

EMPLEO DE LAS REDES SOCIODIGITALES POR LAS INSTITUCIONES DE EDUCACIÓN PÚBLICA: PROBLEMAS Y SOLUCIONES JURÍDICAS

USE OF SOCIAL MEDIA BY PUBLIC EDUCATION INSTITUTIONS: PROBLEMS AND LEGAL SOLUTIONS



Lorena PICHARDO FLORES*

RESUMEN. Cuando las instituciones de educación pública abren y gestionan redes sociodigitales, el número y el tipo de problemas jurídicos que se generan en las redes tienen alcances distintos a los acontecidos en el ámbito privado. La mayoría de las transgresiones a derechos con motivo de su empleo son desconocidas, no se tiene claro cuál es su alcance y la defensa de los afectados es irregular. Las razones son varias, desde la incorrecta elección de la vía jurisdiccional para impugnar una transgresión hasta la falta de herramientas adecuadas que garanticen la prevención, mitigación y no repetición de las afectaciones. Para enfrentar los problemas jurídicos generados por su uso, proponemos considerar los siguientes aspectos: cuál es el derecho aplicable del acto digital que lo generó —civil, penal, administrativo, laboral o varios simultáneamente—; quién funge como infractor —un funcionario, un académico, un alumno, un grupo de ellos o una persona externa a la institución—, y cuál es el contexto en el que se generó. Bajo este panorama, se analizan los riesgos de las redes, para lo cual estudiamos cuatro casos de instituciones

* Doctora en Derecho por la UNAM; maestra en Derecho de la Propiedad Intelectual por World Intellectual Property Organization; maestra en Gestión de Innovación de las Tecnologías de Información y Comunicación por la Universidad de Dallas e INFOTEC; maestra en Docencia por la Facultad de Ciencias Políticas y Sociales, y licenciada en Derecho por la UNAM, con experiencia profesional en los sectores público y privado. Es coordinadora de Protección de Datos Personales de la Unidad de Transparencia de la UNAM. Correo electrónico: ciberality@gmail.com.

Fecha de recepción: 21 de octubre de 2021.

Fecha de dictamen: 8 de abril de 2022.

LORENA PICHARDO FLORES

116

educativas públicas federales, a fin de identificar los problemas jurídicos frecuentes, el tipo de colisiones entre derechos que se exhiben en las redes —entre el derecho a la libertad de expresión, el derecho a la información, el derecho a la privacidad, el derecho al uso de la propia imagen, el derecho a la protección de datos personales, los derechos de autor y propiedad industrial, el derecho del patrón a la secrecía laboral del trabajador—, así como los delitos que se actualizan —ciberacoso, violación a la intimidad sexual y discriminación—. A la par, presentamos alternativas de solución a los problemas antes referidos, consistentes en tres soluciones jurisdiccionales y una autoimpositiva, a veces concurrentes: *a)* la administrativa o sancionatoria; *b)* la laboral; *c)* la civil, y *d)* la autorregulatoria.

PALABRAS CLAVE. Redes sociodigitales, instituciones de educación pública, datos personales, información pública, reparación del daño.

ABSTRACT. *When public education institutions manage social media, the number and type of legal problems that are generated in this media has different scopes than those that occur in the private sphere. Most of the violations of rights due to the use of public social media are mostly unknown, their scope is not dimensioned and an irregular defense of the institution and/or the people who make up the educational community is established. The reasons are various, from the incorrect choice of the jurisdictional route to challenge a transgression to the lack of adequate tools that will guarantee non-repetition, prevention and mitigation of effects. We affirm that in order for said institutions to be able to face the legal problems generated by the use of institutional social media, it is necessary to know the following aspects: what is the applicable law of the digital act that will terminate it (civil, criminal, administrative, labor or several simultaneously); who acts as an offender (an official, academic, student, a group of them or a person external to the institution), and what is the context in which it was left. Here the risks of social networks are analyzed, for which we study four cases of different federal public educational institutions, in order to identify the frequent legal problems, the type of collisions between rights that are exhibited in the media (right to freedom of expression, right to information, right to privacy, right to use of one's own image, right to protection of personal data, copyright and industrial property, the employer's right to the worker's labor secrecy), and the updated crimes for*

the incorrect use of those (cyberbullying, violation of sexual intimacy and discrimination). At the same time, we present alternative solutions to the aforementioned problems, consisting of three jurisdictional solutions and one self-regulatory, sometimes concurrent: a) administrative or punitive; b) labor; c) civil, and d) self-regulatory.

KEYWORDS. *Social media, public education institutions, personal data, public information, damage repair.*

117

I. INTRODUCCIÓN

En el marco de los avances tecnológicos, las redes sociodigitales institucionales son canales indispensables de comunicación, interacción e información masiva de las personas u organizaciones a la par de otros medios tradicionales de comunicación, debido a que entre sus características están la ampliación de la libertad de expresión; el poder entablar conversaciones de dos o más vías; la posibilidad de influir en las personas a través de distintas voces y narrativas; la oportunidad de establecer una comunicación sin jerarquías; el uso de un lenguaje informal y cercano; la creación y difusión de contenidos; la inmediatez de su empleo; la facilidad de la expresión de las ideas, y la convergencia de medios integrados a las plataformas de redes sociodigitales, donde confluyen los medios y la audiencia.

Sin embargo, a menudo se dejan de lado los alcances negativos, puesto que éstos también son un medio donde se presentan expresiones de odio; discriminación; violación a la privacidad; daños al honor, imagen o reputación; suplantación de identidad; ciberacoso —*cyberbullying*—; ofensas en línea —*trolling*—; revelación en Internet de datos personales —*doxing*—; acoso que recibe una persona menor de edad por parte de una adulta que se hace pasar por alguien menor —*cibergrooming*—; envío de mensajes, fotos y videos con contenido sexual —*sexting*—; creación de cuentas automatizadas diseñadas para hacer publicaciones sin intervención humana —*bots*— o redes de ellos —*botnets*—; personas que inician intencionalmente un conflicto *online* y que ofenden para distraer y sembrar divisiones mediante la publicación de declaraciones incendiarias —*trolls*—, y, en otros casos, es un espacio para el anonimato, la creación de perfiles falsos, la difusión de información engañosa, la confección de fraudes e infracciones a derechos de autor y propiedad industrial.

En este contexto, este análisis busca dar a conocer la naturaleza y noción de las redes sociodigitales y, asimismo, su empleo como canal de comunica-

LORENA PICHARDO FLORES

118 ción en las instituciones públicas de educación, particularmente en cuatro instituciones federales: el Instituto Politécnico Nacional (IPN), la Universidad Autónoma Metropolitana (UAM), la Universidad Pedagógica Nacional (UPN) y la Universidad Nacional Autónoma de México (UNAM). Posteriormente, se aborda el caso de la UNAM a través de un diagnóstico de sus redes sociodigitales, tanto principales como secundarias. Después, describimos los problemas jurídicos generados con el empleo de las redes sociodigitales en las instituciones públicas de educación, así como las afectaciones, los daños y las pérdidas que han sufrido.

- La intención del trabajo es nombrar y visibilizar las figuras jurídicas que se actualizan en cada problema jurídico generado por el empleo de las redes sociodigitales, al tiempo que se detalla su marco legal aplicable. También se exhiben las implicaciones y consecuencias de tales problemas, a saber: la exigencia de imposición de sanciones administrativas al responsable —sea funcionario de la educación o a la institución misma— por su omisión respecto a vigilar o gestionar el uso legal de las redes sociales; el pago del daño moral y/o patrimonial que puede sufrir la organización o sus integrantes; la pérdida de credibilidad institucional, la mala reputación o el daño a la propia imagen de los miembros de la comunidad educativa u organización; la presentación de denuncias, que-
rellas o solicitudes de inicio de investigación de la policía cibernética, así como las demandas civiles y laborales.

Simultáneamente, presentamos cuatro alternativas de solución a los problemas jurídicos mostrados, consistentes en tres soluciones jurisdiccionales y una autorregulatoria, a veces concurrentes: *a*) la administrativa o sancionatoria; *b*) la laboral; *c*) la civil, y *d*) la autorregulatoria.

La ruta alternativa (la autorregulatoria) es propuesta a través de la elaboración y emisión de políticas de uso de las redes sociodigitales de cada institución educativa para prevenir y mitigar los problemas jurídicos a los que se enfrentan tales instituciones, así como para disuadir la comisión de actos ilícitos al ofrecer, mediante términos del uso de las redes sociodigitales institucionales, gobernanza y civilidad digital en la comunidad educativa.

II. ENTENDIENDO A LAS REDES SOCIODIGITALES

Debemos partir de una diferencia conceptual entre redes sociales y redes sociodigitales. Mientras que el primer término enfatiza la iniciación de relaciones o *networking*, a menudo entre extraños, las redes sociodigitales se refieren a una comunicación mediada por computadora que articula y hace visibles las redes sociales, lo que permite: “(1) construir un perfil público o semipúblico

dentro de un sistema delimitado, (2) articular una lista de otros usuarios con los que comparten su conexión y (3) ver y recorrer su lista de conexiones y las realizadas por otros dentro del sistema” (Boyd y Ellison, 2007: 211).

Las redes sociodigitales son canales sociales interactivos basados en Internet, libres de restricciones y de comunicación personal masiva, que facilitan las percepciones de las interacciones entre las personas usuarias, donde se obtiene valor principalmente del contenido generado por tales usuarios (Bayer *et al.*, 2020). Además, son personales en el sentido de que permiten a los usuarios transmitir comunicación interpersonal a grandes audiencias. En este espacio de intercambio de intereses y opiniones entre personas, grupos y organizaciones se utiliza un esquema donde el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un número de seis “grados” o enlaces son necesarios para acceder a cualquier persona del planeta, que es conocida como la teoría de los seis grados de separación (Watts, 2004).

Las redes sociodigitales posibilitan la expresión amplia de las personas de manera desinhibida, sin jerarquías, de forma inmediata y en colaboración. Sin duda, el auge de estas plataformas tecnológicas ha modificado radicalmente la forma en que las personas se relacionan y consultan información, ya que asumen, por un lado, el papel de consumidores de contenidos y, por el otro, el de creadores de ellos.

Entre las cualidades que aportan las redes sociodigitales se encuentran las siguientes: la *interactividad* de las voces involucradas en una discusión; la *inmediatez*, que se refiere a la forma instantánea de respuesta; la *interconectividad* de los contenidos agregados, compartidos, vinculados y eliminados; la *viralidad* de la información difundida a través de Internet, que permite que se alcancen grandes cantidades de visitas en poco tiempo; la *inclusividad* de intereses comunes, lo cual posibilita la interacción de ideas; la *universalidad* en la difusión de contenidos, es decir, la ausencia de límites en la distribución, ya que se dirige tanto a la audiencia local como a la global; el otorgamiento del mejor *costo-beneficio* por la visibilidad otorgada en Internet; la *facilidad* de alimentación del diálogo, y la *influencia* de las audiencias.

En relación con el beneficio de las redes sociodigitales, se reconoce su uso como herramientas de solidaridad, toma de conciencia y movilización; de esta manera, tenemos ejemplos que van desde llamamientos a la acción frente a desastres naturales (sismos, huracanes, tormentas, etcétera) hasta otras urgencias de tipo social, político, cultural y económico. No obstante, su empleo también asocia riesgos, los cuales deben analizarse al utilizarlas.

Dentro de los riesgos generados en las redes sociodigitales, se deben citar a los siguientes: la rapidez en que se comunican los contenidos; la forma de-



LORENA PICHARDO FLORES

terminista en que obliga la aplicación tecnológica a presentar la información —por ejemplo, un tuit de sólo 240 palabras no ofrece contexto de lo que se narra, o bien el formato de archivo de imágenes, mensajes, hipervínculos, audio o video define la comunicación permitida—; la falta de control en la transmisión y distribución de los contenidos; el anonimato y las cuentas apócrifas; la presencia de perfiles falsos y de cuentas no oficiales; la facilidad de violar los límites de la libertad de expresión en la comunicación; los aspectos negativos de interacción desde el desarrollo psicosocial y cognitivo;¹ la “configuración desde el diseño”² de las aplicaciones tecnológicas; la propiedad comercial de las redes —Facebook, Google, etcétera—; la falta de neutralidad tecnológica e informacional de las redes sociodigitales.

120

La configuración desde el diseño de la tecnología, la propiedad de las redes y la falta de neutralidad tecnológica e informacional ameritan analizarse con detenimiento. Las empresas *big tech* dueñas de las redes sociodigitales programan, operan, practican, usan y tienen injerencia en las aplicaciones de las redes sociales. Los alcances de la tecnología de las redes sociodigitales están definidos por programadores y diseñadores, quienes establecen ideas sobre los comportamientos de las personas usuarias en ellas y condicionan su empleo, para lo cual generan árboles de decisión de lo que podrán realizar éstas con tales herramientas, junto con los perfiles que recabaron, para después aplicarles sistemas de inteligencia artificial que imitan y aprenden de manera interactiva las capacidades humanas a través de sus preferencias (Rainie *et al.*, 2017).

Es evidente que las grandes empresas tecnológicas controlan las aplicaciones de uso masivo, que Pierre Lévy las denominó “Estados-plataforma”, porque tienen la capacidad de regular la opinión pública, la publicidad y la distribución de contenidos (Hermoso, 2021). Estas compañías censuran información o dan preferencia a algún tipo de ella. Lo anterior significa que la estructura de una red sociodigital no es un medio de comunicación neutral, ya que su influencia y su incidencia están determinadas por la configuración de la propia plataforma tecnológica que otorga un servicio, por sus ajustes de origen y por el tipo de mensajes que aceptan y se cargan. La consecuencia es que este tipo de plataformas definen la manipulación, la desinformación, la censura, la discriminación y la exclusión de información, personas y grupos (Bravo *et al.*, 2019; Zhuravskaya *et al.*, 2020; Shrum, 2009).

¹ Desde agresión, trastornos por déficit de atención con hiperactividad, conductas narcisistas y temprana percepción de la sexualidad hasta la generación de adicción a las plataformas de redes.

² El concepto es una adaptación popular del término “privacidad desde el diseño”, que acuñó por primera vez Ann Cavoukian, excomisaria de Información y Privacidad de Ontario (Canadá) en 1990 (Cavoukian, 2009).

Además, desde la visión de la ciencia de datos (*big data*), el análisis de algoritmos de las plataformas tecnológicas de las redes sociodigitales son “cajas oscuras” de su configuración y capas de operación (Wakabayashi, 2018); realizan redireccionamientos a sitios específicos; establecen niveles de frecuencia de aparición de mensajes, y fijan palabras clave y lugares de conexión, así como jerarquías de contenidos. Esto evidencia que cualquier modificación a sus algoritmos trae consecuencias en la redirección del tráfico y en el comportamiento en ellas (Edgerton, 2021).³

121

Considerando que las redes sociodigitales son creadas por estas megacorporaciones, que generan nuevos tipos de demanda y suministro para los espacios de comunicación, son ellas quienes definen las políticas de uso, las cuales se caracterizan por ser extensas, complicadas, hipervinculadas, fragmentadas, poco claras, no detallan cómo se allegan de los datos personales de sus usuarios, carentes de transparencia en su diseño y programación, con algoritmos que discriminan perfiles, etcétera. En suma, las redes sociodigitales son una serie de secuencias algorítmicas que extraen y mercantilizan los datos e información, muchas veces sin que se conozca qué sucede con los datos ahí contenidos.

III. EMPLEO DE LAS REDES SOCIODIGITALES COMO CANAL DE COMUNICACIÓN DE LAS INSTITUCIONES DE EDUCACIÓN PÚBLICA

Existen dos acotaciones al presente trabajo, que a continuación se enuncian. La primera es que por “redes sociodigitales institucionales” nos referimos a las cuentas, páginas o perfiles de las redes sociodigitales que son creadas, gestionadas y reconocidas como propias por las entidades educativas, mas no a las cuentas abiertas o gestionadas por un particular, alumnado, asociación estudiantil, etcétera.⁴

³ Facebook usa el aprendizaje automático de señales para identificar personas en riesgo o que deseen suicidarse. Sus algoritmos escanean publicaciones, comentarios y videos en busca de indicios de ello; al ser identificada, ésta es revisada por su personal, quienes tienen la capacidad de llamar a miembros de seguridad pública (Facebook Safety Center, 2017; Singer, 2019).

⁴ El caso de las redes sociodigitales del alumnado de la Universidad Anáhuac Mayab, la Universidad Marista y la Universidad Autónoma de Yucatán no es un caso de redes sociodigitales institucionales, sino una red formada por un grupo de 1,280 usuarios de Telegram denominado “Zorritas UAM” para compartir fotos y videos sexuales de mujeres (Santana, 2022). Fue una iniciativa de alumnos, fuera de la esfera de gestión pública de las instituciones de educación, pero llama la atención que sólo acudieran a la vía penal a través de la

LORENA PICHARDO FLORES

Dentro de estas cuentas de redes existen principales y complementarias o secundarias. Las primeras están centralizadas por la rectoría de la institución y manejan información general de toda la institución, mientras que las segundas son cuentas accesorias que representan y facilitan el trabajo de facultades, centros de investigación, áreas de administración escolar y de difusión cultural y científica, etcétera.

122 La siguiente acotación se refiere a que por “institución de educación pública” se entiende a un sujeto obligado consistente en una institución educativa o universidad, a nivel estatal o federal, con autonomía o no, que realiza sus funciones con la recepción de ingresos públicos y, por ende, le son aplicables las leyes generales de transparencia y acceso a la información pública, así como de protección de datos personales en posesión de sujetos obligados; en el mismo sentido, son aplicables las leyes emitidas en la materia por los estados de la República mexicana, los cuales están obligados a promulgar normativa ajustada a los deberes, principios y responsabilidades que establecen las leyes mencionadas.

Las instituciones de educación pública gestionan sus redes sociodigitales de manera distinta a las formas en que lo hacen empresas, profesionistas y cualquier otra persona, porque atienden a la responsabilidad del servicio educativo desde el interés público. Éstas deben considerar una línea editorial que oriente permanente sus publicaciones; fomentar la identidad de la comunidad educativa para crear una imagen que atraiga a estudiantes y a miembros de la academia; promocionar ofertas educativas, académicas, culturales, deportivas y de esparcimiento, y difundir los activos universitarios más importantes: el capital intangible y el capital tangible.

La particularidad de los contenidos digitales o comentarios publicados en las instituciones de educación pública se basan en el capital intangible o intelectual, porque son sus activos relativos a la innovación, el desarrollo, los recursos humanos, la propiedad intelectual y los valores, particularmente la producción de conocimiento (investigación), la transmisión de conocimiento (enseñanza) y su empleo.

A partir de una recolección cuantitativa del número de publicaciones y suscriptores de las redes sociodigitales principales de cuatro instituciones educativas a nivel federal —el Instituto Politécnico Nacional (IPN), la Universidad Autónoma Metropolitana (UAM), la Universidad Pedagógica Nacional (UPN) y la Universidad Nacional Autónoma de México (UNAM)—, se advirtió que los contenidos son controlados por sus respectivas áreas de comunicación social, las cuales dependen de su director general o rector; estas áreas

denuncia de ciberacoso ante la Fiscalía General del Estado, olvidando otras vías jurisdiccionales, como la vía civil (reparación del daño), que veremos en el inciso B de la sección VI.

centralizan y gestionan las siguientes redes sociodigitales con un número dispar de personas usuarias y canales.

<i>Cuentas principales de redes sociodigitales</i>	<i>Número de suscriptores por institución de educación pública</i>			
	<i>IPN</i>	<i>UAM</i>	<i>UPN</i>	<i>UNAM</i>
Facebook	1,068,078	291,228	151,143	3,412,759
Twitter	895,700	20,600	4,220	3,300,000
Instagram	124,000	17,000	7,475	647,100
YouTube institucional	—	30,800	24,800	46,900
Canales relevantes en YouTube	“Canal Once” 1.68 millones	“TV UAM” 911	—	“TV UNAM” 437,000

123



FUENTE: elaboración propia.

De la sola exploración de las cuentas de redes sociodigitales principales, como Facebook, Twitter, Instagram y YouTube, pertenecientes al IPN, la UAM, la UPN y la UNAM, no se advirtió transgresión de derechos en las cuatro redes sociodigitales “principales”. Consideramos que la razón es porque tales redes están a cargo de expertos o profesionales gestores en comunicación social que controlan y centralizan la información, situación que no acontece en las cuentas de redes institucionales complementarias —secundarias—, en las que sí se encontraron una variedad de problemas jurídicos, en atención a que se halló que éstas son administradas por personas que no siempre son expertos en comunicación o área afín.

El hecho anterior obligó a indagar el tipo de contenidos digitales que obran en las redes complementarias o accesorias de las mencionadas cuatro instituciones educativas. El resultado fue que se encontró una serie considerable de información que transgrede varios derechos que se detallan en el apartado “V”, y que tales afectaciones se mezclan con la difusión de su capital intelectual —activos individuales e intransferibles, como conocimiento, habilidades, capacidad de innovación y talento del personal y alumnado— y su capital relacional —las relaciones que genera la institución con otras entidades educativas, los vínculos con el gobierno, la comunidad universitaria, las alianzas, las fundaciones, etcétera—, sin señalar su capital organizativo —caracterizado por ser un conocimiento institucional adquirido, mejoras, rendimientos y experiencia, como las bases de datos, los cuadros de organización, los manuales de procesos, las decisiones y, particularmente, la moral, la ética,

LORENA PICHARDO FLORES

los principios y los valores dentro de las comunidades universitarias— (Católico, 2021; Sánchez *et al.*, 2007).

124 Posteriormente, examinamos los repositorios web de las cuatro instituciones federales en búsqueda de directrices, políticas, términos y condiciones de uso, guías o recomendaciones para el empleo de las redes sociodigitales. Se encontró sólo un “Instructivo de uso para redes sociodigitales de la UNAM”, que fue emitido en 2014 y cuyo contenido está rebasado y no abarca las problemáticas que enfrentamos actualmente.

IV. EL CASO DE LA UNAM: DIAGNÓSTICO E IMPACTO DE SUS REDES SOCIODIGITALES

De acuerdo con el Diagnóstico de redes sociodigitales de la Dirección General de Comunicación Social de la UNAM en 2020, el posicionamiento a nivel mundial de la Universidad es en primer lugar Twitter y en tercer lugar Facebook, mientras que en Latinoamérica es primer lugar en Instagram. De la revisión de 29 sitios web oficiales de las diferentes facultades y escuelas de la UNAM, el 44% de ellas cuenta con la remisión de tres redes sociodigitales, el 52% tiene al menos dos (generalmente Twitter y Facebook) y el 4% posee sólo una (DGCS, 2020).

El informe indica que en algunas redes hay de tres a cuatro semanas de inactividad a partir de la última publicación; el 26% de los perfiles tardó hasta un año en su elaboración; los temas más compartidos son las actividades internas, las actividades culturales y los comunicados oficiales; en las facultades y escuelas existen 119 redes oficiales y 548 redes complementarias (de las áreas internas); el 53% de las instancias que operan las redes sociodigitales no cuenta con un plan estratégico de gestión de redes; el 93% no tiene presupuesto; del total de casos presentados, el 31% sólo tiene una persona que maneja las redes, el 28% cuenta con dos personas, el otro 28% dispone de tres personas, y el 13% restante tiene cuatro o más personas. Asimismo, el informe señala que el 42% de los catorce planteles de bachillerato no cuenta con redes sociodigitales; el 35% tiene dos —Twitter y Facebook—; el 14% sólo dispone de una, y el 9% posee tres.

El Diagnóstico reporta que la gestión de las redes sociodigitales universitarias es heterogénea; incluyen acontecimientos del día; carecen de publicaciones constantes; no interactúan con cibernautas; se omite analizar los resultados de las redes; no cuentan con estrategias para responder a las implicaciones legales suscitadas, y faltan políticas de uso en todas ellas.

Para ampliar el panorama con otros datos, indagamos en las publicaciones de las facultades y de los planteles de la Escuela Nacional Preparatoria

y del Colegio de Ciencias y Humanidades de la UNAM, cuyas publicaciones exhibían comentarios discriminatorios entre alumnos; contenidos digitales compartidos consistentes en libros, artículos y música que violan derechos de autor; difusión de frases agresivas entre el alumnado; información distribuida sin verificar la fuente de la que se obtuvo; alusiones contra el honor y la imagen de autoridades y docentes; quejas de estudiantes; divulgación de datos personales de miembros de la comunidad —calificaciones, edad y correos personales vinculados con los nombres y apellidos—. Tal evidencia da cuenta de la ausencia de gobernanza y fomento a la civilidad digital⁵ en estas plataformas.

125

V. PROBLEMAS JURÍDICOS DEL EMPLEO DE LAS REDES SOCIODIGITALES: VULNERACIÓN DE DERECHOS, DELITOS Y ACCIONES RESARCITORIAS

En este apartado se abordan las transgresiones que se presentan al emplear las redes sociodigitales institucionales en las dependencias de educación pública. El enfoque parte del análisis de los derechos que se contravienen comúnmente en ellas, así como las colisiones de derechos fundamentales, que dan cuenta de cuáles derechos, al encontrarse en disputa en un contexto particular, tienen preponderancia, valor superior o prevalencia.

1. *Libertad de expresión*

La libertad de expresión se ejerce constantemente en las redes sociodigitales. Cuando una persona se comunica e interactúa a través de una red sociodigital con una institución de educación pública, las implicaciones jurídicas van desde la imposibilidad de que una entidad pública no podrá bloquear a personas usuarias o seguidoras de una cuenta institucional⁶ hasta la transgresión de otros derechos en uso de la libertad de expresión.

Para abundar en estas dos implicaciones, es necesario aclarar qué es la libertad de expresión y sus alcances. La libertad de expresión garantiza la posibilidad de reflejar una opinión o pensamiento sobre un asunto o persona y, como derecho humano, facilita el avance y el ejercicio de otros derechos, además del pleno desarrollo de las personas, ya que les permite expresarse. En

⁵ Sobre civilidad digital, véase Beauchere (2021).

⁶ A reserva de que haya un motivo legalmente justificado, como un acto ilícito o se proteja un interés superior.

LORENA PICHARDO FLORES

ella —la libertad de expresión— se encuentran reconocidos varios derechos (Fuzesi *et al.*, 2017):

- A expresar ideas, opiniones y emitir información de toda índole.
- A acceder, buscar y recibir información.
- A difundir información e ideas sin consideración de fronteras y por cualquier medio de expresión.

126

La libertad de expresión conlleva el deber y responsabilidad de respetar otros derechos, la dignidad de las personas, el orden, la salud y la moral públicas. Esto significa que no es un derecho absoluto, sino que su límite es la vulneración de derechos de otras personas, como en aquellas situaciones en que se encuentren en conflicto varios derechos —por ejemplo, el honor o la imagen propia de una persona—; ante la comisión de un delito o infracciones a los derechos de propiedad intelectual, o bien por la incitación al odio, a la violencia, a la discriminación o a la xenofobia.

En las redes sociodigitales educativas, las conductas antes descritas pueden tener consecuencias internas (institucionales), como faltas o sanciones administrativas, académicas o estudiantiles, o consecuencias externas, como afrontar acciones legales relativas a delitos contra la dignidad de las personas.

Una medida resarcitoria al transgredir otros derechos con el uso de la libertad de expresión contemplada en nuestra Constitución es el “derecho de réplica”, que se configura cuando se afectan derechos de alguien más.⁷ Se puede ejercer por la persona ofendida en una red sociodigital, quien podrá defenderse en el mismo medio de comunicación, en el mismo horario y con el mismo tipo de audiencia. Es la medida más flexible que pudiera tomar el afectado o la afectada. No obstante, también existen otros medios jurídicos, como la reclamación de la reparación del daño moral por la vía civil.

Ante la despenalización de los llamados “delitos de prensa”, tanto a nivel federal (injuria, difamación y calumnia)⁸ como a nivel local (difamación y calumnia),⁹ es improcedente privar de la libertad a quienes transgreden el derecho a la dignidad de las personas y se deja abierta la posibilidad de demandar

⁷ Ley Reglamentaria del artículo 6o., párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos, en materia del Derecho de Réplica.

⁸ “Decreto por el que se derogan diversas disposiciones del Código Penal Federal y se adicionan diversas disposiciones al Código Civil Federal”, disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=4975044&fecha=13/04/2007.

⁹ La difamación y la calumnia establecidas en la legislación de la Ciudad de México se derogaron, en particular los artículos del 214 al 219 del Código Penal para el Distrito Federal.

la reparación del daño moral, que se encuentra regulado en el artículo 1916 del Código Civil Federal (CCF) y del Código Civil para el Distrito Federal (CCDF), y que es causado a terceros por afectaciones al honor, la imagen, el decoro, o el uso de la “malicia efectiva”.

La malicia efectiva es una falta de entendimiento de la libertad de expresión y del derecho a la información, al emitir opiniones, ideas o juicios con “información falsa” —en el caso del derecho a la información— o que se haya producido con “real malicia” —aplicable al derecho a la información y a la libertad de expresión—, con la única intención de dañar. Para que se actualice, se necesita demostrar que la información es falsa y que se publicó a sabiendas de su falsedad, o con total despreocupación sobre si era o no falsa.

Cabe agregar que, en torno al nivel de diligencia o negligencia de quien informa, la doctrina de la malicia efectiva señala que la mera negligencia o descuido no es suficiente para actualizarla, sino que se requiere una negligencia inexcusable o una “temeraria despreocupación”, referida a un dolo eventual, lo que presupone la existencia de elementos objetivos que acrediten que su autor, si bien no tenía conocimiento directo sobre la inexactitud de los datos aportados, era consciente de esa inexactitud por las circunstancias de hecho del caso y, además, disponía de los recursos que le permitían verificar, de manera inmediata y sin mayor esfuerzo, aquella inexactitud, y a pesar de ese estado de conciencia y de contar con los medios idóneos para corroborar la información, prescinde de ellos y decide exteriorizar los datos (Jurisprudencia SCJN: 1a./J. 80/2019).

La consecuencia de acreditar la malicia efectiva es la imposición de sanciones civiles y la posibilidad de iniciar la reclamación de la reparación del daño moral.

2. *Derecho a la información y derecho a la privacidad: su interacción*

Toda persona tiene derecho al libre acceso a la información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión, tal y como señala el segundo párrafo del artículo 6o. constitucional.

No obstante, el derecho a ser informado en redes sociodigitales institucionales no es absoluto, pues a pesar de que quienes reciben ingresos públicos deben informar sobre temas de interés y relevancia pública, también deben proteger y garantizar el derecho al honor o a la privacidad de las personas. En



LORENA PICHARDO FLORES

este sentido, predomina el derecho a ser informado, porque forma la opinión pública libre, indispensable para el desarrollo de una verdadera democracia.

De acuerdo con la tesis 2a. XXXIV/2018 de la Suprema Corte de Justicia de la Nación (SCJN), los entes que reciban ingresos públicos —instituciones de educación pública— y que pretendan difundir información requieren que ésta sea:

128

- De relevancia pública, de interés general, de contenido con trascendencia social.
- — Veracruz; una certera aproximación a la realidad en el momento en que se difunde; una diligente difusión de la verdad, que se encuentre basada en investigaciones, datos, informes o estadísticas oficiales que sean propios o de otras autoridades, así como por hechos notorios para la sociedad.
- — Objetiva e imparcial, sin juicios o valoraciones.

Los alcances del derecho a la información se dificultan cuando se presenta un asunto en el que se tiene que ponderar otro derecho frente a éste, como es el caso del derecho a la privacidad, que es la facultad de las personas de separar aspectos de su vida privada del escrutinio público (García Ricci, 2013: 1045); de discernir lo reservado frente al conocimiento de los demás; de no ser objeto de injerencias en su vida privada, familia, domicilio o su correspondencia.¹⁰

En el amparo en revisión 1005/2018,¹¹ la SCJN ponderó este derecho a la privacidad de un servidor público, que en el presente caso fue el fiscal general del estado de Veracruz de Ignacio de la Llave, Jorge Winckler, frente al derecho a la información de un periodista. La cuestión giró en torno a si un servidor público puede bloquear a un ciudadano en Twitter, y qué derecho debe prevalecer. En el caso se comprobó que la cuenta *@AbogadoWinckler* es usada por el servidor público para comunicar información tanto pública como personal. La información pública es de relevancia, porque debe ser accesible para todos los gobernados, incluido el periodista. La condición de servidor público atenúa y hace menos extenso su derecho a la intimidad frente a la sociedad.

¹⁰ Este derecho se encuentra regulado en los artículos 6o., párrafo primero; 7o., y 16, párrafo primero, de la Constitución; 12 de la Declaración Universal de los Derechos Humanos; 17 del Pacto Internacional de Derechos Civiles y Políticos, y 11 de la Convención Americana sobre Derechos Humanos.

¹¹ Resolución del 20 de marzo de 2019.

3. *Derecho a la información y derecho al uso de la propia imagen: su interacción*

Cuando hay una afectación a la propia imagen, implica que se dañó la impresión que esa persona conserva para mostrarse a los demás; nos estamos refiriendo a un derecho a la intimidad personalísimo sobre el que cada persona tiene el derecho de decidir en forma libre.

129

Existen disposiciones legales relacionadas con el derecho a la propia imagen: en la legislación local, la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal (LRCPDVHPIDF), y en la legislación federal, la Ley Federal del Derecho de Autor (LFDA).

La colisión entre el derecho de autor por reproducción de una obra y el derecho a la imagen de otra persona puede presentar un conflicto de intereses, cuando una persona capta o plasma una imagen a través de una fotografía, una pintura, un dibujo o algún otro medio audiovisual sin autorización del titular. El artículo 97 de la LFDA establece que frente a ello debe haber un pago por el daño causado, al tiempo que contempla la posibilidad de recibir una indemnización específica por la vulneración a ese derecho (artículo 216 bis) a través de una acción judicial de reparación del daño (artículo 213) y el procedimiento de infracción administrativa (artículo 231).

Respecto a estos casos, es conveniente referirnos a la sentencia dictada por la SCJN en el amparo directo en revisión promovido por la recurrente Ingrid Coronado Fritz e hijo contra el Grupo Editorial Notmusa —TVNotas—,¹² en el que se solicitó la reparación del daño moral conforme a la LRCPDVHPIDF y la LFDA.

Frente a una afectación al derecho a la propia imagen derivado del abuso del derecho de la información y de la libertad de expresión, la ley aplicable para lograr una reparación integral, específicamente del derecho a la retribución de los daños y perjuicios, será la que más beneficie a la persona afectada. Por ejemplo, si existe una ley local, como pudiera ser la LRCPDVHPIDF, aun cuando ésta pudiera tener preferencia por ser la ley específica en el tema, en el caso de que se alegue la violación al derecho a la propia imagen, al ofrecer la LFDA una mayor garantía de reparación, ésta será la aplicable.

De esta forma, en el caso de la conductora Ingrid Coronado se aplicó el artículo 216 bis de la LFDA, que establece que la reparación del daño material y/o moral, así como la indemnización por daños y perjuicios, no puede

¹² Resolución del amparo directo en revisión 4083/2020, del 15 de octubre de 2020.

LORENA PICHARDO FLORES

ser inferior al 40% del precio de venta al público del producto original o de la prestación original del servicio que implicó la violación al derecho. Como resultado, la afectada obtuvo como mínimo un 40% de las ganancias de venta de TVNotas, al determinarse que la publicación le causó daño al derecho a la propia imagen de la artista, el cual está protegido por el derecho de autor.

¹³⁰ 4. *Derecho a la protección de datos personales
y la recolección de información personal*

-
- En la recolección de datos personales por las empresas Twitter, Facebook —Meta—, LinkedIn, YouTube, Instagram-Pinterest, WhatsApp y TikTok, la regulación mexicana en materia de protección de datos personales establece que el tratamiento de datos personales sólo deberá circunscribirse a los que resulten adecuados, relevantes y no excesivos en relación con la finalidad del tratamiento. En todas estas redes sociodigitales, usuarios y usuarias consienten expresamente otorgar todos sus datos personales al momento en que dan clic en las políticas de uso y condiciones de privacidad, ya que son contratos de adhesión, cuyas cláusulas son hechas por una sola de las partes —la empresa— y condicionan a la aceptación de dimensiones que desconocen, entre ellas que se le otorga una licencia no exclusiva de uso de los datos personales, transferible a todos los que quieran emplear la información y, por supuesto, libre de regalías.
-

Cuando en 2014 Facebook compró por 19,000 millones de dólares a WhatsApp, señaló que no relacionaba las cuentas de WhatsApp y Facebook; no obstante, actualmente reconoce que el conjunto de datos personales recolectados y obtenidos de las personas sí se combinan en volumen, variabilidad y velocidad para analizarlos y orientarlos a la influencia en la toma de decisiones. La nueva política de privacidad de WhatsApp del 15 de mayo de 2021 permite que datos de usuarios y usuarias —excluyendo europeos— sean compartidos con el resto de los servicios de Facebook. Si bien ello no afecta a la Unión Europea, sí lo hace a países como México, de quienes tienen perfiles completos para envío de publicidad personalmente dirigida.

El Instituto Federal de Telecomunicaciones (IFT) analizó los datos personales que recaban Facebook, Instagram, YouTube, Twitter y WhatsApp a través del estudio “Privacidad de la información de los usuarios en el uso de servicios digitales” en 2020. La información se replica y conjunta en el cuadro que se presenta a continuación.

EMPLEO DE LAS REDES SOCIODIGITALES POR LAS INSTITUCIONES...

DATOS QUE RECABA CADA RED SOCIAL

<i>Facebook (Meta)</i>	<i>Instagram</i>	<i>YouTube</i>	<i>Twitter</i>	<i>WhatsApp</i>
Agenda de direcciones: videos	Atributos del dispositivo: nivel de carga de batería, tipos y nombres de aplicaciones, cámara, contenido visto.	Actividad de compra	Acceso a dispositivos	Cookies
Características del dispositivo: uso del servicio.	Cookies	Actividad en el servicio: videos que ves, términos que buscan, usuarios con los que te comunicas, visualizaciones e interacciones de contenido.	Contactos de agenda	Dirección IP
Datos de categorías especiales (opcionales): acontecimientos importantes, opiniones religiosas o políticas, origen étnico o racial, creencias filosóficas, etcétera.	Datos de categorías especiales (opcionales): acontecimientos importantes, opiniones religiosas o políticas, origen étnico o racial, creencias filosóficas, etcétera.	Actividad realizada	Cookies y sistema operativo	Foto de perfil
Datos de pago y transacciones	Fotos y video	Aplicaciones	Datos del dispositivo: sistema operativo, proveedor de telefonía móvil, navegadores usados.	GPS: ubicación
Datos de reconocimiento facial	GPS	Cookies	Dirección OIP	Historial de navegación



LORENA PICHARDO FLORES

132



<i>Facebook (Meta)</i>	<i>Instagram</i>	<i>YouTube</i>	<i>Twitter</i>	<i>WhatsApp</i>
Fotos y cámara	Historial de navegación: personas con las que interactúas y la hora, duración de actividades, etcétera.	Correos que recibes y escribes	Fotos y videos	Identificadores
Historial de navegación: personas con las que interactúas y la hora, duración de actividades, etcétera.	Libreta de direcciones y registro de llamadas: uso de los servicios y funciones.	Dirección IP	Historial de navegación	Información sobre transacciones: información y confirmación y recibos de pago.
Identificadores	Mensajes	Dispositivo y su configuración: número de teléfono y nombre del operador, navegadores utilizados, red móvil, aplicaciones, sistema operativo, sensores del dispositivo.	Idioma	Información sobre tu actividad, interacciones, archivos de registro, etcétera.
Mensajes	Metadatos	Documentos y hojas de cálculo	Información de pago: tarjeta de crédito o débito, transacciones aprobadas, dirección de facturación.	Libreta de direcciones: información de mensajes de estado.
Metadatos	Nombre y correo electrónico	Fotos y videos	Información de tuits y comentarios	Mensajes
Nombre y correo electrónico	Red y conexiones: dirección IP, operador de telefonía móvil o proveedor de Internet.	GPS (ubicación)	Mensajes (SMS)	Nombre y correo electrónico

EMPLEO DE LAS REDES SOCIODIGITALES POR LAS INSTITUCIONES...

<i>Facebook (Meta)</i>	<i>Instagram</i>	<i>YouTube</i>	<i>Twitter</i>	<i>WhatsApp</i>
Red y conexiones: dirección IP, operador de telefonía móvil o proveedor de Internet, velocidad de conexión y señales del dispositivo, como bluetooth, wifi, etcétera.	Transacciones y métodos de pago	Historial de navegación	Nombre y correo electrónico	Número de teléfono
Registro de llamadas: GPS y cookies		Historial de visualizaciones	Número de teléfono	Videos y fotografías
		Identificadores	Páginas visitadas	
		Llamadas y SMS: fecha, hora, duración, números telefónicos de las llamadas.	Proveedor de servicios de telefonía móvil.	
		Nombre y correo electrónico	Tipo de navegador	
			Ubicación	



FUENTE: elaboración propia con datos del IFT (2020: 18-22).

El cuadro anterior revela que la privacidad no existe en las redes sociodigitales. Los datos personales que se comparten en ellas no son proporcionales al servicio prestado, pues se registran, monitorean y transfieren —o venden— a otras empresas —terceros—; incluso, cuando las cuentas se eliminan por las personas usuarias, queda un registro en el sistema y es posible hacer un seguimiento de aquéllas.

La forma más segura de garantizar la protección de los datos personales en ellas es a través de la autodeterminación informativa del usuario, esto es, haciendo valer la libertad de controlar los datos personales que cada uno decide compartir.

LORENA PICHARDO FLORES

5. *Derechos de autor y propiedad industrial: limitaciones y excepciones*

Todas las obras publicadas en una plataforma de redes sociodigitales o página web están protegidas por el derecho de autor y/o conexos, de modo que será necesario obtener el permiso del titular del derecho antes de utilizarla.

134 La persona que gestiona contenidos digitales en redes sociodigitales debe respetar la propiedad intelectual, que incluye a los derechos de propiedad industrial, de autor y conexos de obras, marcas u otros recursos que empleen. En caso de ameritarlo, deberán citarse las fuentes de las que se obtuvo, previa confirmación de que la información a publicarse sea susceptible de ser divulgada y no afecte la propiedad intelectual de terceros.

Asimismo, en el empleo de música, video, fotografías o cualquier otro recurso de terceros en las cuentas institucionales en redes sociodigitales, se deberá contar con la autorización de los autores para su publicación.

La titularidad de los derechos patrimoniales de las creaciones intelectuales que generen el personal académico y los funcionarios en sus instalaciones y con sus recursos son de la institución de educación pública; no obstante, se deben reconocer los derechos morales de sus creadores. Ahora bien, al utilizar la propiedad intelectual de terceros cuyos derechos patrimoniales no le correspondan a la institución de educación pública, se debe conseguir el consentimiento expreso y por escrito del titular del material que se pretenda utilizar, un deber que difícilmente se cumple en redes sociodigitales de cualquier tipo.

En el supuesto de que una obra pudiera utilizarse libremente porque está bajo el dominio público por haber vencido el plazo de la protección del derecho de autor —transcurridos cien años *post mortem* del autor de la obra—, sólo podrá hacerlo si se tiene certeza de no haber otros derechos asociados a la obra, circunstancia similar que se aplica a una canción, un video u otra obra protegida por el derecho de autor.

En el caso de la difusión de marcas, logotipos, emblemas y escudos, así como de obras literarias o artísticas de nueva creación por parte del personal de la institución educativa en redes sociodigitales, se requiere solicitar su protección bajo la LFDA y la Ley Federal de Protección a la Propiedad Industrial (LFPPI) a través del área jurídica interna respectiva. El empleo de marcas, logotipos y escudos de la propia institución de educación pública no requiere autorización si su uso está alineado con los fines institucionales y no implica explotación comercial. Asimismo, deben utilizarse tal como obra en su registro para evitar modificaciones, mutilaciones o deformaciones que puedan alterar su carácter distintivo. Además, deben incluir la leyenda “Marca Registrada”, las siglas “M. R.” o el símbolo ® para acreditar su uso.

Cuando se publiquen contenidos digitales que utilicen “fuentes de acceso público”, se debe contemplar que los artículos 3o., fracción XVII, y 5o. de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados consideran como tales a las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio esté concebido para facilitar información al público y esté abierto a la consulta general; los directorios telefónicos; los diarios, gacetas o boletines oficiales, de acuerdo con su normativa; los medios de comunicación social, y los registros públicos.

135

Cabe hacer especial mención a los “términos y condiciones de uso” o las “políticas de uso” de las plataformas tecnológicas de tales redes, cuyo contenido se caracteriza por conceder una licencia no exclusiva, sublicenciable, mundial, no sujeta a regalías y transferible para usar, reproducir, distribuir, mostrar, ejecutar y crear obras derivadas a partir del contenido digital. Tales verbos son intercambiables o reemplazables por sinónimos en los términos y condiciones de las plataformas de Facebook, Twitter, Instagram y YouTube.

En seguimiento a lo anterior, los citados términos y condiciones de uso de las plataformas en redes sociodigitales sujetan los derechos de autor a consentir una licencia no exclusiva para utilizar su contenido, conservando el usuario los derechos sobre lo publicado, con el “beneficio” de que tal licenciamiento se extingue cuando el contenido se elimina de la red sociodigital respectiva.

6. *Deber de secrecía: su falta motiva la rescisión laboral y actualiza el delito de revelación de secretos*

Las personas que desempeñan un empleo, cargo o comisión tienen la obligación de no revelar en medios de cualquier tipo secretos de su patrón, en este caso de la institución educativa, de conformidad con los artículos 47, fracción IX, y 134, fracción XIII, de la Ley Federal del Trabajo, así como el artículo 44, fracción IV, de la Ley Federal de los Trabajadores al Servicio del Estado, Reglamentaria del Apartado B) del Artículo 123 Constitucional.

Si bien es cierto que no existe ninguna fórmula con la cual se logre cumplir por completo con el deber de confidencialidad, una de ellas es incluir una cláusula en el contrato laboral o como anexo después de firmarse el contrato.

La cláusula de confidencialidad señala a la persona trabajadora este deber y el tipo de información que mantendrá en secreto —no difundirla en redes sociodigitales—, así como el tiempo o duración de esta limitación, pues concluida la relación laboral se mantiene ese compromiso, y también debe incluir

LORENA PICHARDO FLORES

las consecuencias de incumplirla. Si la inobservancia de la cláusula se realiza durante la relación de trabajo, implica la rescisión laboral sin responsabilidad para el patrón. No obstante, si el incumplimiento se da fuera de la relación laboral, pero en el periodo marcado en el que se debería seguir cumpliendo, la institución podrá acudir a los tribunales a solicitar la indemnización por daños y perjuicios. La negativa a firmar la cláusula o acuerdo referido por parte de la persona empleada no lo exime de su deber de confidencialidad.

136

El artículo 210 del Código Penal Federal sanciona el delito de revelación de secretos a la persona que, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

También podrían ser sujetos de infracciones administrativas por el Instituto Mexicano de la Propiedad Industrial, debido a la divulgación de secretos industriales en redes sociodigitales, de conformidad con el artículo 386, fracción XIV, de la LFPPI.

7. Delitos comunes en las redes sociodigitales

A. Ciberacoso (cyberbullying) y sus formas

El ciberacoso, *cyberbullying* o acoso cibernético es la situación en que una persona es expuesta, de manera repetida y de forma prolongada en el tiempo, a acciones negativas con la intención de causar, o tratar de causar, daño o molestias por parte de una o más personas mediante el uso de medios electrónicos, tales como el teléfono celular y la Internet (Peter y Petermann, 2018).

Puede adoptar muchas formas, entre las cuales el Instituto Nacional de Estadística y Geografía (INEGI) señala:¹³

- Recibir mensajes ofensivos, con insultos o burlas.
- Recibir fotos o videos de contenido no sólo sexual.
- Que se publique información personal, fotos o videos —falsos o verdaderos— para dañar a otra (u *outing*).
- Criticar la apariencia (forma de vestir, tono de piel, peso, estatura, etcétera) o clase social.

¹³ El Módulo sobre Ciberacoso (Mociba) 2020 forma parte de la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH) 2020, a cargo del INEGI, y muestra los resultados de la encuesta levantada del 5 de octubre al 27 de noviembre de 2020. Se encuentra disponible en: <https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/MOCIBA-2020.pdf> (fecha de consulta: 14 de septiembre de 2021).

- Recibir insinuaciones o propuestas de tipo sexual para molestar.
- Hacerse pasar por otra persona para enviar información falsa, insultar o agredir.
- Ser contactado(a) por medio de nombres falsos para molestar o dañar.
- Vigilar redes sociodigitales de alguien con el fin de dañarlo (o *cyberstalking*).
- Ser provocado en línea para reaccionar de forma negativa.
- Ser excluido en línea para mantener a la víctima alejada del grupo.
- Enviar mensajes con lenguaje vulgar o discursos incendiarios para incitar a la pelea (o *flaming*).
- Generar y difundir mentiras de alguien para destruir su reputación o alejarle de otros.

137

En ocasiones se confunde con el *cibergrooming* y el *sexting*. El *cibergrooming* es un tipo de acoso que recibe una persona menor de edad por parte de una adulta que se hace pasar por otra menor, mientras que el *sexting* es el envío de mensajes, fotos y videos con contenido sexual a través de aplicaciones de mensajería.

La amplitud de acepciones del ciberacoso hace que el concepto parezca que sólo es de tipo y contenido sexual, y no es así, pues hemos señalado que el INEGI valoró varias nociones del acoso en sentido amplio. En tanto que el acoso sexual es específico, la Ley Federal del Trabajo lo regula y define como “una forma de violencia en la que, si bien no existe la subordinación, hay un ejercicio abusivo del poder que conlleva a un estado de indefensión y de riesgo para la víctima, independientemente de que se realice en uno o varios eventos”.¹⁴

El ciberacoso sexual en el contexto del párrafo anterior se sanciona laboralmente con la rescisión de la relación de trabajo, sin responsabilidad para el patrón o, en su caso, para la persona trabajadora.

El ciberacoso sexual no laboral, y más plausible de presentarse en las redes sociodigitales, es el considerado como una forma de violencia, que consiste en la difusión de audios, fotos y videos sólo de contenido sexual, de acuerdo con la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (LGAMVLV) y el Código Penal Federal (delito de violación a la intimidad sexual en su artículo 199 Octies).

Al generarse el ciberacoso sexual *online*, siempre hay forma de que se deje una huella digital, es decir, un registro que pueda servir de prueba para ayudar

¹⁴ Artículo 3o. Bis, inciso *b*, de la Ley Federal del Trabajo. Este artículo se encuentra vinculado con los numerales 47, fracción VIII; 51, fracción II, y 133, fracciones XII y XIII, de la misma Ley.

LORENA PICHARDO FLORES

a detener el abuso, que va desde capturas de pantalla hasta resguardo de mensajes de texto.

138 Para ello es indispensable denunciarlo a la Policía Cibernética de la Secretaría de Seguridad Ciudadana de la Ciudad de México y, al mismo tiempo, bloquear a la persona acosadora e informar sobre su comportamiento en la plataforma de la red sociodigital, dado que estas aplicaciones ofrecen diferentes herramientas, como los centros de atención y espacios de denuncia, para proteger a las víctimas e informarles cómo bloquear, silenciar o denunciar a las personas agresoras.

● ○ B. *Delito de violación a la intimidad sexual*

La reforma a la LGAMVLV en materia de violencia digital y mediática, conocida como Ley Olimpia, se publicó en el *Diario Oficial de la Federación (DOF)* del 1o. de junio de 2021, la cual añade el capítulo IV Ter, “De la violencia digital y mediática”, que señala las modalidades de violencia, a saber:

- Digital.
- Mediática.
- Violación a la intimidad sexual.

La “violencia digital” es la acción dolosa realizada mediante el uso de tecnologías de la información y comunicación con las que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos, reales o simulados, de contenido íntimo sexual de una persona sin su consentimiento, y que le cause a la persona daño psicológico y emocional, en su vida privada o imagen. También se considera violencia digital a aquellos actos dolosos que causan daño a la intimidad, la privacidad o la dignidad de las mujeres mediante tecnologías de la información y comunicación (artículo 20 Quáter).

La “violencia mediática” es aquella realizada a través de medios de comunicación que, de manera directa o indirecta, promueva estereotipos sexistas, haga apología de la violencia contra mujeres y niñas, permita la producción y difusión de un discurso de odio sexista, así como la discriminación de género o la desigualdad entre mujeres y hombres. Este tipo de violencia puede ser ejercida por una persona física o moral que utilice un medio de comunicación para producir o difundir dichos contenidos (artículo 20 Quinquies).

Además, cuando se trate de violencia digital o mediática, el órgano jurisdiccional podrá ordenar inmediatamente medidas de protección para la víctima,

como requerir vía electrónica a empresas digitales, medios de comunicación, redes sociodigitales o páginas electrónicas, al igual que a personas físicas o morales, que realicen la eliminación de cualquier tipo de imagen, audio o video relacionado con la investigación. Asimismo, la autoridad podrá solicitar el resguardo y conservación lícita de este contenido dañino denunciado. La anterior concepción de la violencia digital en la ley es acotada a la difusión de contenido sexual sin consentimiento y pasa por alto conductas que también son consideradas formas de violencia en línea, como el acoso, el monitoreo y acecho, la suplantación de identidad, entre otras agresiones.

139

La “violación a la intimidad sexual” es un delito cometido cuando se divulga, comparte, distribuye o publica imágenes, videos o audios con contenido íntimo sexual de una persona mayor de edad sin su consentimiento, sin su aprobación o sin su autorización. Igualmente, el delito ocurre cuando se videografe, audiografe, fotografíe, imprima o elabore imágenes, audios y videos con contenido íntimo sexual de una persona también sin su consentimiento (artículos 199 Octies, 199 Nonies y 199 Decies). Se castiga con una pena de tres a seis años de prisión y multa de quinientas a mil unidades de medida y actualización.

C. Delito de discriminación

La discriminación se define en el artículo 1o. de la Ley Federal para Prevenir y Eliminar la Discriminación como cualquier situación que niegue o impida el acceso en igualdad a cualquier derecho; pero no siempre un trato diferenciado se considerará discriminación. Ello significa que la discriminación exige la pérdida de un derecho o que se genere una desigualdad para acceder a ellos. Para efectos jurídicos, sólo se actualizará cuando hay una conducta que evidencie distinción, exclusión o restricción, a causa de alguna característica propia de la persona, que tenga como consecuencia anular o impedir el ejercicio de un derecho.

La discriminación es inconsciente y no se visibiliza; en las instituciones de educación pública es común que se marquen preferencias de acuerdo con el aspecto de las personas o su estilo de vida, tales como el origen étnico o nacional, el color de piel, la cultura, el sexo, el género, la edad, las discapacidades, la situación social o económica, la condición de salud o jurídica, la religión, la apariencia física, las características genéticas, la situación migratoria, el embarazo, la lengua, las opiniones, las preferencias sexuales, la identidad o filiación política, el estado civil, la situación familiar, las responsabilidades familiares, el idioma, los antecedentes penales o cualquier otro motivo.

LORENA PICHARDO FLORES

Por ello, se hace énfasis en que las personas más vulnerables ante la discriminación son las personas con discapacidad: personas adultas, niñas, niños, jóvenes, indígenas, personas con VIH, personas no heterosexuales, personas con identidad de género distinta a su sexo de nacimiento, migrantes y refugiados.

140 En materia penal se sancionan las conductas en contra de la dignidad de las personas a través del delito de discriminación establecido en los artículos 149 Ter del Código Penal Federal y 206 del Código Penal para el Distrito Federal.

En el empleo de las redes sociodigitales, las instituciones de enseñanza superior son responsables de educar para eliminar patrones culturales discriminatorios, así como para evitar la exclusión por motivos de pobreza en ese entorno; si bien no pueden realizar una vigilancia en Internet, estas instituciones sí pueden advertir expresiones discriminatorias en redes sociodigitales y difundir contenidos con enfoques culturales incluyentes.

En suma, son una variedad de problemas jurídicos a los que se enfrentan las instituciones de educación pública con el empleo de las redes sociales. Ante el desconocimiento del panorama que hay entre los funcionarios de la educación, se requieren de soluciones jurídicas y herramientas de prevención y mitigación del daño.

VI. SOLUCIONES JURÍDICAS Y AUTORREGULACIÓN

1. *Vía administrativa (sancionatoria)*

La persona servidora pública de una institución de educación pública que divulgue información reservada y confidencial de la propia institución o datos personales de terceros en redes sociodigitales institucionales es responsable de conformidad con la Ley General de Transparencia y Acceso a la Información Pública (artículo 206) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (artículo 163).¹⁵

Como las leyes de transparencia y protección de datos personales son de carácter administrativo y su dictamen final corresponde a los organismos garantes federal y estatales, cuando éstos se pronuncian al resolver un recurso de revisión, queja o denuncia sobre el incumplimiento de las leyes en la materia por parte de una persona servidora pública de la educación, emiten una resolución que así lo señala y remiten al órgano interno de control o contraloría de

¹⁵ Véase la normatividad análoga institucional o estatal emitida en la materia por los estados de la República y los organismos educativos autónomos.

la institución de educación pública para que sea ella quien defina la forma de fincar responsabilidades a quien cometió la infracción. Así, en los casos del IPN y la UPN, dicha función la hará su órgano interno de control; en el caso de la UAM, no hay un órgano análogo,¹⁶ y en la UNAM se llevará a cabo por su contraloría. Además, tales órganos, en conjunto con su propia legislación interna, tienen la potestad de aplicarla; sin embargo, en la práctica no hay forma de verificar que sí lo hacen y de qué forma.¹⁷

141

Al hacer una revisión de las resoluciones del comité de transparencia de los cuatro sujetos obligados (IPN, UAM, UNAM y UPN), se advierte que no se ha sometido a consideración de esos órganos plenarios ningún caso de redes sociodigitales institucionales que sea deliberado bajo las leyes de transparencia y protección de datos personales,¹⁸ y tampoco se ha ordenado someter a clasificación algún tema relacionado al promoverse un recurso de revisión por el organismo garante federal.

Por otra parte, en el caso del personal docente y alumnado, existe un problema de aplicación de ambas normativas generales, porque su ámbito personal de validez es sólo para personas que desempeñen servicios de carácter administrativo a partir de una jefatura de departamento o equivalente, por lo que a aquellos no les es aplicable. A falta de normatividad en la materia, las instituciones de educación pública aplican la legislación universitaria o educativa de la institución (estatutos generales, orgánicos o del personal académico; leyes orgánicas; acuerdos de creación; códigos de ética; legislación de responsabilidades administrativas, etcétera) a través de las defensorías y tribunales universitarios, que atienden asuntos respecto a las “faltas graves a la disciplina universitaria”, por lo que la eficacia y la aplicación que tienen las leyes especiales de transparencia y protección de datos personales no hacen posible obtener el resultado esperado.

¹⁶ Dicha institución cuenta con una contraloría social, que tiene funciones diversas a un órgano interno de control o fiscalizador.

¹⁷ Por ejemplo, en la única solicitud de información hecha a una contraloría, específicamente a la de la UNAM, se respondió que a la fecha no ha habido sanciones a funcionarios o académicos por infracciones a la LGPDPPSO. Véase folio 330031921000446, disponible en: <https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031921000446&coleccion=2>.

¹⁸ Véanse las resoluciones del Comité de Transparencia de la UNAM (disponible en: <http://www.transparencia.unam.mx/obligaciones/LGTAIP/consulta/sesiones-comite-transparencia>); el de la UAM (disponible en: https://transparencia.uam.mx/comite_resoluciones.html); el de la UPN (disponible en: <https://upn.mx/index.php/transparencia/acceso-a-la-informacion>), y el del IPN (disponible en: <https://consultapublicamx.inai.org.mx/vut-web/faces/view/consultaPublica.xhtml?idEntidad=MzM=&idSujetoObligado=MjE4#tarjetaInformativa>).

LORENA PICHARDO FLORES

2. *Vía laboral*

La vía laboral establece una serie de causales de rescisión de la relación laboral, y entre ellas se encuentran la violencia y los malos tratos u otros análogos en contra del trabajador por parte del patrón —institución de educación pública— o sus representantes, la divulgación de secretos institucionales y los actos de discriminación, conforme a los artículos 47, 51, 133 y 994, fracción VI, de la Ley Federal del Trabajo.

142 ● Tratándose de mujeres como víctimas de violencia laboral, moral y por razón de sexo no sólo en redes sociodigitales, existe la posibilidad de sancionar a quien la efectúe de acuerdo con el numeral 14, fracción I, de la LGAMVLV. ● ○ Por ejemplo, la UNAM, en uso de esta potestad, reformó los artículos 95 y 99 del Estatuto General, calificando a la violencia de género como una causa “especialmente grave de responsabilidad” y que es aplicable a toda la comunidad universitaria.

Por otra parte, cuando se divulga o revela información reservada, al tratarse de bienes inmateriales, la persona que lo realiza se aprovecha de su naturaleza reproducible y transmisible, lo que la hace susceptible de ser explotada; esto perjudica la posición, el valor institucional y el libre desarrollo de algún proceso que beneficia a la comunidad. Hemos dicho que la persona que revela tal información puede ser sujeto de rescisión laboral y, además, el patrón cuenta con la vía civil para reclamar una indemnización por daños a los trabajadores o extrabajadores que lo cometieron.

3. *Vía civil: acciones resarcitorias a través de la reparación del daño*

Tratándose de daños y perjuicios, la persona que obre ilícitamente está obligada a reparar el daño, o cuando ejerza un derecho y cause un daño a otro, está obligada a indemnizarlo si se demuestra que el derecho sólo se ejerció a fin de causar el daño. En este contexto, se presenta la reparación del daño moral por medio de la condena al pago de daños y perjuicios.

Las consecuencias de un hecho ilícito son generar las condiciones para que tal hecho no vuelva a suceder, o sea, que tenga efectos de no repetición, y reparar el daño. Pero ¿qué tipo de reparaciones se pueden dar? Según el artículo 1916 del CCF, daño moral es “la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás”.

Para la procedencia de la reparación civil del daño, se deben acreditar los siguientes elementos (artículos 1910 y 1912 del CCF):

- 1) Una conducta u omisión lesiva o ilícita.
- 2) La existencia del daño (resultado de la conducta u omisión lesiva).
- 3) La relación de causalidad entre la acción y el daño.

La forma en que se repara el daño moral es a través de una indemnización en dinero, cuyo monto lo determinará el juez, para lo cual considerará los siguientes aspectos:

- 1) Los derechos lesionados.
- 2) El grado de responsabilidad.
- 3) La situación económica del responsable, así como de la víctima.
- 4) Las demás circunstancias del caso.

Además, derivado de la despenalización de los “delitos de prensa”, el CCF añadió cuatro casos en los que se obliga a la reparación del daño moral, que antes eran los supuestos de delitos contra la honra:

- I. El que comunique a una o más personas la imputación que se hace a otra persona física o moral, de un hecho cierto o falso, determinado o indeterminado, que pueda causarle deshonra, descrédito, perjuicio, o exponerlo al desprecio de alguien;
- II. El que impute a otro un hecho determinado y calificado como delito por la ley, si este hecho es falso, o es inocente la persona a quien se imputa;
- III. El que presente denuncias o querrelas calumniosas, entendiéndose por tales aquellas en que su autor imputa un delito a persona determinada, sabiendo que ésta es inocente o que aquél no se ha cometido, y
- IV. Al que ofenda el honor, ataque la vida privada o la imagen propia de una persona.

Las instituciones de educación pública están legitimadas para demandar la reparación del daño moral en caso de que se afecte la reputación que tienen los demás respecto de la imagen que se tenga de un colegio, escuela, instituto o universidad, y la reparación deberá contener la obligación de la rectificación o respuesta de la información difundida en el mismo medio donde fue publicada y con el mismo espacio y la misma circulación o audiencia a que se dirigió la información original.¹⁹

¹⁹ La acción para exigir la reparación de los daños causados prescribe en dos años contados a partir del día en que se haya causado el daño.



LORENA PICHARDO FLORES

Creemos que, en la práctica, esta vía puede satisfacer más a la víctima, pues podrá solicitar al juez, además de la indemnización obtenida, la publicación de un extracto de la sentencia a través de los medios informativos que considere convenientes a fin de restituir su decoro, honor o reputación. Si el daño fue por la difusión en redes sociodigitales, se ordenará que los mismos den publicidad al extracto de la sentencia con la misma relevancia que tuvo la difusión original.

144

Ahora bien, la reproducción fiel de la información no da lugar al daño moral, incluso en los casos en que la información reproducida no sea correcta y pueda dañar el honor de alguna persona, pues no constituye una responsabilidad para el que difunde dicha información, siempre y cuando se cite la fuente de la que se obtuvo. Por lo tanto, no hay reparación del daño moral cuando se ejerzan los derechos de opinión, crítica, expresión e información, en los términos y con las limitaciones de los artículos 6o. y 7o. constitucionales (artículo 1916 Bis del CCF).

En ningún caso se considerarán ofensas al honor las opiniones desfavorables de la crítica literaria, artística, histórica, científica o profesional. Tampoco se considerarán ofensivas las opiniones desfavorables realizadas en cumplimiento de un deber o ejerciendo un derecho cuando el modo de proceder o la falta de reserva no tenga un propósito ofensivo.

Es importante señalar el caso de las personas menores de edad. Por ejemplo, si los bachilleres que ejecuten actos que dan origen a la reparación de daño moral se encuentran bajo la vigilancia de la institución de educación pública, ésta como autoridad asumirá la responsabilidad de aquéllos (artículo 1920 del CCF).

4. *Autorregulatoria*

Consideramos que un modelo de prevención legal puede ayudar a prevenir, detectar y gestionar riesgos cuando se concreta en políticas de uso de redes sociodigitales que den cuenta de estrategias, procesos y recomendaciones para el empleo de estas últimas a fin de evitar afectaciones.

Las políticas en la materia proporcionan herramientas para gestionar las crisis, la desinformación, la divulgación de información incorrecta, la mitigación de riesgos, las acciones a seguir en torno a un error o un ataque, la protección respecto a malas relaciones públicas o problemas legales, las actividades que se deben evitar en las redes sociodigitales —por ejemplo, cuestionarios en redes sociodigitales en los que se solicita información personal—, las directrices relacionadas con los derechos de autoría, la confidencialidad de

los datos personales, la violencia digital, el *cyberbullying*, la discriminación, a quién acudir y cómo responder si surge un problema de seguridad en las redes sociodigitales, entre muchos otros. Dentro de los grandes beneficios de contar con políticas de redes sociodigitales se encuentran prevenir y salvaguardar a la institución de educación pública contra problemas jurídicos potenciales, proteger su reputación y aumentar su reconocimiento. Existen algunas guías que contienen elementos que deberían considerarse para la redacción de una política de redes sociodigitales institucionales, que incluso detallan mejores prácticas (Newberry y Cooper, 2021).

145

VII. CONCLUSIONES

En este texto se señalaron las múltiples características de las redes sociodigitales y el alcance digital de sus aplicaciones tecnológicas, donde cada plataforma de redes puede combinarse con otros canales, aplicaciones y otras plataformas de redes, lo cual provoca que los problemas jurídicos se distribuyan con celeridad y se pierda el control en Internet. Al mismo tiempo, se evidenció el tipo y la cantidad de datos personales e información en general que recaban las empresas dueñas de las redes sociodigitales, funciones que no coinciden con las de las instituciones educativas; no obstante, al visibilizarlo se combate el empleo inercial que establecen y promueven las megacorporaciones propietarias.

Por otro lado, se estableció que las redes sociodigitales de las cuatro entidades educativas federales estudiadas cuentan con contenidos heterogéneos, sobre todo en sus cuentas secundarias o complementarias, que son gestionadas por personal que no tiene la experiencia y la trayectoria que sí posee, en cambio, la autoridad central experta en comunicación social de la institución. Esta falla repercute en la diversidad de problemas jurídicos que se presentan con respecto a las transgresiones a la libertad de expresión, al derecho a la información, al derecho a la privacidad, al derecho al uso de la propia imagen, al derecho a la protección de datos personales, a los derechos de autor y propiedad industrial, y al deber de secrecía, así como a los delitos comunes en las redes sociales (ciberacoso, violación a la intimidad sexual y discriminación).

Consideramos que la alternativa más efectiva y contundente para garantizar que un afectado reciba justicia derivado de un problema jurídico es acudir a la vía penal cuando se trate de un delito y a la vía civil para recibir la reparación del daño ante una afectación moral o patrimonial, pues ambas vías no dependen de los órganos internos de control o instancias análogas de la institución educativa. En este sentido, además de obtenerse una resolución por reparación del daño por un órgano jurisdiccional, si se solicita, se obliga al

LORENA PICHARDO FLORES

infractor a difundir una disculpa pública a la víctima en el mismo medio en que se generó el daño. Lo anterior, sin dejar de lado las facultades de las autoridades educativas de iniciar procedimientos administrativos sancionatorios y, en su caso, la rescisión laboral de los funcionarios educativos responsables del uso incorrecto de las redes sociodigitales institucionales.

146 Finalmente, es indispensable sensibilizar y capacitar al alumnado y al personal docente, directivo y administrativo sobre el respeto a los derechos en las redes sociodigitales; en efecto, hacerles partícipes en la forma y el modo de publicar comentarios —el mensaje— en una plataforma tecnológica —el medio— es una manera de manipular al receptor, ya sea de activarlo o desmotivarlo, y configurar su personalidad digital, tal como lo afirmó Marshall McLuhan: “el medio es el mensaje”.

VIII. BIBLIOGRAFÍA

- BAYER, J. B. *et al.*, 2020, “Social Media Elements, Ecologies, and Effects”, *Annual Review of Psychology*, vol. 71, núm. 1, disponible en: <https://doi.org/10.1146/annurev-psych-010419-050944>.
- BOCZKOWSKI, P. J. *et al.*, 2018, “How Young Users Deal with Multiple Platforms: The Role of Meaning-Making in Social Media Repertoires”, *Journal of Computer-Mediated Communication*, vol. 23, núm. 5.
- BOTERO, S. *et al.*, 2020, “Capital intelectual en la creación del conocimiento: hacia el mejoramiento de la calidad académica”, *Revista de Ciencias Sociales*, Colombia, vol. 26, disponible en: <https://produccioncientificaluz.org/index.php/rcs/article/view/34129>.
- BOYD, Danah M. y ELLISON, N. B., 2007, “Social Network Sites: Definition, History, and Scholarship”, *Journal of Computer-Mediated Communication*, vol. 13, núm. 1, disponible en: <https://doi.org/10.1111/j.1083-6101.2007.00393.x>.
- BRAVO, D. Y. *et al.*, 2019, “When Things Go Viral: Youth’s Discrimination in the World of Social Media”, *Handbook of Children and Prejudice: Integrating Research, Practice, and Policy*, Nueva York, Springer.
- BRITO, J. G. *et al.*, 2012, “El uso de redes sociales por parte de las universidades a nivel institucional. Un estudio comparativo”, *Revista de Educación a Distancia (RED)*, vol. 32, disponible en: <https://revistas.um.es/red/article/view/233071>.
- CANO, R. J., 2014, “Facebook compra WhatsApp por más de 13,800 millones de euros”, *El País*, disponible en: https://elpais.com/tecnologia/2014/02/19/actualidad/1392848898_360807.html.

- CATÓLICO, D., 2021, “Las nuevas tecnologías en la divulgación del capital intelectual: análisis en universidades colombianas”, *Apuntes Contables*, núm. 28, disponible en: <https://doi.org/10.18601/16577175.n28.03>.
- CAVOUKIAN, A., 2009, “The 7 Foundational Principles”, disponible en: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.
- CLAYPOOLE, T. F., 2014, “Privacy and Social Media”, *American Bar Association*, disponible en: https://www.americanbar.org/groups/business_law/publications/blt/2014/01/03a_claypoole/. 147
- CONSEJO NACIONAL PARA PREVENIR LA DISCRIMINACIÓN (CONAPRED), s.f., “Discriminación e igualdad”, disponible en: https://www.conapred.org.mx/index.php?contenido=pagina&id=84&id_opcion=142&op=142 (fecha de consulta: 20 de septiembre de 2021). ● ○ ●
- CORONA, S., 2017, “La discriminación que vemos en redes sociales no es distinta de la que hay en la calle”, *El País*, disponible en: https://elpais.com/tecnologia/2017/12/15/actualidad/1513293481_945800.html.
- DIRECCIÓN GENERAL DE COMUNICACIÓN SOCIAL DE LA UNAM (DGCS), 2020, “Diagnóstico de redes sociodigitales en la UNAM”, trabajo interno sin publicar.
- EDGERTON, A., 2021, “Open Facebook’s «Black Box», Whistle-Blower Tells House Panel”, *Bloomberg*.
- FACEBOOK SAFETY CENTER, 2017, “Prevención de suicidios”, disponible en: https://www.facebook.com/safetyv2?locale=es_LA (fecha de consulta: 10 de septiembre de 2021).
- FUZESI, S. *et al.*, 2017, *Estándares internacionales de libertad de expresión. Guía básica para operadores de justicia en América Latina*, Center for International Media Assistance.
- GHERSI, C. A., 2002, *Daño moral y psicológico. Daño a la psiquis*, Astrea.
- HERMOSO, B., 2021, “Pierre Lévy: «Aunque muchos no lo crean, ya éramos muy malos antes de que existiera Internet»”, *El País*, disponible en: <https://elpais.com/eps/2021-06-27/pierre-levy-aunque-muchos-no-lo-crean-ya-eramos-muy-malos-antes-de-que-existiera-internet.html>.
- INSTITUTO FEDERAL DE TELECOMUNICACIONES (IFT), 2020, “Privacidad de la información de los usuarios en el uso de servicios digitales”, disponible en: <http://www.ift.org.mx/usuarios-y-audiencias/privacidad-de-la-informacion-de-los-usuarios-en-el-uso-de-servicios-digitales>.
- INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA (INEGI), 2021, “Módulo sobre Ciberacoso 2020”, *Comunicado de Prensa*, núm. 371/21, disponible en: <https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/MOCIBA-2020.pdf>.

LORENA PICHARDO FLORES

KWESTEL, M. y MILANO, E. F., 2020, "Protecting Academic Freedom or Managing Reputation? An Evaluation of University Social Media Policies", *Journal of Information Policy*, núm. 10, disponible en: <https://doi.org/10.5325/jinfopoli.10.2020.0151>.

LEITNER, K. H. y CURAJ, Adrian (eds.), 2014, *A Strategic Approach for Intellectual Capital Management in European Universities. Guidelines for Implementation*, UEFISCDI.

148

MAC, R. y FRENKEL, S., 2021, "No More Apologies: Inside Facebook's Push to Defend Its Image", *The New York Times*, disponible en: <https://www.nytimes.com/2021/09/21/technology/zuckerberg-Facebook-project-amplify.html>.

●
○
●

McLUHAN, M. y FIORE, Q., 1969, *El medio es el masaje. Un inventario de efectos*, Paidós.

MENDOZA, L. A., 2014, *La acción civil del daño moral*, México, UNAM, Instituto de Investigaciones Jurídicas, disponible en: <https://biblio.juridicas.unam.mx/bjv/id/3636>.

MICROSOFT ONLINE SAFETY, s.f., "Digital Civility Index & Our Challenge", Microsoft, disponible en: <https://www.microsoft.com/en-us/online-safety/digital-civility>.

MILLER, D., 2016, "Politics", *How the World Changed Social Media*, UCL Press, vol. 1, disponible en: <https://doi.org/10.2307/j.ctt1g69z35.17>.

NEL, S., 2016, "Social Media and Employee Speech: The Risk of Overstepping the Boundaries into the Firing Line", *The Comparative and International Law Journal of Southern Africa*, vol. 49, núm. 2, disponible en: <https://www.jstor.org/stable/26367599>.

NEWBERRY, C. y COOPER, P., 2021, "Cómo redactar una política de redes sociales (plantilla gratuita + ejemplos)", *Hootsuite*, disponible en: <https://blog.hootsuite.com/es/politica-de-redes-sociales/>.

PETER, I. K. y PETERMANN, F., 2018, "Cyberbullying: A Concept Analysis of Defining Attributes and Additional Influencing Factors", *Computers in Human Behavior*, núm. 86, disponible en: <https://doi.org/10.1016/j.chb.2018.05.013>.

RAINIE, L. *et al.*, 2017, "The Future of Free Speech, Trolls, Anonymity and Fake News Online", *Pew Research Center*, disponible en: <https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/>.

RICHARDSON, M. E., 2020, "Social Media in the Classroom. The New Normal for University Education after COVID", *International Dialogues on*

- Education Journal*, vol. 7, disponible en: <https://doi.org/10.53308/ide.v7i1/2.19>.
- SÁNCHEZ, A. J. *et al.*, 2007, “El concepto de capital intelectual y sus dimensiones”, *Investigaciones Europeas de Dirección y Economía de la Empresa*, vol. 13, núm. 2.
- SANTANA, R., 2022, “Destapan grupo en Telegram donde alumnos de la Anáhuac compartían contenido íntimo de compañeras”, *Proceso*, disponible en: <https://n9.cl/ae82q>. 149
- SHRUM, L. J., 2009, “Media Consumption and Perceptions of Social Reality: Effects and Underlying Processes”, en BRYANT, J. y OLIVER, M. B. (eds.), *Media Effects: Advances in Theory and Research*, 3a. ed., Nueva York-Londres, Routledge. ●
○
●
- SINANAN, J. *et al.*, 2021, *Education and Young People*, núm. 16.
- SINGER, N., 2019, “El monitoreo de Facebook para prevenir suicidios causa controversia”, *The New York Times*, disponible en: <https://www.nytimes.com/es/2019/01/03/espanol/Facebook-suicidio.html>.
- VALKENBURG, P. M. y TAYLOR, J., 2017, *Plugged in: How Media Attract and Affect Youth*, Yale University Press.
- WAKABAYASHI, D., 2018, “¿Cómo funciona el algoritmo de búsqueda de Google?”, *The New York Times*, disponible en: <https://www.nytimes.com/es/2018/09/07/espanol/google-algoritmo-busqueda-trump.html>.
- WATTS, D., 2004, *Six Degrees: The Science of a Connected Age*, W. W. Norton & Company.
- WELLS, G. *et al.*, 2021, “Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show”, *The Wall Street Journal*, disponible en: <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739>.
- ZHURAVSKAYA, E. *et al.*, 2020, “Political Effects of the Internet and Social Media”, *Annual Reviews*, disponible en: <https://www.annualreviews.org/doi/full/10.1146/annurev-economics-081919-050239#:~:text=The%20spread%20of%20the%20Internet%20and%20social%20media,media%20can%20be%20used%20to%20mobilize%20voters.%203>.