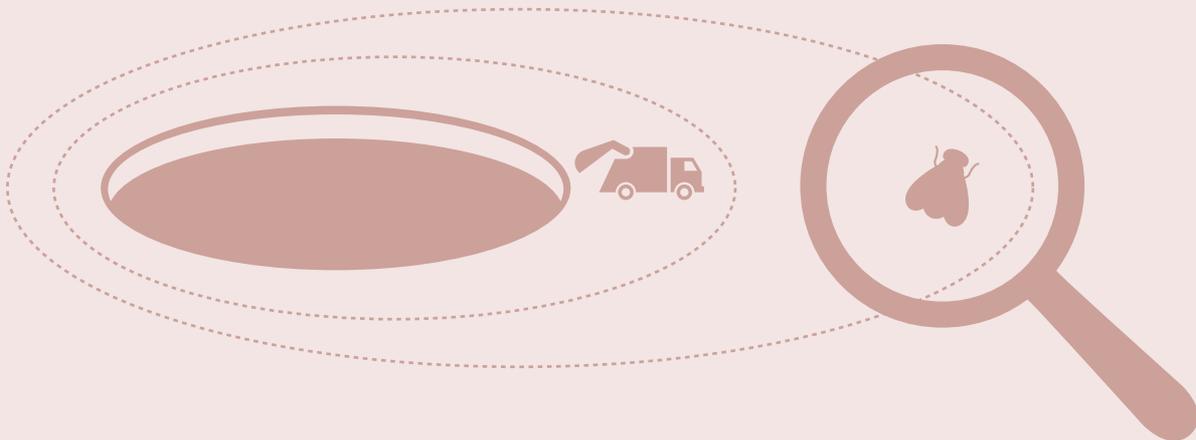
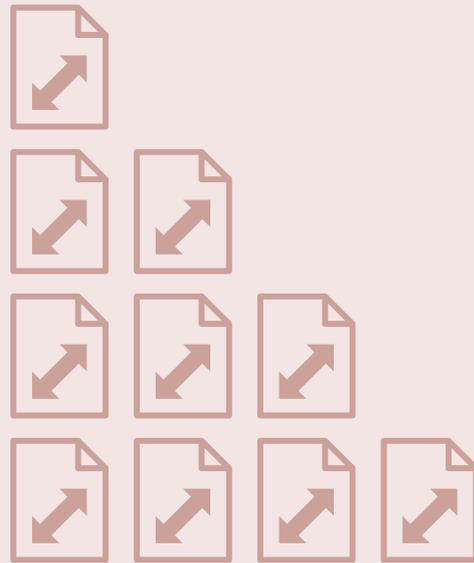
Resolución del ITEI

Es preciso señalar que de conformidad con lo establecido en el numeral 89.1 fracción II de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, la reproducción de documentos no puede imponerse al solicitante, salvo que el sujeto obligado determine que no es viable entregar la información mediante otro formato y no pueda permitirse la consulta directa de documentos por contener información pública protegida; no obstante, en el caso que nos ocupa el sujeto obligado no determinó que no era viable entregar la información en el formato solicitado o que no pudiera permitir la consulta directa.

Por otra parte, si bien es cierto el sujeto obligado manifestó a través de su informe de ley, que serían entregadas al ahora recurrente las primeras 20 veinte copias de manera gratuita, se estima, que de igual forma debe hacer entrega de manera electrónica, del resto de la información; ya sea mediante discos compactos previo pago de los derechos correspondientes o en USB; lo anterior, tiene sustento en la Consulta Jurídica 15/14 emitida por el Pleno de este Órgano Garante.

¿Por qué es relevante esta resolución?

Se garantizó el derecho de acceso a la información pública en poder de los sujetos obligados, privilegiando el principio de gratuidad y celeridad, con el cual, el recurrente no realizó pago alguno por ejercer un derecho considerado como fundamental.





Transparencia

al alcance de todos

Por medio de este proyecto, el ITEI contribuye a la igualdad social de los grupos en estado de vulnerabilidad de nuestra entidad para el pleno ejercicio de los derechos de acceso a la información pública y protección de datos personales.

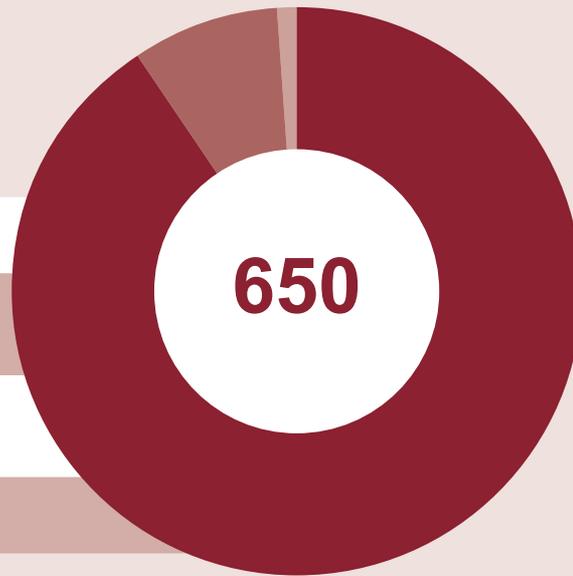
Conoce más en
www.itei.org.mx/alalcancedetodos

Resoluciones aprobadas por tipo de recurso

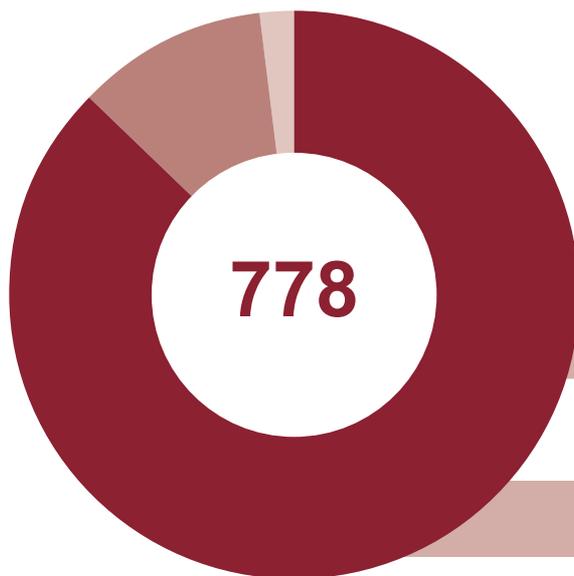
Periodo comprendido del 01 de mayo al 31 de octubre de 2019

Cynthia Patricia Cantero Pacheco

Tipo de recurso	Número total de los recursos resueltos
Recursos de Revisión	589
Recursos de Transparencia	54
Recursos de Revisión de Datos Personales	7
Total	650



- Revisión
- Transparencia
- Revisión de Datos Personales



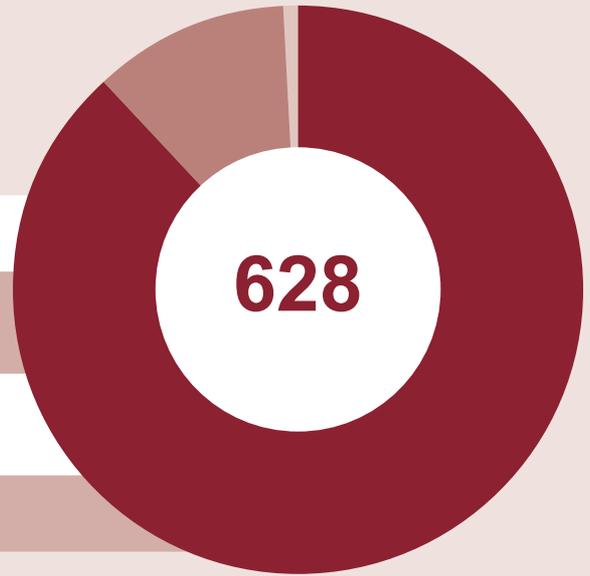
Salvador Romero Espinosa

Tipo de recurso	Número total de los recursos resueltos
Recursos de Revisión	680
Recursos de Transparencia	85
Recursos de Revisión de Datos Personales	13
Total	778

- Revisión
- Transparencia
- Revisión de Datos Personales

Pedro Antonio Rosas Hernández

Tipo de recurso	Número total de los recursos resueltos
Recursos de Revisión	554
Recursos de Transparencia	70
Recursos de Revisión de Datos Personales	4
Total	628



- Revisión
- Transparencia
- Revisión de Datos Personales

Sigue las sesiones de pleno del ITEI
en nuestro sitio web

www.itei.org.mx

o en nuestro canal de youtube

 **iteijalisco**

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

**GOBIERNO
ABIERTO**

Jalisco



gobiernoabiertojalisco.org.mx





Visite nuestro micrositio www.itei.org.mx/cajacristal

Esta revista se terminó de imprimir en junio de 2019 en
XXXXXX XXXXX X X X XXXXX XXXX X
XXXXX X X X X X XXXXX XXXXXXXX

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