El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

25

Cuadernos de transparencia

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

IRENE LEVY MUSTRI

El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

IRENE LEVY MUSTRI

DIRECTORIO

El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

---

Primera edición electrónica en PDF, octubre de 2017.
ISBN: en trámite

Ilustración de portada:
Viridiana Martínez

25

Cuadernos de transparencia

ÍNDICE

LA AUTORA

IRENE LEVY MUSTRI

Abogada egresada de la Escuela Libre de Derecho. Maestra en derecho por el Centro de Estudios de Posgrado en Derecho y con estudios de maestría en administración pública por el Instituto Nacional de Administración Pública de México (INAP). Actualmente es presidenta de Observatel A.C. "El Observatorio de las Telecomunicaciones de México", organización no gubernamental, cuyo objetivo primordial es observar y analizar la actualidad, así como la evolución de las telecomunicaciones, la radiodifusión y, en general, las tecnologías de la información, a partir de diversas perspectivas (www.observatel.org).

Fue miembro del Consejo Consultivo del Instituto Federal de Telecomunicaciones de febrero de 2015 a marzo de 2017; desde 2012 es integrante del Consejo Consultivo del Consumo de la Procuraduría Federal del Consumidor; académica de la Universidad Iberoamericana desde 2001; columnista del periódico *El Universal* desde 2011 y es investigadora honoraria de la Escuela Libre de Derecho.

Desde 1994 y hasta el año 2000, se desempeñó como funcionaria pública en la SCT, así como directora general de la desaparecida COFETEL. Desde entonces, y hasta el día de hoy, es consultora independiente en temas de telecomunicaciones, radiodifusión y tecnologías de la comunicación e información. Entre otros, ha asesorado al Senado de la República, a la Secretaría de Gobernación, así como a la CFE en estos temas.

Ha publicado varios ensayos y artículos en libros y revistas especializadas. Fue columnista de los periódicos *El Economista* y *El Financiero*, y comentarista de radio en temas de telecomunicaciones en Radio Fórmula (103.3 FM), conductora del programa de radio *Mediatelecom: convergencia plena* durante 2012 en MVS Radio (102.5 FM) de la Ciudad de México, así como *contributor* de Bloomberg TV en temas de telecomunicaciones y radiodifusión hasta el año 2015.

25

Cuadernos de transparencia

PRESENTACIÓN

LA RED Y LAS HERRAMIENTAS DE COMUNICACIÓN QUE SE HAN GENERADO EN LA ÚLTIMA DÉCADA, COMO FACEBOOK, YOUTUBE Y TWITTER HAN ALTERADO LAS NORMAS DE COMUNICACIÓN ENTRE LAS PERSONAS Y SUS GOBIERNOS. No se puede negar cómo estos medios influyen profundamente en las formas de organización del trabajo, de las empresas, el tejido social e incluso en cómo se emparentan las personas, manejan y controlan su vida afectiva. Y más lejos, es común escuchar cómo estas herramientas han llevado a la democratización de la información y transparentar las acciones de gobierno.

Pero estas grandes novedades, que en principio las observamos como positivas, transportan un aspecto controvertido: la invasión de la privacidad y la circulación de datos personales sin el control de las personas, creando una gran tensión entre la libertad de expresión, la transparencia y los derechos humanos.

Sin embargo, el propósito de la autora no es estigmatizar a los medios digitales, al contrario nos presenta una crítica positiva sobre sus usos en la función pública. Tomando como ejemplo el uso de la aplicación *Periscope* por parte del *City Manager* de la delegación Miguel Hidalgo de la Ciudad de México como vertebrador de su exposición, nos presenta, de manera ágil, la importancia del debate acerca de la protección de datos personales en el contexto del uso de las nuevas tecnologías de la información y la comunicación (TIC).

En esta publicación donde impera el espíritu que su autora tiende en los diversos espacios de su trayectoria profesional, desde artículos periodísticos, que publica cotidianamente en diversos medios de escala nacional, hasta sus actividades en la esfera académica y en el ámbito de la administración pública, nos lleva de manera

ágil por un tema complejo: tras hacer una revisión del marco normativo, se decanta por una regulación en torno a las fricciones que surgen ante el registro en medios informáticos de captura de video e imagen, de los actos de autoridad en el espacio público y su incidencia en la esfera de los derechos de las personas.

Estimados lectores, nos permitimos recomendar ampliamente la lectura de este *Cuaderno de Transparencia*, puesto que el texto que tiene en sus manos contribuye con reflexiones claras, redondas, a una discusión de carácter público de notable actualidad.

Comité Editorial del INAI

INTRODUCCIÓN

Damiens fue condenado, el 2 de marzo de 1757, a pública retractación ante la puerta principal de la Iglesia de París, adonde debía ser llevado y conducido en una carreta, desnudo, en camisa, con un hacha de cera encendida de dos libras de peso en la mano; después, en dicha carreta, a la plaza de Grève, y sobre un cadalso que allí habrá sido levantado [deberán serle] atenaceadas las tetillas, brazos, muslos y pantorrillas, y su mano derecha, asido en ésta el cuchillo con que cometió dicho parricidio, quemada con fuego de azufre, y sobre las partes atenaceadas se le verterá plomo derretido, aceite hirviendo, pez resina ardiente, cera y azufre fundidos juntamente, y a continuación, su cuerpo estirado y desmembrado por cuatro caballos y sus miembros y tronco consumidos en el fuego, reducidos a cenizas y sus cenizas arrojadas al viento. Finalmente, se le descuartizó, refiere la Gazette d'Amsterdam. Esta última operación fue muy larga, porque los caballos que se utilizaban no estaban acostumbrados a tirar; de suerte que en lugar de cuatro, hubo que poner seis, y no bastando aún esto, fue forzoso para desmembrar los muslos del desdichado, cortarle los nervios y romperle a hachazos las coyunturas.

Michael Foucault[1]

AUNQUE NOS HEMOS VUELTO MENOS SANGUINARIOS Y EL RÉGIMEN PUNITIVO HA CAMBIADO EN LA ERA "MODERNA", SIGUE SIENDO TENTADOR PARA LA AUTORIDAD, Y CATÁRTICO PARA LA POBLACIÓN, CERTIFICAR EN VIVO LA SANCIÓN AL MAL PORTADO.

Los linchamientos a los delincuentes ocurren más frecuentemente de lo que imaginamos, y cuando lo escuchamos o vemos en los medios informativos, normalmente nadie siente pena por el linchado, por el contrario, casi siempre se justifica a pesar de que es literalmente una barbarie, un asunto de psicología de masas que no debe soslayarse en la ponderación del tema que nos ocupa.

Sobre los linchamientos, Carlos Monsiváis (2004) explicaba que esta *masa* de personas consolida su eficiencia gracias a su *rapidez avasalladora*. En

innumerables casos de linchamiento en México, ha resultado suficiente el esparcimiento de un rumor ("han secuestrado niños", "son secuestradores", "son rojillos", "son de una secta", "están violando niñas") para movilizar y enardecer al colectivo. Esa rapidez de alguna forma demuestra la intención de los actos violentos y cierta lógica —perversa— en actos de masificación que parecen mantener la cohesión social, al menos por unas horas. No importa la inocencia de los presuntos delincuentes, a la turba no le preocupan sus derechos humanos y menos aún la presencia de pruebas que verifiquen su inocencia. La sentencia está dictada y como señala Monsiváis:[2]

> En una turba linchadora, cada uno de sus integrantes abandona con presteza sus reservas éticas (las que tenga), su respeto por la vida humana (el que sea) y su miedo al castigo, nunca muy potente porque —esta es la presunción— el crimen cometido por muchos no es culpa de nadie (p.9).

Asimismo, Gustavo Rojas Bravo,[3] citando a Le Bon para plantear el problema, refiere en sus *Apuntes sobre linchamiento y la construcción social del miedo* que:

> En determinadas circunstancias, y tan sólo en ellas, una aglomeración de seres humanos posee características nuevas y muy diferentes de las de cada uno de los individuos que la componen. La personalidad consciente se esfuma, los sentimientos de todas las unidades se orientan en una misma dirección. Se forma un alma colectiva, indudablemente transitoria, pero con características muy definidas. La colectividad se convierte entonces en aquello que a falta de otra expresión mejor, designaré como masa organizada o si se prefiere, masa psicológica. Forma un solo ser y está sometida a la *ley de la unidad mental de las masas*.

¿ES LEGAL QUE LA AUTORIDAD TRANSMITA EN VIVO VIDEOS DE CIUDADANOS INFRACTORES? (...) ¿ES JUSTIFICABLE LA VULNERACIÓN DE LA PRIVACIDAD FRENTE AL VALOR DE LA TRANSPARENCIA –SUPONIENDO QUE ESTE FUERA – EN EL ACTUAR DE LOS FUNCIONARIOS O DE LA EXHIBICIÓN PÚBLICA DEL MAL CIUDADANO?

No tenemos que irnos al extremo de los linchamientos sanguinarios, la sola aparición de una imagen, un video o un audio en las redes sociales que denuncia a una persona que actuó "mal", nos hace presumir su culpabilidad. Nadie, o casi nadie, inicia de manera imparcial su travesía por esa inquisición.

Este ensayo pretende plantear algunos elementos que coadyuven a ponderar el uso de las tecnologías por parte de las autoridades, específicamente de la transmisión de imágenes estáticas o en video donde muestren la imagen, voz y otros datos personales de ciudadanos cometiendo, o relacionados con su comisión, infracciones administrativas. Esta inquietud surge de la recien-

te práctica realizada desde finales del año 2015 por un polémico funcionario encargado de cuidar el orden y la civilidad en la delegación Miguel Hidalgo, en la Ciudad de México, que transmitía videos en vivo, a través de la aplicación llamada *Periscope*,[4] de ciudadanos cometiendo infracciones tales como estacionar el coche en lugares no permitidos o tirar basura en la calle, entre otras conductas. De acuerdo con su propia página, *Periscope* "es la forma más fácil de transmitir en vivo desde tu teléfono" y la aplicación "permite compartir lo que está sucediendo a tu alrededor, con todo el mundo o solo con unos cuantos amigos tal y como sucede en vivo".[5]

Además, como señala Kayvon Beykpour, cofundador de la aplicación, "a diferencia de *YouTube* donde la experiencia de visualización es pasiva, en *Periscope* es activa. Los espectadores pueden comentar, formular preguntas y enviar corazones en tiempo real".[6]

¿Es legal que la autoridad transmita en vivo videos de ciudadanos infractores? ¿Qué fin se persigue con ello: sancionar, obtener pruebas, disuadir a otros de cometer conductas negativas, hacer propaganda política, transparentar su actuación? ¿Es lo mismo jurídicamente que un particular divulgue datos personales de terceros a que lo haga la autoridad? ¿Es justificable la vulneración de la privacidad frente al valor de la transparencia —suponiendo que este fuera— en el actuar de los funcionarios o de la exhibición pública del *mal ciudadano*? ¿Están las autoridades, en dicho papel, ejerciendo su derecho a la libertad de expresión? ¿Se plantea una colisión de derechos válida?

El tema que nos ocupa debe ser analizado desde diversas perspectivas y requiere un enfoque multidisciplinario porque resulta necesario conocer la causa que lleva a estas conductas y reacciones. Me refiero al uso de *Periscope*, pero sobre todo a las diferentes reacciones que esto causa en las personas exhibidas al verse evidenciadas, así como las de la gente que observa; son muchas las reacciones que habrán de observarse y analizarse. ¿Por qué las autoridades querrían exhibir públicamente a sus ciudadanos infractores —o supuestamente infractores— en vivo, en video? ¿Por qué un importante segmento de la población está satisfecho con esta actuación o con la política empleada por sus gobernantes a pesar de que conforma, digámoslo así, un auténtico *bullying*? Esta situación es tan compleja que en realidad no es el resultado, sino el síntoma de una enfermedad que debemos analizar desde el punto de vista psicológico, sociológico, antropológico, comunicacional, regulatorio, político y, desde luego, jurídico. El enfoque jurídico da respuesta a una de las perspectivas del tema: analizan-

do la colisión de derechos que plantea la situación, se podrá concluir si se han violado o no las leyes o los derechos en esta exposición del ciudadano. Pero, además de la propuesta jurídica, es menester analizar el resto de los enfoques. No resulta limitado el análisis del caso *Periscope* que se mencionó en párrafos anteriores, pues aun cuando se trata de una aplicación tecnológica específica, sus repercusiones resultan ser comunes a otros casos con tecnologías similares, por lo que pueden extrapolarse sin mayor análisis.

El estudio de estos temas resulta tan urgente como la definición de las diversas autoridades competentes en torno a sus límites. No cesarán los retos sociales, jurídicos y de política pública que presentan el uso de las tecnologías en los diferentes ámbitos y, con ciertas modalidades de uso, ciertos derechos fundamentales podrían estar comprometidos. Por ello el abordaje y definición en la actualidad de este tema resultan tan oportunos, como necesaria es la protección y garantía de los derechos que pueden verse afectados con su utilización.

No solo tenemos autoridades en las que no confiamos, sino que incluso son abiertamente infractoras. Buena parte de la ciudadanía desprecia la ley, en parte por no tener la certeza de que le irá bien a quien la cumpla y a quien la viole le irá mal. La forma de solucionar las cosas en México parece estar en un terreno lejano a la regulación porque cuando padecemos en carne propia la violación de la ley y nos afecta directamente, hemos observado que la vía para lograr justicia no siempre es la observancia de la ley, sino el compadrazgo, las influencias, la corrupción. Ante un escenario así, los mexicanos nos sentimos huérfanos. La orfandad social atribuible a la ausencia de una autoridad respetable y legítima que nos haga sentir protegidos y cuidados, la orfandad del padre. Ante esa necesidad, la aparición de un justiciero interesado en que se cumpla la ley y someta al escrutinio social al que no la observa, es deseada, aplaudida y bienvenida. Así, aun cuando el problema causante de esta situación es social y no jurídico, la solución formal podemos encontrarla en el marco legal vigente o en una propuesta modificatoria.

No cabe duda: el tema es tan polémico como seductor, y aunque afirmo que la solución jurídica no es la solución de todo el asunto, sí es menester revisar este aspecto porque las autoridades encargadas de revisar la legalidad de la actividad (Poder Judicial, organismos autónomos y Poder Ejecutivo) deben actuar.

A lo largo de estas páginas no analizaré el contexto jurídico del manejo de información entre particulares, es decir, el conflicto jurídi-

co que puede darse si un particular revela datos (incluyendo imágenes) de otro particular, pues cae en una vertiente distinta de estudio. Tampoco analizaré el caso de cuando un ciudadano exhibe a un servidor público. Me he propuesto iniciar con un paseo general por algunas tecnologías y su doble incidencia en la vida social e individual. En el capítulo dos replico las razones que ha dado la autoridad para justificar su práctica, reviso el marco conceptual y jurídico en torno al tema y analizo si existe colisión de derechos. En el capítulo tres, ofrezco algunos ejemplos de países en los que existen ciertas directrices de cómo deben usar las autoridades las tecnologías, concretamente las redes sociales, en el ejercicio de sus funciones. Finalmente, en el último capítulo, ofrezco las conclusiones y mi propuesta sobre la problemática que se me ha encomendado analizar.

El objetivo de los párrafos que componen este *Cuaderno de Transparencia* es ofrecer al lector una visión amplia y documentada que le permita formar su propia opinión con mayores elementos que los que se podrían tener en una simple charla de café. Valdrá la pena seguir el tema a través del tiempo, pues estas son cuestiones sumamente dinámicas.

El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

CAPÍTULO I

NUEVAS TECNOLOGÍAS: ¿SOLUCIÓN O RIESGO?

> *La tecnología […] es una cosa extraña. En una mano trae grandes regalos, y luego con la otra te apuñala por la espalda.*
>
> C.P. Snow, *New York Times*, 1971.[7]

CUANDO HABLAMOS DE INTERNET, REDES SOCIALES U OTRAS TECNOLOGÍAS DE LA INFORMACIÓN TENDEMOS A PERDERNOS EN UN MAR DE CONSIDERACIONES TÉCNICAS Y JURÍDICAS QUE NOS CONFUNDEN MÁS DE LO QUE NOS ACLARAN, Y ESTO SUCEDE, EN PARTE, PORQUE –HAY QUE DECIRLO SIN TAPUJOS– NOS PREOCUPA SER PERCIBIDOS COMO CENSORES, RETRÓGRADAS, POCO MODERNOS, POCO DEMOCRÁTICOS O BIEN, TOCAR EL EXTREMO CONTRARIO.

Pero en el fondo, el estudio de los distintos temas en los que la tecnología se ve involucrada, no escapa de las consideraciones tradicionales del análisis, aunque ciertamente su abrumadora novedad puede confundirnos. No se trata, pues, de satanizar ni deificar a las tecnologías, sino de observar sus bondades y desventajas.

El hecho de que las tecnologías ahora permitan registrar, monitorear y comunicar casi todo, plantea un cambio de paradigma en la protección de la privacidad, se trata de un modelo más bien dinámico que debe estar en permanente observación por encontrarse en tensión entre los intereses que están en juego y los objetivos que se persiguen; por un lado, los gobiernos siempre querrán conocer más de sus ciudadanos y estarán en la constante tentación de invadir su esfera privada en busca de control y gobernabilidad; por su parte, los particulares nos mantenemos en la dualidad de la privacidad contextualizada, tal y como la califica Helen Nissenbaum, en su libro *Privacidad amenazada*,[8] divulgando nuestra información en ciertos contextos (como *Facebook* o *Twitter*) y exigiendo el respeto a nuestra privacidad a quien se encuentre fuera de ese ámbito. Así, lo que se considera como "privado", y lo que se considera como una invasión o violación de la privacidad, variará en diferentes contextos; en otras palabras, afirma Nissenbaum, lo privado es altamente contextual.

Resulta imposible analizar una a una, todas las tecnologías y su manejo por parte de los gobiernos, por eso

he elegido algunas de ellas que tienen tintes similares: la videovigilancia, la utilización del video por *streaming*[9] (como *Periscope*) y los trámites gubernamentales que analizo en tanto sean manejadas por las autoridades pues, como dije en la introducción, no trataré el ámbito de interacción particulares-particulares.

1. VIDEOVIGILANCIA

La colocación de cámaras en las calles que graban ininterrumpidamente lo que pasa ante su ojo es cada vez más común, hemos empezado a acostumbrarnos al "gran hermano". Según un informe en *Forbes*, en los Estados Unidos de América se estima que el número de cámaras de videovigilancia alcanza los treinta millones, lo que arroja la cifra de más de cuatro mil millones de horas semanales de grabación.[10] Sobre la videovigilancia existen numerosos estudios y análisis que profundizan acerca de sus efectos en la conducta de los individuos y ponderan su eficacia frente a la vulneración de la privacidad. Vale la pena tratar este tema como análogo por su similitud con el caso que nos ocupa de *Periscope*, aunque no se trate de transmisiones hechas públicas en tiempo real, lo cierto es que comparten algunas consideraciones de orden jurídico y la videovigilancia tiene ya más historia y, por tanto, contamos con mayor análisis.

LA COLOCACIÓN DE CÁMARAS EN LAS CALLES QUE GRABAN ININTERRUMPIDAMENTE LO QUE PASA ANTE SU OJO ES CADA VEZ MÁS COMÚN, HEMOS EMPEZADO A ACOSTUMBRARNOS AL "GRAN HERMANO"

1.1 LA COCINA DE LA UNIVERSIDAD HEBREA DE JERUSALÉN

Resulta muy interesante el análisis que hace Edna Ullmann-Margalit,[11] sobre la videovigilancia, a partir del caso de la instalación de cámaras en la cafetería de la Universidad Hebrea de Jerusalén. En el verano de 2007, se tomó la decisión de instalar un circuito cerrado en la cafetería del Centro de Estudios de Racionalidad. La Universidad envió un correo a todos los miembros explicando que las cámaras fueron instaladas para solucionar el problema de la limpieza en la cocina, pues no todos recogían su bandeja ni ponían los platos sucios donde debían. En minutos llegaron las respuestas expresando profundo desacuerdo en el sentido de que lo consideraban ofensivo. Lo interesante es que, a partir de ese hecho, la gente empezó a manifestar otra serie de preocupaciones relacionadas con la efectividad de la vigilancia electrónica, así como su moralidad; la diferencia entre ser visto por una persona y ser visto por una cámara, y los métodos y costos involucrados en confrontar y sancionar a los colegas. También se cuestionó si la cafetería era un espacio público o uno privado.

Ullmann analiza las consecuencias que puede tener en la conducta de los individuos y de la sociedad, el actuar sabiendo que estamos siendo vigilados e incluso grabados. La vigilancia

de cualquier tipo puede crear, afirma, efectos aterradores en la conducta de las personas, inhibiéndolos de actuar de manera espontánea, tal y como lo dijo Snowden:

> Estando bajo vigilancia actuamos de forma menos libre, lo que de hecho significa que somos menos libres.[12]

También hace una clara diferencia en la justificación de la videovigilancia para propósitos criminales, como colocar una bomba o robar un establecimiento, y aquellos no delictivos, como tirar basura o pasarse un alto.

Ullmann se pregunta cuál es el efecto esperado de poner cámaras en la cafetería de la universidad. Por un lado, se piensa que la cámara disuadirá a potenciales trasgresores y, por otro, que en caso de que los haya identificará a los culpables. La disuasión puede funcionar hasta cierto punto, mantener la cocina limpia siempre, no puede depender solo del efecto disuasivo de las cámaras. De hecho, la presencia de la cámara puede desatar una cadena de reacciones trayendo consecuencias inesperadas. Por ejemplo, la gente puede buscar evitar los encuentros con las cámaras y dejar sus platos sucios en todos lados en lugar de regresarlos a la cocina. No siempre respondemos de la forma en que se espera. El diseño humano, agrega Ullmann, puede sorprendernos e incluso ofrecernos resultados contrarios a lo esperado.

1.2 MÉXICO Y LA RECOMENDACIÓN 21 DE LA CNDH

En México, la videovigilancia es cada vez más prolífica sin que nos acerquemos aún a países como Reino Unido o China (en donde hay una cámara cada 43 habitantes).[13] La regulación de la videovigilancia en nuestro país en realidad es poco conocida; existen algunas leyes y reglamentos en el ámbito local,[14] pero en realidad poco se ha profundizado sobre el tema, tal pareciera que no se han dimensionado los efectos y consecuencias de la videovigilancia en la conducta de los individuos, pero también en la vulneración real y potencial de la información que se almacena. Al respecto, llama la atención una recomendación de la Comisión Nacional de los Derechos Humanos (CNDH) un tanto preocupante, la número 21 publicada en el *Diario Oficial de la Federación* el 20 de octubre de 2014.[15] Dicha recomendación versa sobre la prevención, atención y sanción de casos de violencia sexual en contra de las niñas y los niños en centros educativos, específicamente se enfoca en el desarrollo del tema de la violencia sexual infantil cuando se suscita en centros escolares tanto públicos como privados, siendo este tema de particular relevancia por los derechos de la

infancia que se vulneran como resultado de este fenómeno, tales como la libertad sexual, la integridad personal, el trato digno, la educación y el desarrollo, y considera, sobre todo, la gravedad que implica que en centros donde deberían ser tratados con dignidad y formados, sean agraviados.

Así, este documento de la CNDH concluye recomendando tanto al secretario de Educación Pública como a los gobernadores y jefe de Gobierno de la Ciudad de México, entre otras cuestiones, lo siguiente:

> Se instruya a quien corresponda, con la finalidad de que se realicen revisiones en los centros escolares con el objetivo de asegurar que las instalaciones sean adecuadas para que las niñas y los niños puedan ejercer de forma sana y segura su derecho a la educación al interior de las mismas, y asimismo, **se gestione la instalación de cámaras de video en puntos estratégicos de los planteles educativos**. [Énfasis añadido]

El problema no es la recomendación en sí misma sino la ligereza con la que se hace, sin aportar absolutamente ningún parámetro o límite sobre los lugares que llamó "puntos estratégicos"[16] (un punto estratégico —de conformidad con lo que la propia CNDH ha alertado— son, por ejemplo, los baños), sin mencionar qué manejo se daría a las horas de video almacenadas ni quiénes podrían tener acceso a dicha información. Con esto, han metido en un gran lío a las instituciones educativas pues estas tienen el deber de proteger los datos personales y la privacidad de los alumnos, profesores y todos los que acudan a la escuela. El de la CNDH es un ejemplo de lo poco que se analizan los efectos que puede tener una medida en la invasión a la privacidad. Aún no existe la cultura en nuestro país de revisar a fondo este tipo de temas.

LA TECNOLOGÍA NO SOLO DEBE SER VISTA COMO SOLUCIÓN, SINO TAMBIÉN COMO UN INSTRUMENTO QUE PLANTEA NUEVOS DESAFÍOS A LA PROTECCIÓN DE LA PRIVACIDAD Y HAY QUE ABORDARLOS SIN TEMOR

2. TRANSMISIÓN DE VIDEOS EN TIEMPO REAL

Aunque *Periscope* no es la única aplicación que permite transmitir masivamente un video en tiempo real, pues existen otras como *Live* video de *Facebook*, *Lifehacker* o *YouTube Connect* de *Google*, el éxito de *Periscope* se debe quizás a que es propiedad de *Twitter* y por tanto está vinculado a esta red social (o red de información como algunos ya catalogan a *Twitter*) o red social de información. Fue lanzado en marzo de 2015, cuatro meses después tenía 10 millones de usuarios[17] y al cabo de un año acumulaba más de 200 millones de transmisiones y el equivalente a 110 años en videos en vivo son vistos cada día. Así, con nuestro teléfono móvil podemos transmitir video en vivo vin-

culándolo a *Twitter*, de tal suerte que lo transmitido puede estar abierto solo a los seguidores o bien a todo aquel que quiera verlo.

Pues bien, como mencioné en la introducción, se ha desatado una interesante polémica debido a que, en los últimos meses, Arne aus den Ruthen, quien fuera[18] director general de Administración Delegacional de la delegación Miguel Hidalgo de la Ciudad de México,[19] cargo conocido como *City Manager*, instauró una práctica que, aunque ha sido más aplaudida que denostada por buena parte de la ciudadanía, lo cierto es que ha abierto la discusión sobre cuáles deben ser los límites de las autoridades frente a la privacidad de los ciudadanos y al manejo de sus datos personales, sobre todo cuando estos son vistos en flagrancia violentando las normas vigentes. La práctica consistió en transmitir, a través de *Periscope*, las diligencias que él personalmente llevaba a cabo en la demarcación de su jurisdicción, a este programa le llamó #vecinogandalla:[20] desde quitar botes y tubos que algunos colocaban para apartar un sitio para estacionarse o identificar coches estorbando, hasta temas de construcción o solicitar a personas, supuestamente ejerciendo la prostitución, que se retiren de la vía pública, entre otras cuestiones. Después remitía presuntos infractores (que de ahora en adelante llamaré infractores sin que esto juzgue sobre su responsabilidad), en algunos casos, al juez cívico. La cuestión fue que esos videos se transmitieron sin censura, mostrando la imagen y la voz de las personas, incluso en algunos de ellos sus nombres, ubicación, placas de los coches, entre otros datos.

La actitud de los exhibidos era generalmente de molestia o enojo profundo. Varios de ellos reaccionaban sacando su propio celular y grababan también al funcionario. Supongo que las diferentes reacciones han sido un banquete intelectual para los psicólogos y sociólogos. Lo cierto es que para los abogados ha representado una interesante polémica sobre la legalidad o ilegalidad de la novedosa práctica gubernamental, este enfoque lo abordaré en el capítulo segundo.

3. ¿QUÉ ESTÁ EN JUEGO?

Algunos autores consideran que las TIC constituyen la tercera de las revoluciones científico-tecnológicas que modificaron los patrones de organización social,[21] y que esta se caracteriza por el desarrollo de tecnologías que permiten procesar, almacenar y transmitir gran cantidad de información en brevísimos lapsos.[22]

La tecnología no solo debe ser vista como solución, sino también como un instrumento que plantea nuevos desafíos a la protección de la privacidad y hay que abordarlos sin temor. Lo que

no podemos hacer es cobijarnos en el manto de la modernidad y dejar que todo fluya sin límites. No solo nuestra información personal está en juego, está en la mesa mucho más que eso, las nuevas tecnologías están modificando la forma en que se relacionan las personas y las reglas de comunicación e interacción social no solo entre los particulares, sino también entre los gobernantes y los gobernados. La legitimación y la confianza en las instituciones se replantean a partir de los nuevos retos que tenemos enfrente. No es algo que hay tomar a la ligera, ni de escapar de la modernidad o regresar a las señales de humo, hay que enfrentar el reto que se presenta y no huir de él. Nuestra privacidad e intimidad están siendo acotadas, amenazadas y modificadas en la forma en que las conocíamos. Ni las leyes ni la jurisprudencia ni nosotros mismos hemos dimensionado el nuevo y dinámico paradigma.

NUESTRA PRIVACIDAD E INTIMIDAD ESTÁN SIENDO ACOTADAS, AMENAZADAS Y MODIFICADAS EN LA FORMA EN QUE LAS CONOCÍAMOS. NI LAS LEYES NI LA JURISPRUDENCIA NI NOSOTROS MISMOS HEMOS DIMENSIONADO EL NUEVO Y DINÁMICO PARADIGMA

Desde luego que la tecnología trae grandes ventajas: nos permite comprar en línea sin tener que movernos de nuestra casa y evitar costos de intermediación; hacer engorrosos trámites gubernamentales y bancarios sin filas; comunicarnos e informarnos de manera más rápida, eficaz y económica; han surgido herramientas nuevas para combatir los delitos; mejorar la salud y la educación, entre otras muchas ventajas. Pero la tecnología también ha cambiado la democracia, ha acortado o, incluso, desaparecido jerarquías; dota a los ciudadanos de información para elegir a sus gobernantes o demandarles acciones de forma más enterada.

Desgraciadamente, las tecnologías también representan un riesgo: millones de cámaras visibles y ocultas que graban nuestros movimientos 24 horas al día los 365 días del año; nuestros propios celulares registran nuestras ubicaciones y hasta el número de pasos que damos al día; celulares ajenos captan nuestras conversaciones e imágenes privadas; internet registra y afina todos los días nuestro patrón de búsqueda; hay hackers dispuestos a revisar nuestra información y vaciar nuestra cuenta bancaria; venta de bases de datos supuestamente confidenciales donde nunca nos hubiésemos imaginado —recordar la venta del padrón electoral mexicano en Amazon—; funcionarios que amedrentan con exponer en video en vivo a sus ciudadanos ya no con un arma, sino con la cámara de su celular; todo esto enfrentamos con el riesgo de que en un segundo nuestra vida cambie precisamente por el uso indebido de nuestra información, de nuestra imagen. ¿Quién resguarda nuestra información? ¿Quién nos garantiza el respeto a nuestros derechos fundamentales?

El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

CAPÍTULO II

AUTORIDADES: ¿AMIGOS O ENEMIGOS DE LA PRIVACIDAD?

La privacidad ha muerto, supérenlo.
Scott McNealy, director general de Sun Microsystems, 1999.

EN ESTE CAPÍTULO EXPONGO BREVEMENTE CÓMO SE HA DESARROLLADO EL CONFLICTO ENTRE LOS CIUDADANOS EXHIBIDOS Y CUÁLES SON LAS RAZONES QUE HA DADO LA AUTORIDAD PARA JUSTIFICAR EL USO DE *PERISCOPE*. Posteriormente despliego un marco conceptual que funcionará como andamiaje para analizar si existe una legítima colisión de derechos entre la actuación de la autoridad y los derechos de los ciudadanos.

Algunas de las personas expuestas a través de *Periscope*, acudieron a la Comisión de Derechos Humanos del Distrito Federal (CDHDF) argumentando que se habían violado sus derechos fundamentales a la seguridad jurídica, a la honra y a la protección a la imagen. La Comisión respondió, entre otras cosas, lo siguiente:[23]

> [A] la CDHDF le preocupa que la utilización de herramientas tecnológicas como la citada aplicación *[Periscope*], exhiba a personas que hubieran realizado conductas que probablemente constituían una falta administrativa, sin que las autoridades observen las obligaciones que tienen en materia de protección de datos personales, al ser la imagen de una persona un dato personal que la hace identificable por sus rasgos físicos. Además, es necesario cumplir el principio de legalidad establecido en el artículo 16 de nuestra Constitución federal.
>
> … [S]i bien algunas de las conductas que se atribuyen a personas son socialmente reprochables y constituyen una infracción cuya sanción se encuentra debidamente establecida en la normatividad, (…) con la utilización de la aplicación Periscope se expone a las personas a quienes se exhibe, a una violencia innecesaria que se constituye en una sanción adicional no prevista en ninguna ley o normatividad, por lo que se vulneran derechos humanos.

En consecuencia con lo señalado, la Comisión solicitó medidas precautorias, como la cancelación de la publicidad de la imagen y los datos personales de las personas agraviadas, con la finalidad de evitar que fueran víctimas de violencia por las redes sociales, además de solicitar que en las acciones de las autoridades involucradas (*i.e.* la delegación Miguel Hidalgo) se respetaran los derechos de las personas, específicamente en lo relativo a la protección de datos personales.

Sobre la ponderación entre la protección de derechos y en respuesta al Boletín 031/2016 de la CDHDF, el funcionario de la delegación (Arne aus den Ruthen) cuestionó en la red social *Twitter,* a través de su cuenta,[24] la solicitud de la Comisión e intentó plantear un supuesto conflicto de derechos que merecía ponderación, con un afán de desacreditar las solicitudes de la CDHDF, al señalar:

> *Prioridades según la @CDHDF*
> *1. El "honor" del infractor o delincuente grabado en FLAGRANCIA*
> *2. Tus derechos*
> *3. El respeto a la ley*[25]

LO QUE INTERESA ANALIZAR ES SI EL USO DE TECNOLOGÍAS COMO *PERISCOPE* POR PARTE DE LAS AUTORIDADES, PUEDE VIOLENTAR LOS DERECHOS FUNDAMENTALES DE LOS INDIVIDUOS RELACIONADOS CON LA PRIVACIDAD O LA PROTECCIÓN A LOS DATOS PERSONALES

Por otro lado, en respuesta al citado boletín, la delegada de Miguel Hidalgo, mediante un comunicado transmitido de propia voz a través de *Periscope*, al que denominó "Boletín Electrónico",[26] argumentó que la delegación había puesto en marcha diversas medidas encaminadas a "ejercer" el principio de *máxima transparencia* en el ejercicio del servicio público y que la herramienta *Periscope* era empleada para *rendir cuentas* e *informar* del trabajo que realiza la delegación en tiempo real.

Además, agregó la delegada, *Periscope* nunca se empleaba [por los funcionarios] para denostar o exhibir a persona alguna ya que "no buscamos el escarnio público en contra de nadie" y señaló que "no aceptaba ningún tipo de censura de las redes sociales" para finalizar ratificando su "compromiso personal y sobre todo como servidora pública de respeto y defensa de los derechos humanos".[27]

En el mismo boletín, otro funcionario de la delegación de nombre Obdulio, argumentó que la difusión de la imagen de los infractores era acorde con la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal (LVPDF)[28] ya que su artículo 19 "señala que la imagen de una persona puede ser difundida sin su consentimiento cuando la reproducción se haga en relación a hechos y acontecimientos que tengan lugar en público" y que esa difusión es permisible cuando los hechos tienen lugar en público y son de interés público.[29]

De igual forma, se argumentó la aplicabilidad de la "eficacia horizontal de los derechos humanos", es decir, la posibilidad de que tales derechos sean violados por particulares, de forma que las autoridades están obligadas a evitar que las violaciones de derechos fundamentales, por ejemplo, a un ambiente sano, trasciendan de una manera irreparable, aunque no señaló cómo el uso de *Periscope* cumplía con ese objetivo. Otros argumentos del funcionario se referían: i) al derecho humano a la verdad y el uso de *Periscope* para su materialización; ii) la posible restricción a la libertad de expresión de la jefa delegacional y sus colaboradores como servidores públicos, y iii) al uso de Internet como derecho humano e instrumento de desarrollo.[30]

Hasta aquí la descripción de los argumentos de unos y otros en relación con una probable colisión de derechos por el uso de *Periscope* por parte de las autoridades. Ahora: ¿Cómo analizar estos argumentos? ¿Estamos realmente frente a una colisión de derechos? Aclaro, antes de entrar en este tema, que lo que está en análisis es el que la autoridad haya transmitido públicamente la imagen, voz y otros datos personales de los ciudadanos (en este caso por *Periscope*) y no así el hecho mismo del ejercicio de sus diversas facultades relacionadas con mantener el orden en la Ciudad de México, ni tampoco con la obligación que tienen las autoridades de transparentar sus actividades, lo que puede realizarse a través de diversas modalidades que no dañen otros derechos.

En este ensayo lo que interesa analizar es si el uso de tecnologías como *Periscope* por parte de las autoridades, puede violentar los derechos fundamentales de los individuos relacionados con la privacidad o la protección a los datos personales. Esto, claro, dependiendo de la forma en que se utilicen. Por ello sugiero a continuación un marco conceptual y jurídico que nos sirva de andamiaje semántico para el arribo a las conclusiones y elaboración de la propuesta que expongo al término de este ensayo.

En diversos análisis se parte de la base de que en la problemática planteada existe una colisión de derechos, ¿realmente es así? Esto se analizará posteriormente en el apartado "Colisión de derechos: ¿existe en el caso *Periscope*?", aunque independientemente de la conclusión a la que se llegue, no escapamos de revisar el marco jurídico del tema en el presente apartado.

1. MARCO CONCEPTUAL Y JURÍDICO

No es escaso el análisis que existe sobre el concepto de privacidad, intimidad, transparencia, derecho a la información, libertad de expresión, protección de datos personales, las fronteras de lo público frente a lo privado, y otras figu-

ras análogas. Quizás el mayor problema es que no existe una solución única al conflicto de colisión entre estos derechos sino que prácticamente todos los actores, incluyendo a la Suprema Corte de Justicia de la Nación (SCJN), concluyen que para declarar ganador a un derecho sobre otro casi siempre es menester hacer un análisis caso por caso y en la mayoría de las ocasiones la línea es muy delgada. ¿Hasta dónde llega el derecho a la información y hasta dónde el derecho a la privacidad o intimidad? ¿Dónde está el límite entre la transparencia y la protección de datos personales? ¿Cómo debe actuar la autoridad en caso de conflicto entre dos derechos? Ojalá hubiese una fórmula mágica que pudiéramos aplicar a todos los eventos y nos diera un resultado incuestionable; no es así, no hay reglas generales, sino quizá solo límites y principios orientadores ciertamente amplios que hay que ajustar casuísticamente. Procedo, pues, al análisis conceptual de los principales términos que se asocian a nuestra discusión.

¿HASTA DÓNDE LLEGA EL DERECHO A LA INFORMACIÓN Y HASTA DÓNDE EL DERECHO A LA PRIVACIDAD O INTIMIDAD? ¿DÓNDE ESTÁ EL LÍMITE ENTRE LA TRANSPARENCIA Y LA PROTECCIÓN DE DATOS PERSONALES? ¿CÓMO DEBE ACTUAR LA AUTORIDAD EN CASO DE CONFLICTO ENTRE DOS DERECHOS?

1.1 DERECHO A LA PRIVACIDAD

El derecho de los individuos a la privacidad, guarda una relación de género a especie con el de protección de datos personales y los derechos a la imagen y honra, es decir, no se puede violar el derecho a la protección de datos personales sin quebrantar simultáneamente el de privacidad. Sin embargo, en diversos ordenamientos y en la doctrina se mencionan de manera diferenciada. En el ámbito internacional, este derecho se encuentra plasmado en diversos tratados internacionales de los que México forma parte, los cuales reconocen que nadie podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación, además de que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.[31]

Por su parte, la Constitución Política de los Estados Unidos Mexicanos (CPEUM)[32] establece, precisamente en el contexto del derecho de acceso a la información contemplado en el Artículo 6º, que:

> *A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:*
>
> *I. …*
>
> *II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*[33]

Es decir, a partir de la redacción del texto constitucional se desprende que:

i) tanto el derecho a la privacidad como la protección de datos personales, son límites al derecho de acceso a la información, y ii) el ámbito de protección a que se refiere la CPEUM alude tanto a la vida privada, como a los datos personales, por lo que puede inferirse que, en realidad, se trata de dos ámbitos de protección distintos, con independencia de que pudiera existir una relación de género a especie entre ellos.[34]

En contraste con la concepción del derecho a la privacidad como límite al derecho de acceso a la información, la Comisión Interamericana de Derechos Humanos (CIDH) ha establecido claramente que las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público.[35]

Ni los textos legales internacionales ni los nacionales, aportan mayores elementos para definir el contorno y los alcances del derecho a la privacidad e incluso instituciones como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, por sus siglas en inglés) han asegurado que:

> La privacidad es un derecho fundamental, a pesar de que es difícil definir exactamente lo que implica ese derecho [y que] Se puede considerar que la privacidad tiene un doble aspecto: se refiere a qué información o lado de nuestras vidas podemos mantener en privado y también con la forma en la que terceras partes tratan la información que poseen (...) Privacidad en el mundo moderno tiene dos dimensiones – la primera, cuestiones que tienen que ver con la identidad de una persona y, la segunda, la forma en la que su información es tratada.[36]

En ese sentido, si acudimos a otras fuentes nacionales para buscar una respuesta sobre los alcances de este derecho en cuanto a lo que puede considerarse *privado* o lo que implica la *identidad de una persona*, observamos que la SCJN ha tratado como sinónimos a la privacidad y la intimidad, lo que se desprende de diversas tesis jurisprudenciales emitidas por ambas salas de nuestro máximo tribunal.[37]

Por otra parte, la privacidad, nos dice Ernesto Garzón Valdés, es el ámbito donde pueden imperar exclusivamente los deseos y preferencias individuales. Es condición necesaria del ejercicio de la libertad individual. Lo público está caracterizado por la libre accesibilidad de los comportamientos y decisiones de las personas en sociedad. Más aún: cuando ellas desempeñen algún cargo dotado de autoridad político–jurídica, la publicidad de sus actos se convierte en un derecho.[38]

1.2 DERECHO AL ACCESO A LA INFORMACIÓN

Constitucionalmente, el derecho a la información implica el libre acceso a información plural y oportuna, así como el derecho a buscar, recibir y difundir información e ideas de toda índole.[39]

Sobre este derecho, la SCJN ha señalado que tiene un doble carácter: i) como un derecho en sí mismo, y ii) como un instrumento para el ejercicio de otros derechos. De esta forma, el acceso a la información como garantía individual tiene por objeto maximizar la autonomía personal, posibilitando el ejercicio de la libertad de expresión en un contexto de mayor diversidad de datos, voces y opiniones, mientras que el derecho a la información como derecho colectivo, funcionalmente tiende a revelar el empleo instrumental de la información como mecanismo de control institucional.[40]

La segunda vertiente, es decir, el derecho a la información como derecho colectivo, es la que interesa para efectos de este análisis ya que, como se describió al inicio del presente capítulo, es la que se ha empleado para justificar el uso de *Periscope* en el actuar de la autoridad. Así, conviene recordar que algunos argumentos de los funcionarios de la delegación Miguel Hidalgo consistían en que la aplicación se empleaba para "rendir cuentas e informar del trabajo que realiza la delegación en tiempo real", *i.e.* como mecanismo de control institucional, además de argumentar el "derecho humano a la verdad y el uso de *Periscope* para su materialización", que claramente se traduce en un derecho colectivo "a saber".

Al respecto, debe subrayarse que la propia CPEUM establece en el Artículo 6º, una serie de principios y bases que deben observar tanto la Federación como las entidades federativas, entre los que se incluyen el principio de máxima publicidad en la interpretación del derecho y la obligación de las autoridades de documentar todo acto que derive del ejercicio de sus facultades. De igual forma, y como se describió en el concepto de privacidad, se establece entre los principios y bases de este derecho, que la información que se refiere a la vida privada y datos personales será protegida en los términos y con las excepciones que fijen las leyes.

Una definición más acabada y reciente de este derecho, aunque a nivel local, podemos encontrarla en la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (LTAIPRCCM), que define el derecho de acceso a la información pública como "la prerrogativa que tiene toda persona para acceder a la información generada, administrda o en poder de los sujetos obligados, en los términos de la presente Ley".[41]

Al respecto, Fernando Escalante explica que:

> … no toda la información del Estado puede hacerse pública, al menos no de inmediato (…) El derecho a la información delimita el polo de la transparencia, por llamarlo de algún modo. Hay la obligación de publicar esa información. En el extremo opuesto está la información personal, los datos sobre la vida privada de cualquier particular, protegidos rigurosamente por el derecho a la intimidad; por oposición, podríamos decir que es el polo de la opacidad, lo que no puede publicarse.[42]

1.3 TRANSPARENCIA

En cuanto a la transparencia, vale la pena destacar que este concepto encuentra una correlación estrecha con el derecho de acceso a la información y, aun cuando no encontramos en nuestro marco jurídico vigente una definición de lo que debe entenderse por "transparencia",[43] podemos decir que se trata de un principio que rige la actuación de los sujetos obligados conforme a la ley y que comprende a prácticamente todas las autoridades, entidades, órganos y organismos de los poderes públicos de los ámbitos federal, estatal y municipal, así como cualquier persona que reciba y ejerza recursos públicos o que realice actos de autoridad.[44]

Ahora bien, en relación con los elementos que conforman el principio de transparencia, el artículo 11 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) señala que toda la información en posesión de los sujetos obligados será: (i) pública; (ii) completa; (iii) oportuna; (iv) accesible; y (v) sujeta a un claro régimen de excepciones que deberán estar definidas y ser además legítimas y estrictamente necesarias en una sociedad democrática.

Por su parte, el artículo 13 de la misma ley, en lo relativo a la generación, publicación y entrega de la información, por parte de los sujetos obligados, señala que esta debe ser: (i) accesible; (ii) confiable; (iii) verificable; (iv) veraz; (v) oportuna, y (vi) debe atender las necesidades del derecho de acceso a la información de toda persona.

Es decir, conforme a nuestro marco jurídico, el principio de transparencia se materializará en la medida en la que toda la información en posesión de los sujetos obligados cumpla con los once elementos descritos en los párrafos anteriores o de forma que los satisfaga en la mayor medida posible.

Además, a propósito de la transparencia proactiva que deben observar los sujetos obligados,[45] la propia LGTAIP establece un marco de referencia relacionado con los objetivos de la política de transparencia, al señalar que:

> La información que se publique, como resultado de las políticas de transparencia, deberá permitir la *generación de conocimiento público* ***útil****, para disminuir asimetrías de la información, mejorar los accesos a trámites y servicios, optimizar la toma de decisiones de autoridades o ciudadanos y deberá tener un objeto claro enfocado en las necesidades de sectores de la sociedad determinados o determinables.*[46] [Énfasis añadido]

En ese sentido, es posible afirmar que las políticas de transparencia y, por tanto, cualquier acto emanado de algún sujeto obligado y que se realice con la finalidad de promover o garantizar la transparencia, debe ajustarse a los objetivos o fines descritos en los párrafos anteriores, incluyendo los fines de la transparencia proactiva. Dicho de otra forma, en caso de que la divulgación de información o los actos tendentes a facilitar el acceso a la misma, que realicen los sujetos obligados, no se ajuste a los fines y características determinadas por la propia ley, no podemos sostener entonces que tales actos encuadren en un objetivo o fin asociado a la política de transparencia y, como consecuencia, resultarán en mayor medida cuestionables o inútiles para tal objetivo, aunque puedan servir a otros.

1.4 DATOS PERSONALES Y DERECHOS ARCO

El Artículo 16 constitucional, en su segundo párrafo, dispone:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Para el presente análisis, es importante tener en cuenta que estamos ante el derecho a la protección de datos personales en el contexto de información obtenida o que se pueda obtener por las autoridades en el ejercicio de sus funciones.

Al respecto, a la fecha de elaboración del presente ensayo se encuentra en estudio en el Congreso de la Unión la ley que regulará precisamente este derecho y, por ello, es importante retomarla ya que otorga mayor claridad sobre sus alcances y objetivos últimos, y porque sus términos han sido aprobados al menos por una de las cámaras.

Así, el Dictamen con proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,[47] de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera de la Cámara de Senadores, establece en su artículo 3 lo siguiente:

> **IX. Se consideran datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.[48]

De igual forma, el artículo 6 del mismo ordenamiento dispone que:

> El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.
>
> El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional en términos de la Ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.[49]

Finalmente, vale la pena mencionar que en el plano internacional el Comité Jurídico Interamericano aprobó el 9 de marzo de 2012, una propuesta de principios de privacidad y protección de datos personales en las Américas,[50] que precisamente intenta armonizar los principios de libertad de expresión, libre flujo de información con los de privacidad y protección de datos personales. En dicho documento se establece una lista de doce principios básicos que deberían adoptarse y aplicarse en las leyes y prácticas nacionales de cada país, para evitar daños a las personas derivados de la obtención o uso incorrecto o innecesario de datos personales e información personal. Entre estos principios destacan los siguientes:

- *Propósitos legítimos y justos*. Los datos personales y la información personal deben ser recopilados únicamente para fines legítimos y por medios justos y legales (Principio Uno).
- *Claridad y consentimiento*. Se deben especificar los fines para los cuales se recopilan los datos personales y la información personal en el momento en que se recopilen. Como regla general, estos solo pueden ser recopilados con el conocimiento o consentimiento de la persona (Principio Dos).

- *Pertinencia y necesidad.* Los datos y la información deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación (Principio Tres).
- *Uso limitado y retención.* Los datos personales y la información deben mantenerse y utilizarse solamente de manera legítima no incompatible con el fin o fines para los cuales se recopilaron. No deben mantenerse más del tiempo necesario para su propósito y de conformidad con la legislación correspondiente (Principio Cuatro).
- *Deber de confidencialidad.* Los datos personales y la información personal no deben divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley (Principio Cinco).
- *Publicidad de las excepciones.* Cuando las autoridades nacionales establezcan excepciones a estos principios por motivos relacionados con la soberanía nacional, la seguridad interna o externa, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, deberían poner en conocimiento del público dichas excepciones (Principio Doce).[51]

Por su parte, los llamados derechos ARCO se refieren a la prerrogativa que otorga la ley a los titulares de los datos personales: acceso, rectificación y cancelación de su información personal en posesión de terceros, así como el derecho a oponerse a su uso.

El propio INAI ha desarrollado la *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO*[52], en la que puede leerse de manera muy sencilla en qué consiste cada uno de ellos:

> **Derecho de acceso:** Es el poder de disposición o decisión que tiene el titular sobre la información que le concierne, conlleva necesariamente el derecho de acceder y conocer si su información personal está siendo objeto de tratamiento, así como el alcance, condiciones y generalidades de dicho tratamiento.
>
> **Derecho de rectificación:** El responsable tiene la obligación de rectificar, a solicitud del titular, la información de este que resulte ser incompleta o inexacta.
>
> **Derecho de cancelación:** El titular tiene el derecho, en todo momento, a solicitar al responsable la cancelación (eliminación) de sus datos personales cuando considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la Ley. Esta cancelación implica la

supresión total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por el responsable, previo bloqueo.

Derecho de oposición: Es el derecho del titular de oponerse o solicitar el cese del tratamiento de su información personal al responsable cuando el tratamiento de datos personales ha sido llevado a cabo con pleno respeto a los principios básicos de protección de datos personales, sin embargo el titular cuenta con una razón legítima derivada de su propia situación personal para oponerse a que sus datos personales sigan siendo tratados para fines específicos, a fin de evitar un perjuicio al titular derivado de la persistencia en el tratamiento de la información que le concierne.

1.5 DERECHO A LA VIDA PRIVADA, EL HONOR Y LA PROPIA IMAGEN

La Convención Americana de Derechos Humanos (CADH) reconoce la protección de la honra y de la dignidad de la siguiente forma:

> Artículo 11. Protección de la Honra y de la Dignidad
> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Como se observa, para la CADH, la protección de la privacidad está comprendida como parte de la protección a la honra y dignidad de las personas aunque también comprende de manera específica el derecho al respeto a la honra y al reconocimiento de su dignidad.

A nivel local, la LVPDF que, como dijimos al inicio del presente capítulo, ha sido empleada por las autoridades para justificar la divulgación de información personal, tiene por finalidad regular el daño al patrimonio moral derivado del abuso del derecho de la información y de la libertad de expresión,[53] según la cual "la imagen es la reproducción identificable de los rasgos físicos de una persona sobre cualquier soporte material".[54]

Asimismo, esta ley señala que "toda persona tiene derecho sobre su imagen, que se traduce en la facultad para disponer de su apariencia autorizando, o no, la captación o difusión de la misma".[55] Por su parte, también se establece que constituirá acto ilíci-

to la difusión o comercialización de la imagen de una persona sin su consentimiento expreso.[56]

Por último, se dispone la excepción al principio de consentimiento expreso de la siguiente forma:

> La imagen de una persona no debe ser publicada, reproducida, expuesta o vendida en forma alguna si no es con su consentimiento, **a menos que** dicha reproducción esté justificada por la notoriedad de aquélla, por la función pública que desempeñe o cuando la reproducción se haga en relación con hechos, acontecimientos o ceremonias de interés público o que tengan lugar en público **y** sean de interés público.[57] [Énfasis añadido]

Sobre esta Ley, la Primera Sala de la SCJN[58] ha dicho que el segundo párrafo del artículo 1 delimita clara y precisamente su objeto: regular el daño al patrimonio moral derivado del abuso del derecho a la información y de la libertad de expresión.

1.6 DERECHO A LA NO DIVULGACIÓN

El derecho a la no divulgación de datos personales, cuando estos se encuentran en posesión de cualquier autoridad o sujeto obligado conforme a la LGTAIP, encuentra sustento en el artículo 68 de dicha ley que establece que los sujetos obligados serán responsables de los datos personales en su posesión y, entre otras acciones, deberán adoptar las medidas necesarias que eviten su alteración, pérdida, transmisión y acceso no autorizado. De forma más específica, el segundo párrafo del mismo artículo señala que los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo con la normatividad aplicable.[59]

1.7 DERECHO A LA LIBERTAD DE EXPRESIÓN

La Declaración Universal de Derechos Humanos, entre otros tratados internacionales, establece que la libertad de opinión y expresión incluye el derecho de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.[60]

Al respecto, el Tribunal en Pleno de la SCJN ha establecido que "el acceso a la información como garantía individual tiene por objeto maximizar el campo de la autonomía personal, posibilitando el ejercicio de la libertad de expresión en un contexto de mayor diversidad de datos, voces y opiniones".[61]

Es decir, en esta dimensión (como garantía individual), se conceptualiza el derecho a la información como un presupuesto de la libertad de expresión.

Por su parte, la Corte Interamericana de derechos Humanos (CoIDH), al referirse al artículo 13 de la CADH denominado "Libertad de Pensamiento y de Expresión", ha sostenido que:

> …el derecho protegido por el artículo 13 tiene un alcance y un carácter especiales. Se ponen así de manifiesto las dos dimensiones de la libertad de expresión. En efecto, **ésta requiere**, por un lado, que nadie sea arbitrariamente menoscabado o impedido de manifestar su propio pensamiento y representa, por tanto, un derecho de cada individuo; pero implica también, **por otro lado, un derecho colectivo a recibir cualquier información y a conocer la expresión del pensamiento ajeno**.[62] [Énfasis añadido]

1.8 SEGURIDAD JURÍDICA: *NULLA POENA SINE LEGE* [63]

Este principio, originalmente del derecho penal, se ha extendido al derecho administrativo. Significa que para que una conducta pueda ser calificada como ilícita, y por tanto sancionada, debe existir una norma o regulación dictada con anterioridad a la comisión de dicha conducta que establezca su ilicitud y además una sanción específica para tal conducta, que sea cierta y que no deje lugar a dudas o interpretación. Por lo tanto, si no existe un ordenamiento jurídico vigente al momento de que se cometa un acto, en el que se establezca que cierta conducta es ilícita y que señale qué sanción específica le corresponde, entonces no podría sancionarse a la persona que realizó la conducta.

1.9 PRESUNCIÓN DE INOCENCIA

Este principio se encuentra reconocido por diversos instrumentos de los que México forma parte y, esencialmente, se refiere a que toda persona acusada de algún delito tiene derecho a que se presuma su inocencia mientras no se establezca legalmente su culpabilidad.[64] En el marco constitucional se encuentra contemplado en el Artículo 20, apartado B, fracción I:

> B. De los derechos de toda persona imputada:
> I. A que se presuma su inocencia mientras no se declare su responsabilidad mediante sentencia emitida por el juez de la causa;

Por su parte, la jurisprudencia de la CoIDH ha señalado que este derecho implica que el acusado no debe demostrar que no ha cometido el delito que se le atribuye, ya que la prueba corresponde a quien acusa.[65] Es decir, bajo

este principio, hasta en tanto una persona no sea declarada culpable de un delito o una conducta administrativa, no podemos decir que lo sea y mucho menos las autoridades deben tratarla como culpable. Ahora bien, aunque originalmente este principio, como el señalado en el apartado anterior, había sido entendido como propio de la materia penal, la SCJN ha establecido que también debe aplicarse al derecho administrativo.[66]

1.10 PRINCIPIO DE LEGALIDAD

Este principio se les olvida muy frecuentemente a nuestras autoridades y es muy importante pues básicamente rige la relación gobernantes-gobernados. Las autoridades solo pueden hacer aquello que les está expresamente ordenado en las leyes, es decir, si hacen algo sin tener atribución o facultad establecida en la ley, entonces están actuando ilegalmente. Por el otro lado, los particulares podemos hacer todo aquello que no nos esté expresamente prohibido en las leyes, es el llamado principio de autonomía de la voluntad.[67]

LA IMAGEN, LA VOZ Y OTRAS CARACTERÍSTICAS FÍSICAS QUE PERMITEN IDENTIFICAR A UNA PERSONA, SON DATOS PERSONALES; EL ESTADO DEBE GARANTIZAR LA PRIVACIDAD Y TIENE EL DEBER DE PROTEGER DICHOS DATOS Y ÚNICAMENTE SE ACEPTAN LAS EXCEPCIONES QUE ESTABLECEN LAS LEYES

2. COLISIÓN DE DERECHOS ¿EXISTE EN EL CASO *PERISCOPE*?

No hay derechos absolutos. Todos los derechos tienen limitaciones porque coexisten con otros derechos con los que pueden entrar en conflicto. La determinación de cuál es el derecho que debe ser tutelado y cuál sacrificado, es un verdadero dolor de cabeza para las autoridades y los juzgadores, sobre todo cuando la línea es delgada.

Ahora bien, en el tema que nos ocupa ¿se actualiza una colisión de derechos o no la hay? ¿Qué derechos se están ejerciendo? ¿Quiénes son sus titulares? Tuve un profesor de derecho laboral que nos repitió hasta el cansancio que "para que haya caldo de liebre, primero tiene que haber liebre"; aplicando esto al caso concreto: para que haya colisión de derechos, primero tiene que haber derechos. Una vez comprobado que existen derechos, de ser el caso, y cuáles son estos, entonces podemos entrar a revisar si existe colisión, de lo contrario no podríamos hablar de conflicto alguno.

Como analicé en el marco conceptual y jurídico, la imagen, la voz y otras características físicas que permiten identificar a una persona, son datos personales; el Estado debe garantizar la privacidad y tiene el deber de proteger dichos datos y únicamente se aceptan las excepciones que establecen las leyes, las cuales solo pueden estar basadas en razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Por lo anterior, si una autoridad divulga datos personales sin consentimiento de su titular o sin sustento en

una excepción establecida en ley, vulnera el derecho que tienen los particulares de su protección. Así, como explico en párrafos posteriores, en el caso de análisis referente a *Periscope*, no existe excepción en ley aplicable al caso concreto que les permita hacerlo.

Por lo que hace al derecho al honor (honra) y la propia imagen, la pretendida excepción para la divulgación de la imagen que utiliza la autoridad delegacional en sus argumentos defensivos basada en que se trata de hechos de interés público, es una interpretación equivocada de la LVPDF, pues aun cuando en ella se establece, en el artículo 19, que "la imagen de una persona no debe ser publicada, reproducida, expuesta o vendida en forma alguna si no es con su consentimiento, a menos que dicha reproducción… se haga en relación con hechos, acontecimientos o ceremonias de interés público o que tengan lugar en público y sean de interés público", lo cierto es que esta ley no es aplicable a los actos de autoridad porque su objeto claramente establece que "**tiene por finalidad regular el daño al patrimonio moral derivado del abuso del derecho de la información y de la libertad de expresión**".[68] [Énfasis añadido] Las autoridades en el ejercicio de sus funciones no tienen derechos humanos, así que la autoridad delegacional no es destinataria de esta norma y por tanto no aplica al caso concreto.[69] No hay, pues, en nuestro marco jurídico vigente, normatividad que establezca excepción alguna que faculte a la autoridad a divulgar la imagen de un particular sin su consentimiento por la comisión de una infracción administrativa.

Más aún, la SCJN ha establecido que todas las autoridades se encuentran obligadas a cumplir con las normas que ordenan garantizar los derechos humanos. El deber de respeto supone obligaciones negativas, es decir, que las autoridades no perpetren violación de derechos humanos; por su parte, el deber de garantía presupone obligaciones positivas, que implica que las autoridades tomen todas las medidas apropiadas para proteger y preservar los derechos humanos reconocidos a través del Artículo 1º constitucional. Dentro del deber de garantía se encuentran los aspectos de prevención, protección, investigación y reparación.[70]

Se violentan también el derecho de presunción de inocencia y el de seguridad jurídica, al exhibir sin su previo consentimiento como responsables a los individuos e imponiéndoles una sanción que no está establecida en nuestro marco jurídico: el escarnio público y la divulgación de sus datos personales.

Por lo que hace a la transparencia, derecho a la información y libertad de expresión, las autoridades, como dije, no tienen derechos humanos, es decir,

no es válido argumentar que estas se encuentran ejerciendo derechos al obtener la información y divulgar el momento en que se capta la comisión de una infracción. Diferente es cuestionarnos si la divulgación en tiempo real de los videos, satisface el acceso a la información y la transparencia de todos los particulares. En este derecho, al igual que en el de libertad de expresión en su parte pasiva de recibir opiniones e información, los individuos pueden conocer lo que los sujetos obligados realizan en el ejercicio de sus atribuciones, como sería en el caso concreto, el mantener o poner orden en la Ciudad de México, pero eso no significa que para ello sea necesaria ni proporcional la medida tomada por las autoridades consistente en divulgar los datos personales de los infractores, suponiendo que ese fuera el objetivo. Es más, la exhibición de las imágenes ni siquiera ha sido consecuencia de una solicitud de información, sino una iniciativa espontánea de las autoridades con lo que, además, están violentando el principio de legalidad debido a que no hay norma que los autorice a hacerlo y, por el contrario, sí hay diversos preceptos que les presentan esta carga negativa que mencionamos de no violentar los derechos humanos máxime que, como se dijo, el tercer párrafo de la CPEUM impone a todas las autoridades el deber de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.[71]

LAS AUTORIDADES EN EL HECHO MISMO DE TRANSMITIR EN TIEMPO REAL LAS IMÁGENES DE LOS CIUDADANOS INFRACTORES NO ESTÁN EJERCIENDO UN DERECHO, PORQUE LAS AUTORIDADES NO TIENEN DERECHOS, NI UNA ATRIBUCIÓN, PORQUE NO HAY LEY QUE LOS MANDATE, MUCHO MENOS TIENEN OBLIGACIÓN ALGUNA DE HACERLO

De lo anterior se concluye, entonces, que las autoridades en el hecho mismo de transmitir en tiempo real las imágenes de los ciudadanos infractores no están ejerciendo un derecho, porque las autoridades no tienen derechos, ni una atribución, porque no hay ley que los mandate, mucho menos tienen obligación alguna de hacerlo.

Por lo que hace a la posible colisión entre los derechos de privacidad, protección de datos personales y a la propia imagen frente a los derechos de información, transparencia y libertad de expresión , existen una serie de técnicas y principios que pueden servir para llegar a una solución, en caso de que se sostenga que existe tal conflicto. Sin embargo, en mi opinión, aquí tampoco estamos frente a una colisión porque es la autoridad quien está cometiendo la conducta —ilícita— de divulgación de la imagen de los ciudadanos y no cuenta con atribución específica para hacerlo, incluso tiene prohibición expresa; luego entonces, afirmar que la conducta de las autoridades consistente en divulgar datos personales sin que le asista una atribución, permite ejercer un derecho a los particulares, es un contrasentido, pues no podemos reconocer efectos jurídicos a un acto ilícito.

Olga Sánchez Cordero, cuando era ministra de la SCJN, señaló:

> … no puede soslayarse que el Estado, como sujeto informativo que genera información, que tiene el carácter de pública, y supone, por lo tanto, el interés de los miembros de la sociedad por conocerla, se encuentra obligado a comunicar a los gobernados sus actividades y éstos tienen el derecho correlativo de tener acceso libre y oportuno a esa información, con las limitantes que para fines prácticos se pueden agrupar en tres tipos: limitaciones en razón del interés nacional e internacional, limitaciones por intereses sociales y limitaciones para protección de la persona. Tales limitaciones o excepciones al derecho a la información, de suyo implican que no se trata de un derecho absoluto, y por tanto, debe entenderse que **la finalidad de éstas es la de evitar que este derecho entre en conflicto con otro tipo de derechos**, con los que puede colisionar, como comúnmente ocurre con los relativos a la intimidad o vida privada.[72]
> [Énfasis añadido]

3. ALGUNOS PRINCIPIOS PARA ANALIZAR LA COLISIÓN DE DERECHOS

Tanto para los casos específicos de pretendida colisión que se han analizado, como en general para la probable colisión de otros derechos humanos, la literatura, la legislación y la práctica jurisdiccional, tanto nacional como internacional, han generado algunos exámenes o principios cuyo empleo puede llevarnos a una interpretación en materia de derechos humanos, más adecuada del texto constitucional.

Uno de los principios se refiere a la *expectativa razonable de privacidad*. ¿Tiene una expectativa razonable de privacidad alguien que sale al parque con su perro y no levanta sus desechos? ¿Puede esperarse una diferencia en el tratamiento del material grabado por un particular frente a lo grabado por una autoridad? La expectativa razonable de privacidad consiste en un *test* o examen que se ha desarrollado principalmente en el derecho anglosajón, para que los tribunales puedan determinar el alcance del derecho a la privacidad en casos que involucran una posible colisión entre este derecho y la libertad de expresión. Se refiere mayormente al balance del derecho a la privacidad con la libertad de expresión y todos los casos de referencia tienen que ver con la divulgación de información de un particular en ejercicio de la libertad de expresión por parte de otro particular que acude al Poder Judicial a reclamar su derecho a la privacidad, por lo tanto es aplicado *a posteriori*, es decir, cuando se

analiza una probable violación al derecho a la privacidad que ya tuvo lugar.

No obstante, para el objeto de análisis de este ensayo, de considerar que sí existe una colisión de derechos, bien podrían emplearse diversos elementos desarrollados por instancias extranjeras, que permitan llegar a principios orientadores y criterios sobre el balance de este derecho en relación con el derecho de acceso a la información que, como he señalado, ha sido la principal justificación para realizar intromisiones de autoridades y divulgar información de los particulares.

Otro principio es el llamado principio tripartito (idoneidad, necesidad y proporcionalidad), que está *orientado* a resolver conflictos entre derechos, intereses o valores entre sí. La ventaja del enfoque de proporcionalidad es que permite decidir esos conflictos sin necesidad de generar jerarquías en abstracto de los derechos, intereses o valores involucrados y, por tanto, sin necesidad de prejuzgar su mayor o menor legitimidad, ni producir prohibiciones absolutas.[73]

Para efectos de este análisis, es necesario destacar que el principio de proporcionalidad se realiza una vez que los derechos o intereses entraron en conflicto y este produce "soluciones ajustadas al caso" sin prejuzgar sobre casos futuros en los que los mismos derechos o intereses entren en conflicto.[74] Esto dificultaría su aplicación como criterio de elaboración de normas generales, especialmente si estas buscan recoger conductas que involucran el uso de TIC que, por naturaleza, son dinámicas y se multiplican exponencialmente, lo que podría llevar al diseño y aplicación de las normas.

No obstante, en mi opinión, emplear la aplicación de un principio como el de proporcionalidad antes de que surjan los conflictos para la definición de criterios generales no solo es posible, sino conveniente, debido a que permitiría prescindir del uso de medidas intrusivas en muchos casos que, por ejemplo, puedan resolverse objetivamente mediante la aplicación de los subprincipios de idoneidad y necesidad. Adicionalmente, sería un buen ejercicio para conocer la motivación de la medida adoptada (transmitir en *Periscope* a un ciudadano infractor), así como los resultados buscados.

Por otra parte, también se ha reconocido que, a pesar de tratarse de un principio que no ofrece soluciones generales aplicables a todos los casos, esto pudiera lograrse en la medida en la que las circunstancias sean las mismas.[75]

Así, los criterios que se pudieran desarrollar, acompañados de una intensiva y constante capacitación de los funcionarios que empleen las TIC en el cumplimiento de sus facultades, conforme al principio de máxima publicidad en observancia al derecho de acceso a la in-

formación, podría llevar a una práctica que se ajuste más a los principios constitucionales en juego que, no debe olvidarse, derivan de derechos humanos.

Por último, tenemos la denominada "prueba de interés público", la cual debe ser aplicada por el sujeto obligado que corresponda cuando se pretenda exentar la obligación de obtener el consentimiento del titular de la información confidencial para permitir el acceso a ella, cuando se requiera su publicación por razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros. Para aplicar dicha exención, como dije, la propia ley exige que el sujeto obligado aplique esta prueba de interés público. El artículo 149 de LGTAIP establece que los organismos garantes también deberán aplicar la prueba de interés público al resolver los recursos de revisión que se interpongan. Resulta interesante que, a diferencia del mandato del artículo 120, fracción IV, descrito anteriormente, en este caso (artículo 149) se especifica que la prueba de interés público debe realizarse con base en "elementos de idoneidad, necesidad y proporcionalidad", *i.e.* conforme al principio de proporcionalidad y define cada uno de estos elementos:

> **Artículo 149.** El organismo garante, al resolver el recurso de revisión, deberá aplicar una prueba de interés público con base en elementos de idoneidad, necesidad y proporcionalidad, cuando exista una colisión de derechos.
> Para estos efectos, se entenderá por:
> I. **Idoneidad:** La legitimidad del derecho adoptado como preferente, que sea el adecuado para el logro de un fin constitucionalmente válido o apto para conseguir el fin pretendido;
> II. **Necesidad:** La falta de un medio alternativo menos lesivo a la apertura de la información, para satisfacer el interés público, y
> III. **Proporcionalidad**: El equilibrio entre perjuicio y beneficio a favor del interés público, a fin de que la decisión tomada represente un beneficio mayor al perjuicio que podría causar a la población.

En ese sentido, es posible afirmar que conforme al artículo 149 citado, la prueba de interés público que deben aplicar los organismos garantes en realidad se traduce en la aplicación del principio de proporcionalidad mencionado en párrafos anteriores.

4. OBJETIVOS DE LA DIVULGACIÓN DE IMÁGENES EN TIEMPO REAL (VÍA *PERISCOPE*): ¿JUSTIFICAN LA VIOLACIÓN DE LA PRIVACIDAD?

Saldré por un momento del ámbito estrictamente jurídico. ¿Qué beneficio conlleva la exposición de la imagen detallada y en

tiempo real de los infractores? ¿Cuáles podrían ser los objetivos que se pretende perseguir con el uso de *Periscope* en las diligencias que hace la autoridad delegacional, tomando en cuenta lo argumentado por estas?:

1. Ser transparente y mostrar sus acciones en un afán de rendición de cuentas.
2. La obtención de elementos probatorios de las infracciones cometidas.
3. Combatir la violación de derechos humanos por otros particulares.
4. Ejercitar la libertad de expresión de las autoridades.
5. Disuadir conductas indebidas de otros ciudadanos, a través de la exhibición y escarnio público.

Ya analicé en párrafos anteriores que la transparencia, la rendición de cuentas, la información, la máxima publicidad y el ejercicio de la supuesta libertad de expresión de las autoridades, no son justificación para divulgar los datos personales de los individuos. Ahora bien, si la captación y obtención de la información (videos) por parte de las autoridades tuvieran como finalidad alguno de los cuatro objetivos arriba listados, ¿por qué y para qué exponer la imagen de los ciudadanos? Esto no es necesario para obtener los fines planteados, pues lo mismo se lograría al transmitir los videos omitiendo la imagen y voz de las personas y así evitar el daño causado. La autoridad no tiene obligación ni atribución de transmitir sus actos cuando estos involucran a particulares, sin hacer una valoración previa de los daños que se pueden causar.

LA TRANSPARENCIA, LA RENDICIÓN DE CUENTAS, LA INFORMACIÓN, LA MÁXIMA PUBLICIDAD Y EL EJERCICIO DE LA SUPUESTA LIBERTAD DE EXPRESIÓN DE LAS AUTORIDADES, NO SON JUSTIFICACIÓN PARA DIVULGAR LOS DATOS PERSONALES DE LOS INDIVIDUOS

Los videos no son información que ya se encontraba en los archivos y que, por lo tanto, bajo el principio de máxima publicidad, se ha decidido publicar. Imaginemos por un momento que en lugar de transmitir los videos en vivo se hubiesen guardado como prueba y que un particular, en ejercicio de su derecho a la información, solicite por transparencia dichos videos. Bien, pues en ese caso la autoridad tendría la obligación de "editar" la información ahí contenida para crear una versión pública de dicho documento videograbado, tal y como sucede en una sentencia del Poder Judicial o en una resolución administrativa.

Así, desde hace varios años, distintos órganos que forman parte tanto de la SCJN como del Consejo de la Judicatura Federal han establecido, mediante diversas disposiciones, criterios conforme a los cuales en las versiones públicas de expedientes y sentencias, debe suprimirse cierta información, con la finalidad de dar cumplimiento al marco normativo en materia de transparencia, acceso a la información y protección de datos personales.[76]

Dichos criterios han dado lugar a una práctica común, consistente en suprimir y, en su caso, sustituir, *inter alia*, los nombres, alias, seudónimos o cualquier otra denominación que identifique o haga identificable a una persona, los números, letras o caracteres que conformen alguna clave vinculada a una persona (por ejemplo, RFC, CURP), así como las características físicas e intelectuales descriptivas de las personas (por ejemplo, color de piel, estatura, peso, edad, complexión).

Es decir, el Poder Judicial Federal ha considerado que, como regla general, esta información corresponde a la categoría de "datos personales" y, por tanto, se trata de: (i) información confidencial y (ii) su difusión requiere el consentimiento de los individuos.

De hecho, fue precisamente a partir de la Reforma Constitucional al Artículo 6º,[77] por medio de la cual se elevó a rango constitucional la protección de la vida privada y de los datos personales, que la SCJN decidió modificar el "Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental", debido a que con anterioridad a dicha reforma, el criterio adoptado era que no debían suprimirse los nombres de las partes en las versiones públicas de las determinaciones dictadas en un juicio seguido ante la SCJN, los tribunales de Circuito y los juzgados de Distrito.

Lo anterior obedecía, entre otras consideraciones manifestadas por el Pleno de la SCJN, a que: "en términos de lo previsto en el párrafo último del artículo 18 de la referida Ley Federal se considera como pública la información que se ubique en fuentes de acceso público".[78] Sin embargo, este criterio se modificó con la finalidad de "lograr su plena adecuación a la reforma constitucional antes referida", es decir, la reforma al Artículo 6º constitucional.

Al respecto, vale la pena retomar el contenido del considerando cuarto de las reformas al citado Reglamento:

> **CUARTO**. Por su naturaleza la información contenida en las resoluciones y en las demás constancias que obran en los expedientes judiciales se relaciona generalmente con la vida privada de las partes, incluso con su intimidad, ámbito que por mandato constitucional y conforme a lo previsto en el artículo 11 de la Convención Americana sobre Derechos Humanos, requiere de especial tutela constitucional, tal como lo reconoció la Primera Sala de la Suprema Corte de Justicia de la Nación al resolver el veintitrés de mayo de dos mil siete, el amparo directo en revisión

402/2007, por lo que *se estima conveniente establecer una regulación que,* **por regla general**, *proteja los datos personales de las partes en un juicio, incluyendo su nombre, máxime que esta información por lo regular es innecesaria para conocer y dar seguimiento al criterio de los juzgadores y al contenido de las resoluciones.* [Énfasis añadido]

En ese sentido, las reformas mencionadas tuvieron, al menos, cinco consecuencias relevantes para efectos de nuestro análisis, que se traducen en las siguientes normas:

> (i) En las resoluciones públicas **que se difundan por medios electrónicos en todos los casos se suprimirán los nombres** de las partes;[79]
> (ii) **En todo caso**, de las sentencias ejecutorias y las demás resoluciones así como de las constancias que obren en el expediente, **se suprimirán los datos sensibles** que puedan contener, procurando que la supresión no impida conocer el criterio sostenido por el respectivo órgano jurisdiccional;[80]
> (iii) En caso de que las partes ejerzan, en cualquier instancia seguida ante la Suprema Corte, el Consejo o los Órganos Jurisdiccionales, el **derecho de oposición** a la publicación de sus datos personales, **cuando se presente una solicitud de acceso** a alguna de las resoluciones públicas o a las pruebas y demás constancias que obren en el expediente respectivo, se generará la versión pública de las resoluciones requeridas **suprimiendo el nombre de las partes así como cualquier otra información de carácter personal** que contengan, procurando que la referida supresión no impida conocer el criterio sostenido por el respectivo órgano jurisdiccional;[81]
> (iv) Las determinaciones adoptadas en relación con la supresión de datos personales de las partes también **podrán impugnarse por el solicitante** mediante el recurso de revisión previsto en este Reglamento, y[82]
> (v) Todo interesado tiene derecho a que se le informe **de manera expresa y oportuna sobre la posibilidad de** ejercer los derechos de acceso, de rectificación y de cancelación de los datos personales que le conciernan así como de **oponerse a su publicación.**[83]
> [Énfasis añadido]

Lo anterior fue posteriormente detallado por los órganos de transparencia de la propia Corte y aunque el análisis de cada instrumento normativo emitido escapa al objeto de estudio del presente

ensayo, vale la pena retomar algunos criterios de supresión de datos personales que adoptó el Comité de Acceso a la Información y de Protección de Datos Personales para las versiones públicas de las sentencias dictadas por el Pleno y las salas de la SCJN. Entre los datos susceptibles de supresión consideró los nombres, alias, seudónimos o cualquier otro sobrenombre de las partes, entre otros involucrados, así como los datos sensibles relacionados con la intimidad, entre los que se encuentran *las características físicas* como tipo de sangre, ADN, huella digital, *color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, origen racial*. Es decir, mediante diversos instrumentos en la SCJN se adoptaron criterios de protección de datos personales que, conforme a su evolución, se traducen en:

- Por regla general, los nombres de las partes no son susceptibles de divulgación, cuando esta se realice por medios electrónicos.
- En ningún caso, los datos sensibles de las personas son susceptibles de divulgación.
- El análisis sobre la posibilidad de divulgar constitucionalmente esta información, en todo caso, debe realizarse de manera previa a su divulgación.
- El titular de los datos debe ser informado, de forma oportuna, sobre la posibilidad de oponerse a la publicación de sus datos personales.

Al respecto, por lógica elemental, la oportunidad señalada en el último punto, en todo caso se debe dar con anterioridad a la divulgación de la información. Siguiendo dicha lógica, que en mi opinión es adecuada, tenemos entonces que distinguir el momento en el que podría darse la colisión de derechos y, en su caso, qué elementos deben acudir para hablar de una verdadera colisión.

En ese sentido, es claro que, como regla general, no existe un derecho de acceso a los datos personales que se actualice de forma automática cuando se transfiere información de un particular a la autoridad, sino que, por el contrario, el particular posee en todo momento el derecho a que sus datos sean resguardados y, excepcionalmente, se divulguen, previo aviso al que debe recaer una notificación, lo que no sucede en el caso de *Periscope*.

Dicho de otra forma, siguiendo el criterio de la Corte, no puede afirmarse que exista en nuestro marco jurídico un derecho colectivo a conocer los nombres de las personas, su domicilio, sus características físicas, su ideología, simplemente por el hecho de que esa persona ha formado o forma parte de un procedimiento seguido ante autoridades. De hecho, por principio constitucional esa información debe tratarse

con el carácter de confidencial y solo en el supuesto de que se obtenga el consentimiento, se podrían divulgar algunos aspectos de ella.

Es decir, existe una presunción de que esa información forma parte de los datos que las personas no desean compartir, tanto es así que el propio marco jurídico dispone que solo en los casos en los que se obtenga el consentimiento de esa persona, la información podrá difundirse.

Sin embargo, esto no debe quedar al arbitrio de la autoridad porque no le corresponde a esta detonar una colisión de derechos unilateralmente, bajo pretexto de respetar el derecho de otro particular o de la colectividad, sino que debe buscar proteger ambos y, únicamente en caso de que alguno de ellos se cuestione por restringir otro, entonces le corresponderá realizar un análisis o ponderación que le permita concluir que la restricción de uno es estrictamente necesaria para el cumplimiento del otro.

A LA AUTORIDAD NO LE ASISTE NINGÚN PRECEPTO JURÍDICO QUE LE PERMITA DIVULGAR INFORMACIÓN COMO SE HIZO CON *PERISCOPE*, ANTES AL CONTRARIO, ENTRAÑA UNA VIOLACIÓN JURÍDICA POR LO QUE NO CABE HABLAR DE COLISIÓN [DE DERECHOS] ALGUNA

De hacerlo, es decir, en caso de que la autoridad decida anular sin razonamiento alguno, de forma unilateral, irreparable y sin que medie un mínimo ejercicio de ponderación o la exigencia jurídica de hacerlo, entonces estamos ante una franca violación de derechos humanos, en este caso a la privacidad, y no ante una colisión que, en todo caso, se presentaría en un momento posterior y no al momento mismo de la violación gestada por la propia autoridad.

Por otra parte, es claro que los datos se transfieran, voluntaria o involuntariamente, a las autoridades, no hace que muten de naturaleza por ese solo hecho. Esto es, la colisión de derechos no tiene lugar en el momento en que una autoridad recaba los datos personales de los particulares, ya que no puede aceptarse válidamente (legalmente) en ese momento, que como colectividad tenemos un derecho a conocer la identidad de la persona o que se convierte en información pública, por ello, la presunción es que se trata de información confidencial en todos los casos.

Esto queda claro si analizamos el artículo 116 de la LGTAIP, en relación con el 111 y el 106 de la misma ley:

> Artículo 116. Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.
> La información confidencial no estará sujeta a temporalidad alguna y **solo podrán tener acceso a ella** los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello…
> Artículo 111. *Cuando un Documento contenga partes o secciones reservadas o confidenciales*, los sujetos obligados,

para efectos de atender una solicitud de información, deberán elaborar una Versión Pública *en la que se testen las partes o secciones clasificadas*, indicando su contenido de manera genérica y fundando y motivando su clasificación.

Artículo 106. La clasificación de la información se llevará a cabo en el momento en que:

I. …
II. …
III. Se generen versiones públicas para dar cumplimiento a las obligaciones de transparencia previstas en esta Ley. [Énfasis añadido]

De la transcripción realizada, queda claro que las autoridades, siempre que se encuentren frente a información confidencial, deben reservarla y hacer un ejercicio de clasificación al momento de generar la versión pública de lo contenido en la información reservada. Lo dicho, no hay colisión alguna tratándose de información confidencial.

Como se observa, existe un marco conceptual jurídico muy vasto sobre el tema pero no hay reglas absolutas que permitan dilucidar un posible conflicto de derechos. Sin embargo, como apunté en este capítulo, no se puede establecer tal conflicto si no existen derechos en colisión. En el caso que analizo, como demostré, a la autoridad no le asiste ningún precepto jurídico que le permita divulgar información como se hizo con *Periscope*, antes al contrario, entraña una violación jurídica por lo que no cabe hablar de colisión alguna.

El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

CAPÍTULO III

TECNOLOGÍAS EN MANOS DEL GOBIERNO: ¿ARMA O HERRAMIENTA?

LAS RELACIONES GOBERNANTES-GOBERNADOS ESTÁN EN CONSTANTE CAMBIO DEBIDO A LAS TIC Y LAS REDES SOCIALES. La horizontalidad, la interacción y comunicación están transformando la forma de administrar y eso es relevante, no hay que pasarlo por alto, es necesario documentarlo y ordenarlo. Desde luego que las tecnologías son una estupenda herramienta de información, comunicación, capacitación, medición, de combate a la inseguridad, de monitoreo, entre otras muchas bondades, pero todos sabemos que las tecnologías también pueden generar ciertos problemas en los mismos rubros mencionados, así que la pregunta es: ¿deben las administraciones públicas regular el uso que hagan sus funcionarios de las tecnologías y redes sociales? Yo sostengo que sí, en tanto las usen ostentándose como funcionarios.

Lo anterior por el sistema restrictivo que envuelve a las autoridades y que está compuesto por tres elementos: i) los gobernantes en su actuación, como se revisó en el capítulo anterior, no tienen derechos humanos; ii) limita su ámbito de actuación el principio de legalidad que los obliga a circunscribir sus acciones solo a aquello que les está expresamente atribuido en las leyes, y iii) tienen la obligación negativa y positiva de respetar los derechos humanos.

Así, es indispensable capacitar a los empleados y funcionarios de las diferentes instancias gubernamentales sobre cómo usar las tecnologías y aplicaciones (redes sociales), pero también sobre cuáles son sus límites de actuación. La realidad es que las limitaciones que tienen en su campo jurídico las tendrán también al usar las redes y tecnologías, el problema es que no todos tienen claro cuáles son aquellas. Bien, pues la capacitación, la emisión de un manual de uso de tecnologías y redes sociales, el desarrollo de una estrategia global común en la administración pública, así como la conformación de un área o comité en las dependencias y organismos al que pudieran acudir los propios empleados en caso de duda, pudieran ser de mucha utilidad. No hay que confundir regulación con miedo,

las tecnologías y aplicaciones son para usarse y tienen muchísimas ventajas, el tema es que en ocasiones no se saben utilizar. En varios países y ciudades ya se han expedido manuales de uso.

El Reino Unido, por ejemplo, establece en su *Guía de Medios Sociales para Servidores Públicos*[84] (*Social media guidance for civil servants: October 2014*) que deben guardar cierto comportamiento tanto en su uso como funcionarios como en privado, dado que pueden prestarse a confusión ambos papeles. De hecho, la misma guía incluye otra guía llamada *Libro de Uso de Medios Sociales* (*Social Media Play Book*),[85] en la que se recuerda a los servidores públicos el cumplimiento de las leyes, especialmente las de privacidad en el caso de *Periscope* y *Meerkat*, en el sentido de solicitar el permiso de las personas que aparezcan en los videos.

MÉXICO DEBE ENTRAR AL TEMA [LAS TIC Y LAS REDES SOCIALES] DE MANERA GENERAL Y NO CASUÍSTICAMENTE, LOS CONFLICTOS EN EL USO DE LAS REDES SOCIALES Y EN LAS NUEVAS APLICACIONES Y ESCENARIOS QUE VENDRÁN, SEGUIRÁN MULTIPLICÁNDOSE. NO ES CONVENIENTE ADOPTAR TECNOLOGÍAS SIN CONSTRUIR SUS FRONTERAS

Un texto que vale la pena hojear es la *Guía de Usos y Estilo en las Redes Sociales de la Junta de Castilla y León,* España,[86] que ya va por su cuarta edición y está destinada a ayudar y orientar a todos aquellos centros directivos de la Junta de Castilla y León sobre la mejor manera de utilizar las redes sociales en sus relaciones con los ciudadanos, en ella se establece de manera llamativa y gráfica desde qué son las redes y cómo usarlas, hasta qué hacer y qué no hacer. En el apartado de *Periscope*, señalan lo siguiente:

> Aunque generar, producir y compartir un vídeo se ha facilitado mucho gracias a las nuevas tecnologías y aplicaciones (Instagram, Vine, Periscope, etc.), debemos tener en cuenta algunas cuestiones mínimas de calidad para que esta publicación no genere una mala reputación:
>
> - Es recomendable que esté grabado y/o emitido en horizontal.
> - Si va a contener audio, debemos asegurarnos que se escucha correctamente.
> - Debe estar iluminado convenientemente.
> - Si incluye banda sonora, debemos asegurarnos que tenemos los permisos pertinentes para su reproducción.
> - **Asegurarnos que las personas que salen en el mismo han dado el consentimiento para el uso de su imagen.** [Énfasis añadido]

En México, el gobierno del Estado de México expidió en 2010 un manual de políticas y lineamientos para el uso de redes sociales,[87] un documento muy rudimentario que más bien refleja la falta de conocimiento del tema y el miedo a cambiar la perspectiva de comunicación, así como la actitud, lo que se entiende un poco más considerando que se elaboró hace seis años; por ejemplo, la

página 11 señala que si existe duda respecto de qué publicar, mejor no publicar.

El caso de Nueva Zelanda resulta muy interesante. Han desarrollado un sitio llamado *Conjunto de Herramientas para el Gobierno de Nueva Zelanda*,[88] (*New Zealand Government Web Toolkit*), que provee guía, estándares y algunos consejos estratégicos para usar la red de manera efectiva, aunque no específicamente las redes sociales, sí contiene límites en materia de privacidad. Tiene varios temas desarrollados, lo interesante es que no solo aconseja al propio gobierno sino también a los particulares.

Así, México debe entrar al tema de manera general y no casuísticamente, los conflictos en el uso de las redes sociales y en las nuevas aplicaciones y escenarios que vendrán, seguirán multiplicándose. No es conveniente adoptar tecnologías sin construir sus fronteras. Por ejemplo, en el caso de la videovigilancia que traté en el primer capítulo, aun con las legislaciones que se han expedido, no se responden todas las preguntas cruciales sobre el tema: ¿Quién puede ver las grabaciones? ¿Cómo prevenir un mal uso o abuso de su contenido? ¿Cómo impedir el acceso por personas no autorizadas? ¿Cuánto tiempo deben ser guardadas? ¿Cuáles son los procedimientos correctos?

Hay que hacer las preguntas y construir las respuestas en un entorno de legalidad, apertura y respeto a los derechos humanos. México está muy rezagado en este tema y mientras más tiempo pase, más conflictos teóricos y reales se presentarán.

CONCLUSIONES Y PROPUESTA

1. El uso de las tecnologías de la información y la comunicación (incluyendo redes sociales) está cambiando las relaciones entre particulares, pero también entre gobernantes y gobernados. Aunque en el ámbito mundial encontramos escenarios de prueba-error, lo que no significa que no deba existir un orden y ciertos límites, los retos que se presentan deben de ser abordados desde un estándar mínimo que dé cumplimiento a los derechos fundamentales. Un sujeto que se siente observado, nunca se sentirá libre.

2. La práctica de transmitir videos en tiempo real por parte de algunos funcionarios de la Ciudad de México, en los que exponen las imágenes, voz y otros datos personales de ciudadanos infractores, ha despertado el debate sobre la ética y legalidad de esta acción. Muchas personas simpatizan irracionalmente con la idea de que se exhiba públicamente al infractor. A primera vista, esto puede parecer una buena solución al mal comportamiento, al desprecio que tienen algunos a las leyes, a la civilidad, así como a la falta de confianza a la autoridad, pero este linchamiento puede tener consecuencias preocupantes.

3. Esta problemática debe ser estudiada integralmente desde un enfoque multidisciplinario, siendo el psicológico uno de los análisis más importantes; el punto de vista jurídico es limitado y solo nos ofrece una solución formal y no de fondo. El que la autoridad considere que requiere exponer a los ciudadanos —cuya privacidad debe proteger— para ser obedecida, tiene causas y efectos que deben ser estudiados desde diferentes áreas. Las consecuencias del escarnio público en una persona, familia o grupo social, no deben subestimarse.

4. Las autoridades únicamente pueden hacer aquello que les está expresamente conferido en las leyes, no pueden crear su propio sistema de actuación al margen o en contra de la ley, esto es

violatorio de los principios de legalidad y seguridad jurídica.

5. Las autoridades —todas— tienen obligación de respetar los derechos fundamentales de los individuos, pero también deben hacer lo posible, dentro de sus atribuciones, para que se respeten por terceros; la violación a la ley que perpetre un individuo no justifica, en el caso que nos ocupa, la transgresión de sus derechos fundamentales.

6. No existe ningún precepto legal expreso que faculte u ordene a la autoridad transmitir públicamente la imagen de ciudadanos que cometen infracciones a las leyes.

7. La transmisión que haga la autoridad de la imagen de un ciudadano como infractor sin su consentimiento, viola sus derechos fundamentales, específicamente el derecho al resguardo de sus datos personales, el derecho a la propia imagen, ambos encuadrados en el derecho a la privacidad, así como los de seguridad jurídica y presunción de inocencia.

8. Adicionalmente, esta práctica no permite a la autoridad hacer una valoración *ex ante* sobre si existe una causa de excepción que permita la divulgación de los datos personales, lo que conlleva a un daño irreparable que entraña una sanción en sí misma —el escarnio público—no prevista, hasta el día de hoy, en ninguna norma.

9. Las autoridades, en el ejercicio de sus funciones, no tienen derechos. Por tanto, es incorrecta la defensa relativa a que la transmisión en tiempo real de las imágenes se realiza en ejercicio de su derecho a la libertad de expresión.

10. El pretendido conflicto entre el supuesto derecho a la libertad de expresión (de las autoridades) y el de privacidad (de los particulares exhibidos) no es tal, puesto que para que exista colisión de derechos, debe haber al menos dos derechos que se confronten, y en este caso no los hay.

11. Respecto de los derechos *erga omnes* a la transparencia, a la información y de libertad de expresión en su vertiente pasiva, la divulgación de la imagen de los ciudadanos sin previa valoración ni consentimiento, tampoco concibe una colisión de derechos puesto que al ser ilícita la difusión, dicha situación no puede tener efectos jurídicos y menos actualizar un derecho en otra persona que supuestamente pudiera verse beneficiada (directa o indirectamente) del acto ilícito.

12. Aun si se llegase a la conclusión de que es positiva la práctica de que las autoridades exhiban la imagen y otros datos personales de los infractores, a fin de desincentivar el mal comportamiento, bajo el actual marco jurídico no es posible hacerlo, habría que reformarlo y tener este método en

observación para comprobar que el balance costo-beneficio es adecuado para continuar implementándolo.

13. Distinto resulta si se transmitieran los videos sin divulgar ningún dato personal de los individuos (incluyendo la voz), o bien si se grabaran sin publicarse y solo para efectos de contar con un elemento probatorio en el procedimiento que corresponda. En tal caso, no podríamos hablar de una violación a los derechos fundamentales.

14. Las tecnologías pueden y deben ser utilizadas por los funcionarios públicos, pero para ello es importante capacitarlos a fin de que se aproveche su potencial y, sobre todo, para que conozcan sus atribuciones y restricciones en los distintos ámbitos, así como los problemas específicos que pueden presentarse al usar las tecnologías y redes sociales.

15. Es necesario que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales especifique, a la brevedad, el estándar mínimo de derechos que deben ser respetados por parte de las autoridades en el uso de tecnologías y redes sociales.

16. Resulta conveniente que se diseñen lineamientos o guías que incluyan límites positivos y negativos de lo que las autoridades deben y pueden hacer con las tecnologías, incluyendo redes sociales. Esto debe hacerse de forma democrática e incluyente a través de foros y consultas, escuchando a la gente que desee participar, convocando a la academia, la industria, a los gobiernos federal, estatales y municipales, así como incorporando experiencias internacionales.

REFERENCIAS

El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

[1] Foucault, Michel, (2002). *Vigilar y castigar, nacimiento de la prisión*, Siglo XXI Editores, p.11.

[2] Monsiváis, Carlos, (2004). "Que esta vez sí detengan a Fuenteovejuna", *Proceso*, 1465, pp. 6-11.

[3] Rojas Bravo, Gustavo, (2009). "Apuntes sobre linchamiento y la construcción social del miedo", *Tramas, Subjetividad y procesos sociales,* UAM-X, 30, pp. 135-158, cita a Le Bon, Gustave (1895, 1995), *Psicología de las masas*, Editorial Morata, Madrid, Tercera edición.

[4] Utilizaremos el ejemplo de la aplicación *Periscope* de transmisión en vivo porque fue la utilizada en el caso que nos ocupa y así ha sido identificada la práctica, pero podría ser otra distinta y aplican las mismas consideraciones.

[5] https://help.periscope.tv/customer/en/portal/articles/2016126-what-is-periscope- (Consulta realizada el 1 de julio de 2016).

[6] Shontell, A. (2016). *What it's like to sell your startup for ~$120 million before it's even launched: Meet Twitter's new prized possession, Periscope*. Business Insider. [En línea]. Disponible en: http://uk.businessinsider.com/what-is-periscope-and-why-twitter-bought-it-2015-3 (Consultado el 21 diciembre de 2016).

[7] Citado por Albrecht, Katherin y Mcintyre, Liz, (2006). *Chips espías: Cómo las grandes corporaciones y el gobierno planean monitorear cada uno de sus pasos con RFID,* Grupo Nelson, p. 1.

[8] Nissenbaum, Helen, (2004). *Privacy as contextual integrity*. Washington Law Review Association.

[9] De acuerdo con Christensson, Per. *Streaming Definition.* TechTerms. (2006). http://techterms.com/definition/streaming (consultado el 1 de julio de 2016), el término *streaming* o *data streaming,* se refiere a la posibilidad de reproducir un archivo multimedia sin necesidad de descargarlo completamente primero. El *streaming* se encuentra comúnmente asociado a audio y/o video. Con una conexión a internet rápida, incluso se puede transmitir desde y hacia un dispositivo audio y video en vivo vía *streaming* (*live streaming*). De hecho, esto último es precisamente lo que aplicaciones como *Periscope* permiten: transmitir y recibir audio y video en vivo.

[10] Tarun Wadwa, The Next Privacy Battle: Cameras That Judge Your Every Move, *Forbes*, 30 de agosto de 2012 http://www.forbes.com/sites/singularity/2012/08/30/dear-republicans-beware-big-brother-is-watching-you/#4d-5359947cec (Consultado el 26 de octubre de 2016).

[11] Ullmann-Margalit, E., *The case of the camera in the kitchen: Surveillance, privacy, sanctions, and governance. Regulation & Governance*, 2008, 2(4): pp. 425-444.

[12] https://www.rt.com/usa/snowden-obama-whistleblower-protection-101/ (Consultado el 12 de julio de 2016).

[13] Keenan, Thomas P., (2015). *Tecno siniestro. El lado oscuro de la red: la rendición de la privacidad y la capitalización de la intimidad,* Melusina, p. 299.

[14] Como la Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México, publicada en la *Gaceta Oficial* el 14 de mayo de 2014.

[15] http://www.cndh.org.mx/sites/all/doc/Recomendaciones/generales/RecGral_021.pdf

[16] Ver el blog de www.hectorguzmanmx.wordpress.com sobre el tema (Consultado el 2 de junio de 2016).

[17] http://www.bbc.com/mundo/noticias/2015/08/150814_tecnologia_periscope_ventajas_riesgos_lv

[18] Renunció temporalmente al cargo el 22 de junio de 2016.

[19] Este cargo tiene bajo su responsabilidad las direcciones ejecutivas de Servicios Urbanos, Obras Públicas, Desarrollo Social, así como de Modernización Administrativa, Prevención del Delito, Coordinación de Gestión e Indicadores y la operación de Protección Civil. Fue aprobado mediante el Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Reglamento Interior de la Administración Pública del Distrito Federal, publicado en la *Gaceta Oficial de la Ciudad de México* el 15 de enero de 2016, artículo 171.

[20] *Gandalla* es un mexicanismo para señalar a alguien abusivo.

[21] La primera revolución de este tipo es la llamada "Revolución Industrial", a partir del surgimiento de la máquina de vapor en el siglo XVIII, mientras que la segunda surge a inicios del siglo XX caracterizada por la organización de las industrias a partir de la línea de montaje, para la producción masiva de productos en serie.

[22] Pedregal, Nicolás y Tarasow, Fabio, (2005). *Tecnologías de la Información y la Comunicación,* Stella, p. 30.

[23] Boletín de prensa de la CDHDF 031/2016 del 23 de febrero de 2016. Disponible en http://cdhdfbeta.cdhdf.org.mx/wp-content/uploads/2016/02/boletin0312016.pdf

[24] @arnemx

[25] https://twitter.com/arnemx/status/702482879989702656

[26] Se puede consultar en: https://www.youtube.com/watch?v=mEUcXiawSaI (Consultado el 19 de julio de 2016).

[27] *Ídem.*

[28] Publicada en la *Gaceta Oficial del Distrito Federal* el 19 de mayo de 2006.

[29] https://www.youtube.com/watch?v=mEUcXiawSaI (Consultado el 19 de julio de 2016).

[30] *Ídem.*

[31] Así lo establecen los artículos 17 del Pacto Internacional de Derechos Civiles y Políticos, 11 de la Convención Americana sobre Derechos Humanos, 12 de la Declaración Universal de Derechos Humanos, así como el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre.

[32] Publicada en el *Diario Oficial de la Federación* el 5 de febrero de 1917, última reforma el 25 de julio de 2016.

[33] Artículo 6, Apartado A, fracción II de la CPEUM.

[34] De hecho, posteriormente el Artículo 16 de la propia CPEUM, separó nuevamente los dos ámbitos de protección al señalar, por una parte, que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento, protección que se acerca a la definición del derecho a la privacidad contenida en los textos de instrumentos internacionales, y por otra parte, al establecer que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

[35] Declaración de Principios sobre la Libertad de Expresión. Adoptada por la CIDH en su 108° período ordinario de sesiones celebrado del 2 al 20 octubre de 2000.

[36] UNESCO, (2012). *Global Survey on Internet Privacy and Freedom of Expression*. P. 7, 9 (traducción propia del texto en inglés).

[37] Al respecto, basta la lectura de rubros de Tesis Aisladas como la siguiente: Derecho a la Privacidad o Intimidad. Está protegido por el Artículo 16, Primer Párrafo, de la Constitución Política de los Estados Unidos Mexicanos (Segunda Sala).

[38] Garzón Valdés, Ernesto, (2015). *Lo íntimo, lo privado y lo público*. *Cuaderno de Transparencia* Núm. 6. México, INAI.

[39] Artículo 6, segundo párrafo, de la CPEUM.

[40] Tesis: P./J. 54/2008. Acceso a la Información. Su naturaleza como garantías individual y social. SCJN, Pleno. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVII, junio de 2008.

[41] Artículo 6, fracción XIII de la LTAIPRCCM.

[42] Escalante, Fernando, (2015). *El derecho a la privacidad*. *Cuaderno de Transparencia* Núm. 2, pp. 38 y 39.

[43] A pesar de que el artículo 8, fracción IX, de la LGTAIP establece una definición de *transparencia*, esta se restringe a la obligación de "los organismos garantes del derecho de acceso a la información" de regir su funcionamiento conforme a este principio, por lo que no podemos decir que sea una definición aplicable a todos los sujetos obligados ni podemos decir que esta sea la definición que adopta nuestro marco jurídico y, por lo tanto, se afirma que no existe una definición del concepto de transparencia en nuestro marco jurídico.

[44] Artículo 23 de la LGTAIP.

[45] Al respecto, el artículo 45, fracción IX, de la LGTAIP, establece que las Unidades de Transparencia de los Sujetos Obligados deben promover e implementar políticas de transparencia proactiva procurando su accesibilidad.

[46] Artículo 58 de la LGTAIP.

[47] Dictamen aprobado por la Cámara de Senadores el 28 de abril de 2016, fue turnado a la Comisión de Transparencia y Anticorrupción de la Cámara de Diputados y publicado en la *Gaceta* el 3 de mayo de 2016, pendiente de discusión y aprobación (Nota del Editor: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se publicó el 26 de enero de 2017 en el *Diario Oficial de la Federación*, esto es, en fecha posterior a la elaboración de este *Cuaderno de Transparencia.* Sin embargo, las notas hechas por la autora corresponden a pie juntillas a esa publicación oficial).

[48] *Ídem.*

[49] *Ídem.*

[50] http://www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf

[51] *Ídem.*

[52] http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf (Consultado el 31 de octubre de 2016).

[53] Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal. Artículo 1, segundo párrafo.

[54] *Ibídem,* artículo 16.

[55] *Ibídem,* artículo 17.

[56] *Ibídem,* artículo 18.

[57] *Ibídem,* artículo 19.

[58] *Semanario Judicial de la Federación y su Gaceta*. Libro XIII, octubre de 2012, Tomo 2, p. 732.

[59] Artículo 68, fracción VI y segundo párrafo de la LGTAIP.

[60] Artículo 19 de la Declaración Universal de Derechos Humanos.

[61] Tesis: P./J. 54/2008. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVII, junio de 2008, Novena Época, p. 743.

[62] Corte Interamericana de Derechos Humanos. Opinión Consultiva OC-5/85 del 13 de noviembre de 1985.

[63] Frase del latín que se traduce como "no hay pena sin ley".

[64] Así lo establecen, por ejemplo, la Convención Americana sobre Derechos Humanos (artículo 8.2), la Declaración Universal de los Derechos Humanos (artículo 11.1), y el Pacto Internacional de Derechos Civiles y Políticos (artículo 14).

[65] Jurisprudencia surgida del caso Ricardo Canese vs Paraguay. Citada por la SCJN en la Sentencia relativa a la Contradicción de Tesis 200/2013, párr. 80.

[66] Definida por el propio Pleno de la SCJN al resolver la Contradicción de Tesis 200/2013 como: "el conjunto de actos o formalidades concatenados entre sí en forma de juicio por autoridad competente, con el objeto de conocer irregularidades o faltas ya sean de servidores públicos o particulares, cuya finalidad, en todo caso, sea imponer alguna sanción". *Ibídem,* párr. 45.

[67] Se excluyen los casos de actividades reguladas y que, por tanto, requieren de la expedición de un título habilitante como una concesión.

[68] Artículo 1, segundo párrafo, de la LVPDF.

[69] Al respecto, basta señalar que existe jurisprudencia que niega la procedencia del juicio de amparo por parte de las autoridades (Tesis. XV.2o. J/6), o bien, tesis que establecen expresamente que cuando los actos del Estado son en ejercicio de poder, o sea, que obra en calidad de autoridad, actuando sin el concurso de la voluntad del gobernado, y tales actos son sometidos al examen de legalidad por parte de autoridades de instancia, en caso de que aquellos sean declarados ilegales, la autoridad no puede acudir al juicio de garantías, pues ya se dijo que este no fue instituido a favor de las autoridades sino de los gobernados (Tesis: X.3o.19 K).

[70] Derechos Humanos. Todas las autoridades están obligadas a cumplir con las obligaciones de respeto y garantía. Primera Sala, tesis aislada, registro 2010422. Libro 24, noviembre de 2015, Tomo I. Tesis 1ª. CCCXL/2015 (10ª) p. 971.

[71] Artículo 1, tercer párrafo, de la CPEUM.

[72] https://www.scjn.gob.mx/conocelacorte/ministra/conferencia20111025.pdf (Consultado el 10 de julio de 2016).

[73] Roca, E. y Ahumada, M. *Los Principios de Razonabilidad y Proporcionalidad en la Jurisprudencia Constitucional Española*. Octubre, 2013. p. 3. http://www.tribunalconstitucional.es/es/actividades/Documents/XV%20Trilateral/PONENCIA.pdf (Consultado el 10 de julio de 2016).

[74] Roca, E. y Ahumada. *Op. Cit*. 78.

[75] *Loc. Cit*.

[76] Ver, por ejemplo: (i) Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (conforme a su reforma publicada en DOF el 12/12/2007); (ii) "Acuerdo general de la Comisión para la Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales de la Suprema Corte de Justicia de la Nación, del nueve de julio de dos mil ocho, relativo a los órganos y procedimientos para tutelar en el ámbito de este Tribunal los derechos de acceso a la información, a la privacidad y a la protección de datos personales garantizados en el artículo 6o. constitucional" (DOF 15/07/2008); (ii) Recomendaciones para la Supresión de Datos Personales en las sentencias dictadas por el Pleno y las Salas de este Alto Tribunal (Aprobadas por el Comité de Acceso a la Información y de Protección de Datos Personales. 11/03/2009).

[77] Publicada en el *Diario Oficial de la Federación* el 20 de julio de 2007.

[78] Reformas al Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Publicado en el *Diario Oficial de la Federación* el 12 de diciembre de 2007.

[79] *Ibídem*, artículo 9.

[80] *Ibídem*, artículo 8, tercer párrafo.

[81] *Ibídem*, artículo 8, primer párrafo.

[82] *Ibídem*, artículo 8 *in fine*.

[83] *Ibídem*, artículo 33.

[84] https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants#propriety-and-ethics (Consultado el 1 de agosto de 2016).

[85] https://gdsengagement.blog.gov.uk/playbook/#brief-twitter (Consultado el 1 de agosto de 2016).

[86] http://www.jcyl.es/junta/cp/guia_usos_redes_sociales_jcyl.pdf (Consultado el 20 de junio de 2016).

[87] http://salud.edomexico.gob.mx/html/Otros/POLITICAS%20Y%20LINEAMIENTOS%20PARA%20EL%20USO%20DE%20REDES%20SOCIALES.PDF (Consultado el 1 de agosto de 2016).

[88] https://webtoolkit.govt.nz/ (Consultado el 1 de agosto de 2016).

BIBLIOGRAFÍA

El ejercicio de la función pública: una perspectiva desde las nuevas tecnologías, la transparencia y los derechos humanos

- Albrecht, Katherin y Mcintyre, Liz, (2006). *Chips espías: Cómo las grandes corporaciones y el gobierno planean monitorear cada uno de sus pasos con RFID*, Grupo Nelson.
- Alexy, Robert. Constitutional rights and proportionality. https://revus.revues.org/2783#tocto2n2 (Consultado 12 de julio 2016).
- Barendt, Eric, (2016). A reasonable expectation of privacy' a coherent or redundant concept? En *Comparative Defamation and Privacy Law* Cambridge.
- Cervantes, Pere y Tauste, Oliver, (2016). *Internet Negro, el lado oscuro de la red*. Paidós.
- Escalante, Fernando, (2015). *El derecho a la privacidad. Cuaderno de Transparencia* Núm. 2.
- Fernández Rodríguez, José Julio, (2004). *Lo público y lo privado en Internet*. UNAM Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica, Núm. 154.
- Foucault, Michel, (2002). *Vigilar y castigar, nacimiento de la prisión*, Siglo XXI Editores.
- Garzón Valdés, Ernesto, (2015). *Lo íntimo, lo privado y lo público*, (INAI), *Cuaderno de Transparencia* Núm. 6.
- Gómez Marinero, Carlos Martin *et al*., (2016). El acceso a la videograbación de audiencias en el nuevo proceso penal. Comentario de la resolución IVAI-REV/976/2013/II. Estudios en Derecho a la Información enero-junio de 2016. 1: 89-102.
- Keenan, Thomas P., (2015). *Tecno Siniestro. El lado oscuro de la Red: la rendición de la privacidad y la capitalización de la intimidad*, Melusina.
- Mattelart, Armand y Vitalis, André, (2015). *De Orwell al cibercontrol*, Gedisa.

- Monsiváis, Carlos, (2004). "Que esta vez sí detengan a Fuenteovejuna", *Proceso*, 1465, pp. 6-11.

- Nissenbaum, Helen, (2004) *Privacy as contextual integrity. Washington Law Review Association.*

- Pedregal, Nicolás y Tarasow, Fabio, (2005). *Tecnologías de la Información y la Comunicación*, Stella.

- Perello Domenech, Isabel, (1994). *Derecho Administrativo Sancionador. Jueces para la democracia*. 22:76-81. Consultado en https://dialnet.unirioja.es/servlet/articulo?codigo=2552535

- Rojas Bravo, Gustavo, (2009). "Apuntes sobre linchamiento y la construcción social del miedo", *Tramas* UAM-X, 30, pp. 135-158.

- Sánchez Cordero de García Villegas, Olga, (2010). "Conferencias de los Ministros de la Suprema Corte de Justicia de la Nación". Vida privada del personaje público. Privacidad y cambio de identidad, participación de la ministra Olga Sánchez Cordero en el Seminario de Acceso a la información judicial 2009 que tuvo lugar en el área de murales del edificio sede de la SCJN el 26 de noviembre de 2009, (SCJN).

- Ullmann-Margalit, E., (2008) *The case of the camera in the kitchen: Surveillance, privacy, sanctions, and governance*. Regulation & Governance.

- UNESCO, (2012). *Global Survey on Internert Privacy and Freedom of Expression.* (traducción propia del texto en inglés)

Legislación y Tratados

- Constitución Política de los Estados Unidos Mexicanos. Publicada en el *Diario Oficial de la Federación* el 5 de febrero de 1917 (última reforma publicada en el DOF el 25 de julio de 2016).

- Convención Americana sobre Derechos Humanos. Suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (B-32) San José, Costa Rica, 7 al 22 de noviembre de 1969.

- Declaración Americana de los Derechos y Deberes del Hombre. Aprobada en la Novena Conferencia Internacional Americana en Bogotá, Colombia, 1948.

- Declaración de Principios sobre la Libertad de Expresión. Adoptada por la CIDH en su 108° período ordinario de sesiones celebrado del 2 al 20 octubre de 2000.

- Declaración Universal de los Derechos Humanos. Adoptada y proclamada por la Resolución de la Asamblea General de la ONU, 217 A (III) del 10 de diciembre de 1948.

- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México. Publicada en la *Gaceta Oficial de la Ciudad de México* el 6 de mayo de 2016.

- Ley Federal de Transparencia y Acceso a la Información Pública. Publicada en el *Diario Oficial de la Federación* el 9 de mayo de 2016.

- Ley General de Transparencia y Acceso a la Información Pública. Publicada en el *Diario Oficial de la Federación* el 4 de mayo de 2015.

- Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal. *Gaceta Oficial del Distrito Federal*, 19 de mayo de 2006 (última reforma publicada en *Gaceta* el 28 de noviembre de 2014).

- Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México. *Gaceta del Gobierno*, Estado de México, 14 de mayo de 2014.

- Pacto Internacional de Derechos Civiles y Políticos. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de la ONU, en su resolución 2200 A (XXI), de 16 de diciembre de 1966.

- Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Publicado en el *Diario Oficial de la Federación* del viernes 2 de abril de 2004 (conforme a su reforma publicada en DOF el 12 de diciembre de 2007).

- Reglamento Interior de la Administración Pública del Distrito Federal. *Gaceta Oficial del Distrito Federal*, 28 de diciembre del 2000 (última reforma publicada en *Gaceta* el 16 de junio de 2016).

Sitios Web

- http://www.hectorguzmanmx.wordpress.com sobre el tema (Consultado el 2 de junio de 2016).

- http://techterms.com/definition/streaming (Consultado el 1 de julio de 2016).

- https://www.rt.com/usa/snowden-obama-whistleblower-protection-101/ (Consultado el 12 de julio de 2016).

- http://www.cndh.org.mx/sites/all/doc/Recomendaciones/generales/RecGral_021.pdf (Consultado el 2 de julio de 2016).

- https://help.periscope.tv/customer/en/portal/articles/2016126-what-is-periscope- (Consultado el 1 de julio de 2016).

- http://uk.businessinsider.com/what-is-periscope-and-why-twitter-bought-it-2015-3 (Consultado el 2 de julio de 2016).
- http://www.bbc.com/mundo/noticias/2015/08/150814_tecnologia_periscope_ventajas_riesgos_lv (Consultado el 3 de julio de 2016).
- https://www.youtube.com/watch?v=mEUcXiawSaI (Consultado el 19 de julio de 2016).
- http://www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf (Consultado el 12 de julio de 2016).
- https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants#propriety-and-ethics (Consultado el 1 de agosto de 2016).
- https://www.scjn.gob.mx/conocelacorte/ministra/conferencia20111025.pdf (Consultado el 10 de julio de 2016).
- https://gdsengagement.blog.gov.uk/playbook/#brief-twitter (Consultado el 1 de agosto de 2016).
- http://www.jcyl.es/junta/cp/guia_usos_redes_sociales_jcyl.pdf (Consultado el 20 de junio de 2016).
- http://salud.edomexico.gob.mx/html/Otros/POLITICAS%20Y%20LINEAMIENTOS%20PARA%20EL%20USO%20DE%20REDES%20SOCIALES.PDF (Consultado el 1 de agosto de 2016).
- https://webtoolkit.govt.nz/ (Consultado el 1 de agosto de 2016).
- http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf (Consultado el 31 de octubre de 2016).
- BBC Mundo. (2016). *Ventajas y desventajas de Periscope, la app que logró 10 millones de usuarios en 4 meses - BBC Mundo*. [En línea]. Disponible en: http://www.bbc.com/mundo/noticias/2015/08/150814_tecnologia_periscope_ventajas_riesgos_lv (Consultado el 21 diciembre de 2016).

- Guzmán, H. (2016). *Capacitación y principio de responsabilidad. Cuidando el eslabón más débil. Dato Data Int.* [En línea]. Disponible en: http://www.hectorguzmanmx.wordpress.com (Consultado el 2 de junio de 2016).

- Christensson, P. (2006). *Streaming Definition.* [En línea]. de: http://techterms.com (Consultado el 1 de julio de 2016).

- Comisión Nacional de los Derechos Humanos (2014). Recomendación general Núm. 21, sobre la prevención, atención y sanción de casos de violencia sexual en contra de las niñas y los niños en centros educativos. [En línea]. De: http://www.cndh.org.mx/sites/all/doc/Recomendaciones/generales/RecGral_021.pdf (Consultado el 2 de julio de 2016).

- Periscope. (2016). *What is Periscope?* [En línea]. Disponible en: https://help.periscope.tv/customer/en/portal/articles/2016126-what-is-periscope (Consultado el 21 diciembre de 2016).

- Roca, E. y Ahumada, M. (Octubre, 2013). *Los Principios de Razonabilidad y Proporcionalidad en la Jurisprudencia Constitucional Española.* [En línea] p. 3. https://www.tribunalconstitucional.es/ActividadesDocumentos/2013-10-24-00-00/2013-PonenciaEspa%C3%B1a.pdf (Consultado el 10 de julio de 2016).

- RT International (2014). Snowden Q&A: Indiscriminate mass surveillance is the biggest problem we face. [En línea]. De: https://www.rt.com/usa/snowden-obama-whistleblower-protection-101/ (Consultado el 12 de julio de 2016).

- Shontell, A. (2016). *What it's like to sell your startup for ~$120 million before it's even launched: Meet Twitter's new prized possession, Periscope.* Business Insider. [En línea]. Disponible en: http://uk.businessinsider.com/what-is-periscope-and-why-twitter-bought-it-2015-3 (Consultado el 21 diciembre de 2016).

- Tarun Wadwa, The Next Privacy Battle: Cameras That Judge Your Every Move, *Forbes*, 30 de agosto de 2012. [En línea]. Disponible en http://www.forbes.com/sites/singularity/2012/08/30/dear-republicans-beware-big-brother-is-watching-you/#4d5359947cec (Consultado el 26 de octubre de 2016).
- YouTube. (2016). *Nosotros no exhibimos a nadie, se exhiben solos.* [En línea]. Disponible en: https://www.youtube.com/watch?v=mEUcXiawSaI (Consultado el 21 diciembre de 2016).
- Comité Jurídico Interamericano. Propuesta de Declaración de principios de privacidad y protección de datos personales en las Américas. [En línea]. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf (s/f)
- Gobierno del Reino Unido (2016). *Social media guidance for civil servants: October 2014 - GOV.UK.* [En línea]. Disponible en: https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants/social-media-guidance-for-civil-servants#propriety-and-ethics (Consultado el 21 diciembre de 2016).
- Gobierno del Reino Unido (2016). *Social Media Playbook*. [En línea]. Disponible en: https://gdsengagement.blog.gov.uk/playbook/#brief-twitter (Consultado el 21 diciembre de 2016).
- Junta de Castilla y León (s.f.) *Guía de usos y estilo en las redes sociales*. [En línea]. Disponible en: http://www.jcyl.es/junta/cp/guia_usos_redes_sociales_jcyl.pdf (Consultado el 21 diciembre de 2016).
- Gobierno del Estado de México (2010). *Políticas y lineamientos para el uso de redes sociales*. [En línea]. Disponible en : http://salud.edomexico.gob.mx/html/Otros/POLITICAS%20Y%20LINEAMIENTOS%20PARA%20EL%20USO%20DE%20REDES%20SOCIALES.PDF [Consultado el 21 diciembre de 2016].
- Gobierno de Nueva Zelanda (2016). *New Zealand Government Web Toolkit*. [En línea]. Disponible en: https://webtoolkit.govt.nz/ (Consultado el 21 diciembre de 2016).

El ejercicio de la función pública: una perspectiva
desde las nuevas tecnologías,
la transparencia y los derechos humanos,
Primera edición electrónica en PDF, octubre de 2017.
Edición a cargo de:
Dirección General de Promoción y Vinculación con la Sociedad,
Dirección General de Comunicación Social y Difusión.
Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Delegación Coyoacán, Ciudad de México, C. P. 04530.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Delegación Coyoacán, Ciudad de México, C.P. 04530.
Primera edición electrónica en PDF, octubre de 2017.