Inteligencia Artificial: ¿una nueva herramienta para la violencia digital?

Dra. Laura Coronado Contreras
Investigadora del IMEESDN. Profesora de la Escuela Libre de Derecho de la cátedra Derecho y Tecnología.

1. Introducción

Casos como el de los 15 adolescentes de Almendralejo, Diego "N", el entonces estudiante del Instituto Politécnico Nacional o la controversia entre la senadora Andrea Chávez y el caricaturista Antonio García Nieto han dado la vuelta al mundo en los últimos meses. En ellos, se han utilizado imágenes de mujeres —muchas de ellas jóvenes menores de edad— para alterarlas con Inteligencia Artificial (IA). La manipulación utilizando una herramienta tecnológica tan poderosa, redundó en contenidos lascivos, desnudos, fotografías y videos íntimos propagados en distintas redes sin autorización. Lamentablemente, dichos delitos muestran la falta de cultura digital de la población, la ausencia de procedimientos que realmente sean ágiles, la apremiante necesidad de que las plataformas cuenten con mayores controles y reflejan, en definitiva, lo mucho que aún nos falta construir para erradicar la violencia digital de género.

Sanciones como un año de libertad vigilada, cursos de formación afectivo-sexual[1] o resoluciones en donde se señala que si bien existió un delito y además, una vulneración a las víctimas, no se puede probar la autoría del implicado,[2] simplemente sirven para demostrar que las herramientas tecnológicas y las vías jurídicas son pocas e insuficientes. Tal parece

[1] "Un año de libertad vigilada para 15 menores de Almendralejo por manipular imágenes de niñas", [en línea]: *https://elpais.com/sociedad/2024-07-09/un-ano-de-libertad-vigilada-para-15-menores-de-almendralejo-por-manipular-imagenes-de-ninas.html*

[2] "Caso Diego 'N': ¿Por qué absolvieron al estudiante del IPN que hacía 'deepfakes' de sus compañeras?" [en línea]: *https://www.elfinanciero.com.mx/cdmx/2024/12/05/caso-diego-n-por-que-absolvieron-al-estudiante-del-ipn-que-hacia-deepfakes-de-sus-companeras/*

que el mensaje es que hay muy poco en lo que se puede perder y mucho por ganar en una industria que genera, sólo en Estados Unidos, un valor de casi 977 millones de dólares anualmente.[3]

Por desgracia, conceptos como ciberacoso o sextorsión, se integran como parte de nuestro lenguaje cotidiano en un marco de normalización e impunidad. Conductas abusivas, agresiones constantes, comentarios nocivos y muchas otras expresiones de violencia conviven en un espacio abierto, universal, libre, como lo es, el ciberespacio y, sin la adecuada regulación. Por ejemplo, según el "Informe Ciberviolencia y Ciberacoso contra las mujeres y niñas en la Convención Belém Do Pará", elaborado por el Mecanismo de Seguimiento de dicho tratado (MESECVI), ONU Mujeres y la Unión Europea tenemos grandes pendientes en la materia. Por ejemplo, en América Latina, el 65% de las mujeres encuestadas en Argentina no denuncian actos de violencia digital y en Chile del 18% de las víctimas que decidieron acudir a las autoridades, sólo poco más del 6% recibieron la denuncia.[4]

Aunque podrían existir una multiplicidad de causas para dichas estadísticas, como el miedo a denunciar o la minimización de las agresiones, lo cierto es que no contamos con un marco legal adecuado para conocer aquellas conductas que son consideradas como delitos, cuáles serían sus penas, los procedimientos a seguir y autoridades capacitadas para responder a realidades diferentes a aquellas con las que comúnmente están en contacto. Tal es el caso que, de las 14,526 denuncias registradas en México entre 2017 y 2023, sólo se

[3] "Market size of the online pornographic and adult content industry in the United States from 2018 to 2023", [en línea]: *https://www.statista.com/statistics/1371582/value-online-website-porn-market-us/#:~:text=Adult%20and%20pornographic%20website%20industry%20market%20size%20in%20the%20U.S.%202018%2D2023&text=In%202022%2C%20the%20adult%20online,58%20percent%20compared%20to%202018*.

[4] "Informe Ciberviolencia y Ciberacoso contra las mujeres y niñas en la Convención Belém Do Pará" [en línea]: *https://www.oas.org/es/mesecvi/docs/MESECVI-Ciberviolencia-ES.pdf*

han emitido 2 sentencias y se ha llegado en 5 expedientes a acuerdos reparatorios,[5] es decir, más del 80% de los delitos digitales investigados en nuestro país, permanecen "en trámite".

La IA se ha convertido en un parteaguas en los años más recientes. Sus detractores ven los peligros de su uso desmedido —y sin regulación— y que pueden desembocar en desinformación, pérdida de empleos, dependencia digital y, en el tema que nos ocupa, violencia. Sus partidarios lo analizan como una nueva revolución tecnológica que automatizará procesos y brindará mayor calidad de vida a sus usuarios, reducirá costos para las empresas y optimizará a los gobiernos. Ciertamente, la digitalización no tiene marcha atrás y ya hemos presenciado sólo algunos de los primeros ejemplos de lo negativo que puede ser un uso focalizado en delinquir. Este pequeño análisis busca abrir el debate sobre una de las áreas más delicadas y trascendentales para cualquier ser humano: su identidad, su imagen y el libre desarrollo de su personalidad.

2. Concepto de violencia digital

Dos problemas fundamentales atañen a la conceptualización de la llamada violencia digital: por un lado, su falta de identificación y, por el otro, la normalización de las agresiones y, en determinadas ocasiones, hasta su promoción. La Real Academia de la Lengua Española define a la *violencia* con una serie de sinónimos como brutalidad, salvajismo, ferocidad, crueldad, ensañamiento, furia, arrebato o coacción y también nos señala a aquella "acción contra el natural modo

[5] "Víctimas de violencia digital siguen sin acceder a la justicia pese a tipificación del delito" [en línea]: *https://www.milenio.com/tecnologia/victimas-violencia-digital-siguen-acceder-justicia*

de proceder".[6] Es así que, cuando hablamos de violencia en el ciberespacio, podemos definirla como aquella conducta agresiva, constante, intrusiva que inhibe o coarta el libre desarrollo de una persona en su entorno digital ya sea con amenazas, comentarios lascivos, acosándola, hostigándola, difundiendo imágenes o videos —íntimos o no— sin autorización, compartiendo sus datos personales, rasgos de su identidad o de sus familiares que puedan significar un peligro, o cualquier otra situación que le impida considerarse en un espacio seguro, sano y tranquilo.

Por su parte, la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, define a ésta como "cualquier acción u omisión, basada en su género, que les cause daño o sufrimiento psicológico, físico, patrimonial, económico, sexual o la muerte tanto en el ámbito privado como en el público" y, propiamente, a la violencia digital como "toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la 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, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia".[7] Para dimensionar, tan sólo un poco lo dilatado que ha sido visibilizar estos temas, podemos simplemente ver que dicha ley fue publicada en 2007 y que el concepto de violencia digital fue incluido hasta 2021, es decir, mucho más de una década después. En ese mismo año, se realizaron reformas al Código Penal Federal conocidas por el

[6] *Diccionario de la Real Academia de la Lengua Española* [en línea]: *https://dle.rae.es/violencia?m=form*

[7] "Ley General de Acceso de las Mujeres a una Vida Libre de Violencia" [en línea]: *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf*

público en general como la llamada "Ley Olimpia" para sancionar el *grooming* y la pornovenganza (ambas conductas que definiremos más adelante). Ello ha significado un paso importante pero no un logro definitivo en la prevención y erradicación de estos fenómenos.

Derechos tan esenciales —y globalmente reconocidos— como la intimidad y la privacidad, la libertad de expresión, la identidad, la libertad sexual, la inviolabilidad de las comunicaciones o del domicilio, son menoscabados cuando se presentan conductas de violencia digital contra niñas, adolescentes y mujeres. El problema reside en que se les incluye —en México y otras regiones— en otros tipos penales simplemente añadiendo una frase como "y en medios digitales" o "utilizando las nuevas tecnologías", o bien, se les tipifica pero los procedimientos para llevarlos a su fin no contemplan puntualmente escenarios tan relevantes como la presentación y la admisión de pruebas. Por ello es de la mayor de las relevancias la alfabetización digital, la construcción de entornos virtuales sanos, la cultura de la denuncia, la profundización en valores como la verdad y el establecimiento de un marco legal justo, igualitario, ágil y de vanguardia en estos temas.

3. Tipos de violencia digital

Una de las características principales de la violencia y, especialmente de la violencia digital, es que ésta comienza con pequeñas conductas que pueden ser calificadas incluso, de inofensivas. La violencia va escalando al no encontrar los cauces y límites bien establecidos. Va haciéndose cotidiana, constante y hasta imperceptible o peor aún, permitida o promovida desde los ámbitos que deberían ser más seguros: nuestro hogar, la escuela o el trabajo. Quienes la ejercen son personas cercanas a la víctima: figuras de crianza, pareja,

compañeros, colegas en gran parte de las ocasiones. En cualquiera de sus modalidades podemos ver que "siempre que hay violencia se producen daños o lesiones, aunque no se vean ni se reproduzcan. Por lo tanto, cuando hay violencia se transgrede el derecho de otra persona, es decir, toda violencia implica agresión... es ahí donde entra la noción de *poder*. En suma, toda violencia *implica abuso, poder y voluntad*. Un aspecto determinante del comportamiento violento es que el provocador ejerce su poder con abuso para nulificar la voluntad de la víctima que es a quien se pretende someter y controlar".[8]

Como mencionábamos, la violencia digital puede comenzar con hechos tan normalizados como el llamado ***"stalkeo"***, ***"stalkear"*** o ***"ser un stalker"*** que se refiere a una práctica generalizada que consiste en "espiar" a alguien por medio de sus redes sociales o la de sus amigos. Esta "vigilancia" para conocer detalles de la vida de otros puede derivar en otro tipo de conductas —mucho más peligrosas— aunque comúnmente se realizan "por curiosidad" sobre la vida de personas conocidas pero que no son nuestros seguidores o amigos. Por ejemplo, una expareja, una amiga de hace tiempo, un jefe. "Todos lo hemos hecho", "no se daña a nadie" o "es sólo para saber si está bien o qué pasó" son frases comunes utilizadas como respuesta por los "espías cibernéticos". ¿Cuál es la diferencia con un merodeador?

Un merodeador es una persona que vaga de un lugar a otro, generalmente, con la intención de atacar o robar. Por definición, tiene un comportamiento sospechoso que puede implicar una amenaza para la seguridad de las personas o la propiedad. ¿Cómo nos sentimos cuando alguien revela que nos ha buscado en redes sociales, conoce nuestras aficiones,

[8] "Centro para el Desarrollo Humano e Integral de los Universitarios de la Universidad Veracruzana" [en línea]: *https://www.uv.mx/cendhiu/files/2012/09/violencia.pdf*

relata lugares en donde hemos estado o con quiénes convivimos? Por ello, algunas personas dicen que si se sanciona en algunas legislaciones "los actos preparatorios", también debería de evitarse este tipo de prácticas. ¿Podríamos realmente considerar el stalkear como punible? ¿Técnicamente podría evitarse? El contexto y el propósito son fundamentales pero, para la mayoría, el stalkeo es una práctica cotidiana e inofensiva. Aunque quizá cambiaríamos de opinión si hacemos la traducción literal de la palabra y leemos "acechar".[9]

Otra conducta violenta en línea que se toma como "una broma" es aquella conocida como ***zoombombing*** que se desarrolló durante la Pandemia pero sigue vigente. Dicha práctica consiste en la intrusión no deseada en videollamadas, particularmente conferencias, con el fin de compartir o insertar material de naturaleza lasciva, obscena, racista o antisemita para que se cierre la sesión. Sin duda, las vulnerabilidades de plataformas como Zoom dieron pie a que hackers (expertos en tecnología) exhibieran sus deficiencias de seguridad, pero no por ello puede justificarse su actuación. Una particularidad es que no se realiza por una sola persona. Para su ejecución, varios agentes se coordinan a través de foros de otras plataformas como Reddit o Discord: "trataban sus redadas como si se tratara de un videojuego multijugador. Los atacantes compartían un plan, actuaban al unísono, se felicitaban por ataques efectivos, abrumaban a sus víctimas y se jactaban de sus habilidades".[10] ¿Sólo una broma?

Una práctica que quizá, ya podríamos identificar como violenta, es la del ***doxing*** (algunos autores la manejan como *doxxing*) que se describe como investigar y publicar información personal, privada o identificante con el propósito de in-

[9] *Cambridge Dictionary* [en línea]: *https://dictionary.cambridge.org/es/diccionario/espanol-ingles/acechar*

[10] "Zoombombing: Una tendencia en ascenso" [en línea]: *https://observatorio.tec.mx/edu-news/zoombombing/*

timidar, humillar o amenazar. Obviamente, dicha difusión de datos (nombres reales o completos, direcciones, números de teléfonos, información financiera, declaraciones de impuestos) es sin consentimiento de la víctima y ésta se siente humillada y exhibida. En sus comienzos, el *doxing* (*dropping documents* o "soltar documentos") se realizaba con el hackeo de correos electrónicos, bases de datos, dispositivos o páginas de internet. Aunque la práctica comenzó en los años 90's del siglo pasado, un caso de lo más emblemático fue el de la entonces candidata a la Presidencia de Estados Unidos, Hillary Clinton en 2016. La ex Primera Dama y ex Secretaria de Estado norteamericana sufrió de un hackeo en sus correos como funcionaria y éstos fueron publicados por WikiLeaks. La falta de cuidado en la seguridad digital de sus dispositivos y la exposición de información sensible, tuvieron un impacto significativo en su campaña.[11]

Años más tarde, otro líder estadounidense, Donald Trump, también sería hackeado en diversas ocasiones. En los supuestos donde están involucrados personajes públicos, el *doxing* ha sido sumamente debatido por si pudiera convertirse en un mecanismo de censura o para negar el acceso a la información o, inclusive, el "derecho a conocer la verdad". Y, a pesar de que las figuras políticas o del entretenimiento, tienen una esfera más amplia de escrutinio público, no por ello, dejan de ser personas cuya intimidad y privacidad merecen reconocimiento y respeto. Sumándose a este debate, sobre el límite entre la protección de datos personales y la libertad de expresión, existen muchos argumentos ya que durante años en México, vimos cómo en la conferencia del entonces Presidente se compartieron datos sensibles de periodistas, partidarios de otros grupos políticos, empresarios y un largo

[11] "Los polémicos emails de la campaña de Hillary Clinton que no se alcanzaron a colar en el debate" [en línea]: *https://www.univision.com/noticias/elecciones-2016/los-polemicos-emails-de-la-campana-de-hillary-clinton-que-no-se-alcanzaron-a-colar-en-el-debate*

etcétera. ¿Podríamos considerar que nuestro exmandatario realizaba doxing o simplemente era una práctica dentro de su discurso político?

Sin embargo, el *doxing* no se constriñe al uso indebido de información derivado del hackeo o los problemas de seguridad, ahora, las modalidades son diferentes como lo son el famoso "siempre hay un tuit" y los "post de ayuda" en comunidades digitales. La primera vertiente, se comenzó a utilizar para exhibir y, especialmente avergonzar, a políticos que habían "tropezado" o se habían contradicho en distintos momentos en el ciberespacio. Por ejemplo, el entonces Jefe de Gobierno, Marcelo Ebrard cometió un error tipográfico en 2012 y hasta la fecha, cada vez que ocurre un evento telúrico, el hashtag (etiqueta) #TenemosSismo vuelve a viralizarse para hacer alusión a su equivocación y, a la vez, informarse y "divertirse".[12] La segunda, se realiza generalmente en comunidades y grupos de Facebook o WhatsApp como "información relevante" para "quemar a alguien", por ejemplo, una empleada del hogar quien presuntamente robó o tuvo alguna conducta "denunciable", o bien, microempresarias que presumiblemente entregaron productos defectuosos o no realizaron servicios aunque los cobraron y, en casos extremos, testimonios sobre personas infieles quienes dañaron a sus parejas o no pagan alimentos a sus hijos. En dichos casos, credenciales de elector, perfiles de redes, lugares de empleo y hasta teléfonos son compartidos sin ningún tipo de limitación.

Lo lamentable es que, al igual que en otros tipos de violencia digital, el tratamiento para las mujeres es diferente que para los hombres. Casos como el del exfutbolista Luis Roberto Alves "Zague" y su entonces esposa, la conductora Paola

[12] "TenemosSismo: esta es la aportación de Marcelo Ebrard a los memes del 19 de septiembre" [en línea]: *https://www.infobae.com/mexico/2023/09/19/tenemossismo-esta-es-la-aportacion-de-marcelo-ebrard-a-los-memes-del-19-de-septiembre/*

Rojas, quienes en 2018 sufrieron por la filtración de un video íntimo del exdeportista que desembocó en su divorcio, muestran que las redes sociales no reaccionan igual entre los distintos géneros. A pesar de que no aparecía en las imágenes y que claramente, el video no era dirigido a su persona, mostrando la infidelidad de su marido, la periodista fue blanco de burlas y memes mientras que el ahora conductor deportivo incluso, "monetizó la viralidad" del contenido, haciendo comerciales al respecto.[13]

¿No debería ser un tema de reflexión que, mientras memes sobre casos como el del excanciller o como del exdeportista son menos agresivos, en la narrativa de las mujeres son más crueles, denostativos y "virales" como los de Itatí Cantoral que cada año es recordada por su polémica interpretación de "La Guadalupana" en la Basílica?[14]

¿Una víctima de *doxeo* no tiene "redención" cuando todos nos podemos equivocar diariamente en nuestras actividades?

¿Es responsable publicar, difundir y hasta comercializar con información que no nos pertenece y que no sabemos si es cierta?

Al ir escalando y normalizando la violencia digital, pensamos que su única forma de expresión es el ***ciberacoso***. Si bien es cierto, como hemos mencionado, no es la única modalidad, sí es aquella con la que se ha detectado en mayor medida. Por ejemplo, en 2023, en nuestro país, 22% de las mujeres mayores de 12 años fueron víctimas de este, lo que es un por-

[13] "¡Impresionanti! Zague se burla de su video íntimo en comercial junto a Campos y el Dr. García" [en línea]: *https://lasillarota.com/deportes/futbol-mx/2019/10/7/impresionanti-zague-se-burla-de-su-video-intimo-en-comercial-junto-campos-el-dr-garcia-201594.html*

[14] "'Nosotros tenemos a Itatí Cantoral': los mejores MEMES para celebrar el regreso de la actriz a Las Mañanitas a La Virgen" [en línea]: *https://www.infobae.com/mexico/2024/12/12/nosotros-tenemos-a-itati-cantoral-los-mejores-memes-para-celebrar-el-regreso-de-la-actriz-a-las-mananitas-a-la-virgen/*

centaje importante si vemos que casi 47 millones del total de usuarios de internet pertenecen a este género.[15]

Podemos definir a grandes rasgos que el acoso es una conducta repetitiva y dañina realizada por una persona —o grupo— hacia otra con el objetivo de intimidarla, humillarla, incomodarla o hacerle de alguna manera daño. No podemos dejar de enfatizar que es un delito. En México, esta conducta delictiva está regulada principalmente por el Derecho Penal. Según el artículo 259 bis del Código Penal Federal, el acoso se define como el acto de "asediar reiteradamente a una persona con fines lascivos, aprovechándose de una posición jerárquica derivada de relaciones laborales, docentes, domésticas o cualquier otra que implique subordinación".[16]

A su vez, existen distintos tipos de acoso como el laboral también conocido como *mobbing,* que consiste en que una o varias personas realizan acciones discriminatorias como insultos, humillaciones o degradación y aislamiento, en repetidas ocasiones, en contra de un colaborador; el acoso callejero que es un comportamiento en público, ofensivo como lo son comentarios vulgares, miradas lascivas, silbidos, gestos obscenos, con el propósito de hacer sentir a la otra persona incómoda e insegura o avergonzada. Y el acoso escolar también conocido como *bullying* que es una conducta repetitiva y dañina, que ocurre en las escuelas y que puede ser verbal, físico o emocional; y por último, el que nos ocupa, cuyas características son:

- Ocurre 24 horas al día, los 7 días de la semana
- Es público

[15] INEGI. Módulo sobre Ciberacoso (MOCIBA) 2023 [en línea]: *https://www.inegi.org.mx/app/saladeprensa/noticia.html?id=9159#:~:text=En%20M%C3%A9xico%2C%20en%202023%2C%2020.9,vivi%C3%B3%20alguna%20situaci%C3%B3n%20de%20ciberacoso*.

[16] Código Penal Federal [en línea]. Disponible en: *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf*

- Denigrante y
- Sus efectos no son sólo virtuales

Los signos de que una persona puede ser víctima de este tipo de delitos son muy claros y podemos detectarlos. Por una parte, vemos ciertos problemas externos como el cambio de desempeño de sus rutinas, la modificación en sus actividades extracurriculares o hobbies y menos concentración y ausentismo. Asimismo, pueden presentarse problemas físicos y mentales como: ansiedad, depresión, aislamiento y problemas para dormir.

Los riesgos del ciberacoso además de aquellos que sufre la víctima son la normalización de cualquier modalidad de violencia, la falta de protocolos por instancias o autoridades y la falta del conocimiento del marco legal.

Algunos consejos que podemos dar para evitar el ciberacoso son:

- Identificarlo tanto en el entorno como en otras instancias
- Señalarle a la víctima que no es su culpa y tratarle con dignidad y respeto
- Establecer límites claros y respetuosos
- Contar con una red de apoyo entre familia y amigos
- Evitar ser blanco fácil al propagar datos personales sin límite y
- Priorizar el bienestar de las personas a través de hábitos digitales sanos.

4. Sextorsión, *grooming* y pornovenganza

En años recientes, una práctica cotidiana entre los más jóvenes es el llamado *sexting* que consiste en el envío de mensajes íntimos eróticos o de carga sexual (“nudes” o “packs”)

por medio de dispositivos móviles. Más allá de la cuestión ética y moral, si el *sexting* se realiza de manera consensuada y entre adultos, desde nuestro particular punto de vista no tendría por qué ser de estudio para la ciencia jurídica. El problema reside cuando se "rompe el círculo de confianza y confidencialidad". Y, por ello, algunos doctrinarios son proclives a analizar al *sexting* como un paso previo a la sextorsión, una manera de ser más vulnerables y quedar expuestos o, erroneamente, señalar que al existir consentimiento de la víctima al compartir imágenes, ésta "conoce los riesgos".[17]

No obstante, periodistas, legisladores, juristas, pedagogos y figuras de crianza, conceptualmente lo confunden con la ***sextorsión***. Este último consiste en el chantaje realizado a partir de la posesión de imágenes o videos de carácter íntimo o sexual con el propósito de obtener dinero, el dominio de la voluntad de la víctima y/o la victimización sexual de la misma. Uno de los casos más emblemáticos de nuestro país fue el de alumnas de la UNAM quienes fueron grabadas en los baños de dicha institución y algunas de ellas pagaron para no ser expuestas en sitios pornográficos.[18]

Por desgracia, conceptos como pornovenganza, acoso sexual digital, violación a la intimidad, robo de material sexual y difusión de material íntimo son cada vez más comunes. Es por ello, que víctimas de éstas han sufrido por la falta de regulación de las mismas. La lucha ha tenido distintos frentes ya que, como en parte hemos señalado, nos falta mucho por construir una sociedad igualitaria, menos violenta y que no revictimice a quien ha sufrido por una conducta nociva.

[17] *Cfr.* "Observatorio de Derecho Público. Sexting y sextorsión: algunas aclaraciones conceptuales" [en línea]: *https://idpbarcelona.net/sexting-y-sextorsion-algunas-aclaraciones-conceptuales/*

[18] "Alumnas de la Facultad de Ciencias (UNAM) acusan que las graban en baños y videos van a sitio porno" [en línea]: *https://www.sinembargo.mx/3538730/alumnas-de-facultad-de-ciencias-unam-acusan-que-las-graban-en-banos-y-videos-van-a-sitio-porno/*

La actriz mexicana, Michelle Vieth fue estigmatizada a través de la prensa cuando se difundió un video íntimo por su exesposo en 2005.[19] Más allá de encabezados, entrevistas de su expareja y el daño a su imagen, la protagonista de telenovelas se enfrentó a un marco legal que no contemplaba este tipo de supuestos y cuyos legisladores no eran sensibles sobre este tipo de violencia.

Fue a través de movilizaciones y campañas de la sociedad civil acompañando a otras víctimas como Ana Baquedano[20] y Olimpia Coral[21] que se reformaron algunos códigos penales locales, muchos años después (2018). Hasta el momento, 28 de 32 entidades federativas han aprobado reformas en ese sentido. No obstante, no existe uniformidad en las medidas. Por ejemplo, en Ciudad de México, las penas pueden ir de 4 a 6 años de privación de la libertad, en entidades como Jalisco y Michoacán hasta 8 años pero en Sinaloa, la sanción oscila de 1 a 3 años de prisión. En 2021, se reformó el Código Penal Federal con penas de 3 a 6 años de prisión. ¿Podemos sentirnos protegidos y, especialmente protegidas, cuando no hay una armonización sobre las penas de una conducta desarrollada además en el ciberespacio donde no existen fronteras geográficas establecidas? ¿Qué mecanismos tendrán las víctimas para saber si acuden a instancias federales o locales?[22]

Más allá del término "pornovenganza", la **violencia digital** consiste en aquellas acciones que atentan contra la integridad, dignidad y privacidad de las personas causándoles un

[19] "Michelle Vieth promueve campaña para penalizar la 'pornovenganza'" [en línea]: *https://www.proceso.com.mx/nacional/2019/8/15/michelle-vieth-promueve-campana-para-penalizar-la-pornovenganza-229516.html*

[20] "Ana Baquedano: la desafiante forma como combate la 'pornovenganza' de la que fue víctima" [en línea]: *https://www.bbc.com/mundo/noticias-internacional-47938198*

[21] "Ni porno, ni venganza: violencia digital, afirma la inspiradora de la Ley Olimpia en México" [en línea]: *https://news.un.org/es/story/2023/03/1519217*

[22] Violencia de género. Ficha técnica: *Ley Olimpia* [en línea]: *http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf*

daño psicológico, económico o sexual y, por ello, la ley tipifica a aquellas conductas que atentan contra la intimidad sexual consistentes en videograbar, audiograbar, fotografiar o elaborar videos reales o simulados, de contenido sexual íntimo, de una persona sin su consentimiento o mediante engaño. Asimismo, exponer, distribuir, exhibir, reproducir, transmitir, comercializar, ofertar, intercambiar y compartir imágenes, audios o videos de contenido sexual íntimo de una persona, a sabiendas de que no existe consentimiento, mediante materiales impresos, correo electrónico, mensajes telefónicos, redes sociales o cualquier medio tecnológico.[23]

Nuestro país ha sido precursor en América Latina —y el mundo— con la Ley Olimpia. Actualmente, Argentina tiene su propia regulación inspirada en México e incluso se le conoce tanto como Ley Belén como Ley Olimpia a las reformas que fueron promulgadas en 2023.[24] Por su parte Honduras y Ecuador se encuentran trabajando en el mismo sentido. También de manera local, en Los Ángeles y Washington se empieza a cabildear al respecto.

Si bien es cierto, que las mujeres somos las principales víctimas de la violencia digital, un grupo aún más vulnerable es el de las menores de edad quienes pueden ser agredidas a través del ***grooming***. Desde hace muchos años, se ha ido popularizando el uso de videojuegos en línea y la presencia en redes por los llamados "nativos digitales". El *grooming* es aquel proceso en el que un adulto crea una relación de confianza con una niña, niño o adolescente a través de plataformas digitales, para después utilizar la información que posee como un mecanismo para acosarlos, controlarlos emocional-

[23] *Cfr.* Violación a la intimidad sexual: Código Penal Federal [en línea]: *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf*

[24] *Cfr. Guía para la prevención de las violencias de género en los entornos digitales* [en línea]: *https://www.argentina.gob.ar/sites/default/files/2022/08/231030-guia_para_la_prevencion_de_las_violencias_de_genero_en_entornos_digitales-v7.pdf*

mente, chantajearlos con fines sexuales o recibir imágenes o videos de desnudos, o audios o contenidos eróticos de la víctima. El adulto generalmente se hace pasar por un niño o adolescente de edad cercana a la víctima, a través de perfiles e imágenes falsas para manipular al menor y vulnerar los controles parentales de las aplicaciones.

Afortunadamente, esta vertiente de la pederastia ya se encuentra contemplada en nuestra legislación federal con una pena de 4 a 8 años de prisión y ha sido ampliamente difundida a través de campañas de prevención. No obstante, aún nos falta una mayor cultura digital y alfabetización ya que, al convertirse en un concepto "coloquial", se usa indiscriminadamente, confundiendo al público en general, por simplificar su significado, a sólo aquellas relaciones en donde las parejas tienen un margen amplio de diferencia en edad, olvidando también que hasta hace relativamente poco tiempo, se permitía por la ley y la sociedad el enlace matrimonial de personas menores de edad, lo cual ha sido modificado afortunadamente.[25]

Por último, pero no por ello menos importante, no podemos dejar de mencionar uno de los grandes temas, desde los inicios del internet, que es la **pornografía infantil**. Desde los años 90's del siglo pasado ya se hablaba de la urgente necesidad de prevenir y erradicar uno de los efectos más detestables del ciberespacio. Cientos de miles de páginas, aplicaciones, plataformas de mensajería y un largo etcétera son visibilizados, con contenido de menores de edad o de personas que no tienen capacidad para oponerse, obviamente, sin autorización. Nuestra legislación, prevé de 7 a 12 años de prisión a quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias personas a realizar actos sexuales

[25] "Ingrid Coronado reacciona a las acusaciones del supuesto 'grooming' de Aleks Syntek hacia su esposa Karen" [en línea]: *https://www.excelsior.com.mx/funcion/ingrid-coronado-reacciona-grooming-aleks-syntek-karen/1632039*

o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de videograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Asimismo, a quien almacene, compre, arriende, el material aún sin fines de comercialización.[26]

Bajo estos supuestos, el caso de la creadora de contenido (influencer) YosStop generó un amplio debate ya que mostró el poco cuidado de quienes están frente a una cámara para compartir o, en este caso, describir y estigmatizar, con tal de ser rebeldes, contestarios o, simplemente, queriendo ser "ocurrentes" con tal de ser "virales". Aunque para algunos era descrito como excesivo el tratamiento que recibió la influencer o para otros que no ameritaba la privación de su libertad, lo cierto es que son temas que el legislador y los jueces no pueden pasar como inadvertidos.[27]

5. Conclusiones y prospectivas

Agradezco profundamente a la Escuela Libre de Derecho, y a cada una de las personas de su comunidad, que han hecho posible la inclusión de este tema en el *Boletín Jurídico Práctico*. Por medio de este breve análisis, haciendo referencia a casos sumamente mediáticos, utilizando fuentes de acceso libre en internet, se ha buscado reflejar la urgente relevancia de conocer, discutir y regular un tema tan trascendental como lo es, la violencia digital. Sin querer ser exhaustivo, el presente tra-

[26] Código Penal Federal [en línea]. *op. cit.*

[27] "Ainara Suárez, tras la liberación de YosStop: 'Decidí darle una segunda oportunidad'" *https://elpais.com/mexico/2021-12-02/ainara-suarez-tras-la-liberacion-de-yosstop-decidi-darle-una-segunda-oportunidad.html*

bajo da un panorama muy general sobre las conductas más frecuentes, pero no son las únicas, tristemente.

La suplantación o el robo de identidad, el daño en la reputación de otra persona, las amenazas directas de daño o de violencia, la trata de personas o el ataque sistemático a grupos, organizaciones o comunidades de mujeres son una realidad. La IA puede ser una enorme herramienta para la automatización de tareas, la transformación de procesos y la creatividad humana. Al igual que ha sucedido con las redes sociales, su popularización puede cambiar la forma en la que comerciamos, socializamos, viajamos y nos divertimos. No obstante, su regulación es un enorme pendiente alrededor del mundo.

La disyuntiva reside en si el panorama actual nos hace sentir que estamos preparados para enfrentar los retos que la IA conllevan. El contar con una cultura de la denuncia, de la verdad, de respaldo a las víctimas, de construir una sociedad más igualitaria, con sistemas legales acordes a la realidad, autoridades sensibles a estos temas y procesos claros y que reflejen la preocupación por dar cauce y solución, está en nuestras manos. Sirva el presente para abrir la discusión.