DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214 

# Desafiando la brecha digital: Derechos y perspectiva de género en la era de internet

## Challenging the digital divide: Rights and gender perspectives in the internet age

**Pilar Badillo Virués* y Arturo Hernández Abascal****

* Licenciada en Derecho por la Universidad Veracruzana y maestra en Derechos Humanos y Juicio de Amparo por la Universidad de Xalapa. Abogada impulsora del conjunto de reformas sobre violencia digital mejor conocida en México como Ley Olimpia, y defensora de espacios digitales libres de violencia para mujeres y niñas.
✉ badillovirues@gmail.com
https://orcid.org/0009-0000-0645-575X

** Licenciado en derecho por la Universidad Veracruzana, maestro en Derecho Constitucional y Amparo por la Universidad Cristóbal Colón y Doctorado en Derecho Constitucional con mención internacional y Cum Laude por la Universidad de Valencia, España. Autor de los libros *¿Qué es la justicia constitucional?* y *Nuevos modelos de justicia constitucional.*
✉ abascalarturo@hotmail.com
https://orcid.org/0009-0006-7883-2722

Recibido: 14.4.2023
Aceptado: 2.10.2023

## Resumen

La internet ha revolucionado la forma en que las personas transmiten y difunden información, creando un entorno donde las líneas entre lo público y lo privado se desdibujan. Esta transformación ha tenido un impacto directo en los derechos humanos, especialmente respecto al derecho a internet, que a veces entra en conflicto con otros derechos debido a la dificultad técnica para regular los contenidos en línea. Problemas como la violencia digital y la trata de personas han destacado la importancia de abordar estas cuestiones desde la perspectiva de los derechos humanos y del derecho comparado. Es crucial que todos los participantes en internet asuman compromisos de regulación y supervisión para proteger los derechos vulnerados, con especial atención a la perspectiva de género. En resumen, la necesidad de equilibrar la libertad en internet con la protección de los derechos humanos es fundamental para garantizar un entorno en línea seguro y justo.

**Palabras clave:** internet, derechos humanos, derecho del ciberespacio, violencia de género.

## Abstract

The Internet has revolutionized the way people transmit and disseminate information, creating an environment where the lines between public and private are

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214

blurred. This transformation has had a direct impact on human rights, especially with respect to the right to the Internet, which sometimes conflicts with other rights due to the technical difficulties in regulating online content. Issues such as digital violence and human trafficking have highlighted the importance of addressing these problems from a human rights and comparative law perspective. It is crucial that all Internet participants assume regulatory and supervisory commitments to protect violated rights, with special attention to the gender perspective. In short, the need to balance Internet freedom with the protection of human rights is fundamental to ensuring a safe and fair online environment.
**Keywords:** Internet, human rights, cyberspace law, gender-based violence

## Introducción

La regulación o no de la Internet no es un tema nuevo, pero no por eso deja de ser de actualidad y de la mayor importancia dada la cantidad de violaciones a la privacidad que se generan constantemente en la red, vulnerando especialmente a las mujeres. Es por lo que al abordar este tema se comienza por explicar qué son las TIC.

En un segundo momento se toca el tema del rompimiento de la línea, siempre muy delgada, entre lo público y lo privado, al participar en el funcionamiento de la red un número excesivo de personas y una cantidad inmensa de empresas, así como gobiernos, en un sistema tan fragmentado y en constante crecimiento a partir del Derecho a la Internet que nos lleva a la conclusión de que regular del todo el flujo de información es técnica y jurídicamente complejo debido a la gran cantidad de participantes en la construcción y operación de la World Wide Web.

No obstante, ponemos de relieve que la violencia digital obliga a generar compromisos y adecuaciones legislativas, que si bien no controlarán del todo algo tan caótico como es el flujo de miles de millones de interacciones diarias, desde el punto de vista ético y por supuesto práctico, la búsqueda de reducción de violaciones constantes de derechos merece la pena, dado el inmenso número de mujeres que son víctimas de la mencionada violencia digital. En ese marco, un auténtico consentimiento informado puede ser un buen principio. La necesidad de un acuerdo global de protección escalable es tan urgente como lo es la lucha por la protección de todas las personas, en particular de aquellas que por cuestiones de género se encuentran en una situación de especial vulnerabilidad.

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214 

## Las tecnologías de la información y la comunicación (TIC)

Es importante comenzar haciendo mención de Arpanet, una red de comunicaciones producida por la Agencia de Proyectos de Investigación Avanzada de los Estados Unidos (ARPA), evolucionando hasta convertirse en Internet. Fue en 1990 cuando con la web y la invención de navegadores que eran más alcanzables y sencillos para el público en general se logró la popularización a nivel mundial.

TIC es un término amplio que implica tecnologías diversas que han ido evolucionando. Su expansión se acrecentó con la llegada de la internet y la digitalización de la información en las décadas del siglo XX y principios del XXI (Aranda, 2004). Los procesos y productos de las TIC permiten procesar, transmitir y difundir información de manera instantánea y masiva, como pueden ser: computadoras, teléfonos celulares, cables de fibra óptica, satélites, programas, aplicaciones y cualquier otra cosa relacionada con el universo virtual, cuyo eje es por supuesto internet.

La diferencia entre las viejas tecnologías (como la imprenta, la radio o los teléfonos fijos) y las nuevas tecnologías es fundamentalmente la posibilidad de realizar una comunicación instantánea de texto, imágenes y videos desde cualquier punto del globo.

### Tabla 1

| Antiguas TIC | TIC |
|---|---|
| Radio | Software |
| Teléfono | Hardware |
| Televisión | Funciones de la internet |
| Telégrafo | |
| El salto de unas a otras se da por la internet. | |

**Fuente:** Adaptado de Ortí (2011).

Características de las tecnologías de la información y la comunicación:

1. **Inmaterialidad**. Se almacenan grandes cantidades de información remotamente, sin necesidad de dispositivos propios.
2. **Instantaneidad**. La información y la comunicación fluyen de forma instantánea por el mundo.
3. **Interactividad.** Permiten la comunicación bidireccional entre personas o grupos sin importar la distancia entre ellos.

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214

Es así que la irrupción de Internet permitió el advenimiento de la era del conocimiento y originó una gran cantidad de elementos materiales e inmateriales, que en su momento se llamaron *nuevas tecnologías de la información y la comunicación*, ahora por su consolidación llamadas únicamente TIC, que formaron un mundo virtual que interactúa con el mundo real a tal grado que se ha difuminado por completo la línea divisoria entre ambos y genera tensiones sociales y daños personales para nada menores.

El rompimiento de una línea clara entre lo público y lo privado compromete a sectores de la población que comparten su información personal sin contar con una idea clara de los riesgos, debido a una falta clara de regulación y educación digital. Como veremos más adelante, las empresas simplemente no asumen responsabilidad alguna.

## Entre lo público y lo privado

Empecemos, de ser posible, por explicar la diferencia entre lo público y lo privado, tomando en cuenta que entre lo privado también se encuentra lo íntimo, un posible espacio definible de forma independiente. En un primer acercamiento a Arendt (1958), podemos señalar que los antiguos griegos diferenciaban la organización política (pública) de la asociación natural en el hogar y en la familia (privada). Con el tiempo se empezó a entender lo público como aquello relacionado con el Estado y lo privado constituido por la vida de las personas en una esfera no relacionada con aquel.

En el presente trabajo distinguiremos lo público de lo privado basándonos en el escenario de acción y consentimiento: por una parte, la vida de las personas que es de dominio público por la forma en que la comunican o por su consentimiento para hacerla pública; por otra, los acontecimientos personales o íntimos que la persona dispone que no pertenezcan a la esfera pública, ya sea por la forma en que los comunican o por su falta de consentimiento.

Dicho lo anterior expongamos, con un ejercicio imaginativo, la complejidad resultante de separar lo público de lo privado en la época de las TIC:

Está usted sentado con el teléfono celular en la mano y recibe un mensaje de texto de WhatsApp (WA) de un amigo que se encuentra en Madrid, entonces usted le contesta el mensaje e inician una conversación, incluyendo por supuesto expresiones o temas que no desearía que se hicieran públicos. Usted no está preocupado por eso, dado que la virtualidad y la realidad ya son una sola cosa en su vida cotidiana, y siente que está hablando, o escribiendo para ser más exacto, en privado, como si estuviera en persona frente a su amigo.

Intentemos en todo caso seguir la ruta de la «privacidad» de sus mensajes: para empezar, está su teléfono mismo que guarda en algún lugar desconocido dentro de sí todo lo que usted y su amigo están escribiendo, además de subirlo a algún lugar llamado nube donde lo almacena. Ya llevamos cuatro lugares o empresas distintas que tuvieron

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214 

acceso a sus mensajes y apenas estamos empezando, a saber: WA, su teléfono celular, la empresa que fabricó su teléfono y la nube, donde quiera que esté (en un servidor en Singapur, recorriendo un cable en el fondo del mar o vaya usted a saber dónde).

Volvamos entonces a los pasos siguientes: usted cuenta con un proveedor de internet el cual toma su mensaje y lo envía a otro proveedor y este a otro y ese otro a alguno más, partiendo de su ciudad, y seguramente atravesando el fondo del mar, para llegar a alguna costa española y seguir una ruta de proveedores distintos hasta llegar al proveedor de su amigo, al teléfono de su amigo, a la empresa que fabrica el teléfono de su amigo y a la nube donde se almacenan los mensajes de su amigo.

Difícil saber exactamente por cuántas «manos» pasó su mensaje, ¿diez?, ¿veinte? Pero no se preocupe, su empresa de mensajería le dijo que sus mensajes están cifrados de extremo a extremo, cosa que usted no entiende, pero que seguramente lo deja dormir tranquilo.

Esas diez o veinte empresas o gobiernos (dado que en algunos casos los gobiernos son dueños de alguno de los cables submarinos para internet) tienen sus propios términos y condiciones, que usted suele aceptar sin leer, como es el caso de WA, que hace responsable al usuario de su propia cuenta y es a él al que le prohíbe difundir contenido ilegal, aunque por supuesto los intermediarios por los que pasa su mensaje ni eso tienen, además de pasar por países con diferentes leyes, en el fondo del mar en aguas internacionales y muchos proveedores tienen su matriz en alguna isla de algún lugar del mundo, que probablemente ni leyes en la materia tenga.

Lo anterior sin contar con la infinidad de hackers, instituciones de gobierno, empresas de opinión y hasta gente conocida que pudiera tener interés en sus mensajes o imágenes enviadas. Pero no se preocupe, su empresa de mensajería le dijo que sus mensajes están cifrados de extremo a extremo, por lo que usted no debería preocuparse de que lo privado se vuelva público. Por cierto, se me olvidaba que también le pueden robar su teléfono.

Ahora imagine lo anterior enviando a su pareja una foto o video íntimos, poniéndose en riesgo, no solo por la posible traición a su confianza por parte del destinatario, sino sobre todo por la dificultad de contar con una seguridad absoluta en la protección de su intimidad. La delgada línea entre lo público y lo privado ha desparecido.

## Derecho a internet

Todas las personas tienen derecho a usar internet de manera segura y que el mundo *online* sea libre de violencia, sin embargo, las medidas legales a nivel mundial se han visto rebasadas ante el crecimiento de las TIC. La Organización de las Naciones Unidas (ONU) reconoció el derecho a internet como derecho humano. La Agenda 2030 marca una pauta importante ya que reconoce el acelerador potencial del progreso humano

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214

mediante las Tecnologías de la Información y Comunicación y la interconectividad global. Internet abre oportunidades, pero al mismo tiempo crea problemáticas en torno a nuestra seguridad en todos los sentidos.

Derivado de lo anterior, una de las problemáticas existentes en el contexto social y jurídico es que no hay una correcta comprensión o asimilación de las distintas amenazas que han causado vacíos para la protección de las personas que habitamos ambas realidades expuestas. Además de la poca aceptación del sector privado o público, según sea el caso, en la responsabilidad que comparte.

Por otra parte, la necesidad urgente de cerrar la brecha digital existente entre géneros se contempló entre las preocupaciones de la ONU, incluyendo la cooperación internacional para trabajar por las disparidades en el acceso a las TIC en donde todas las personas tengan acceso sin distinciones y se promueva el alfabetismo digital.

En São Paulo (Brasil) se celebró la Reunión Global de Múltiples Partes Interesadas sobre el Futuro de la Gobernanza de Internet, celebrada en 2014. En esta se mencionó la necesidad de que los derechos que tienen las personas fuera de línea también deban protegerse dentro de ella, particularmente aquellos relacionados con la no violencia.

La *Resolución sobre la promoción, protección y disfrute de los derechos humanos en internet* toca el tema de los actores del sector privado y especifica que deben seguir los lineamientos del derecho internacional de derechos humanos como base no solo para la moderación de contenido, sino también para la confidencialidad de las comunicaciones digitales (medidas de codificación y anonimato). Todo lo dicho con la intención de disfrutar del derecho a la privacidad, libertad de expresión, libertad de reunión pacífica y asociación.

El incremento de usuarios de internet a nivel mundial tiene entre otras consecuencias el aumento a la vulneración de la seguridad digital cuando no existe alfabetización en la materia que incluya derechos al respecto. La Unión Internacional de Telecomunicaciones en el informe de 2019 tiene el registro de que solo el 48% de las mujeres del mundo tenían acceso a internet, en comparación con el 55% de los hombres. Esta diferencia de acceso impacta claramente en el tema de la alfabetización digital (Unión Internacional de Telecomunicaciones [UIT], 2019).

Los marcos de regulación son aún carentes para el gran impacto que generan los avances tecnológicos. Pongamos como ejemplo una comparativa entre España y México en la regulación del tema: España cuenta con la Ley de Servicios de la Sociedad de la Información y del comercio electrónico (LSSI, España, 2002) que regula actividades comerciales en internet y establece procedimientos sancionadores. El consentimiento expreso es uno de los aspectos relevantes en la LSSI, así como en la Ley Orgánica de Protección de Datos. A título de ejemplo, cuando recibes *spam* o información no deseada se establece que se vulnera la prestación de consentimiento (artículos 21 y 22 LSSI) y se puede enviar el caso a la Agencia Española de Protección de Datos (AEPD), que aplica sanciones calificadas como leves, graves y muy graves que van de los 30.000 a los

600.000 euros. La inspección y el procedimiento sancionador está a cargo del Ministerio de Energía, Turismo y Agenda Digital.

En los artículos 14 al 17 de la LSSI (España, 2002) se describe la responsabilidad de los prestadores de servicios de intermediación, dividiendo entre los que se dedican a la provisión de acceso, almacenamiento de datos, instrumentos de búsqueda, etcétera, teniendo en cuenta que existe una imposibilidad práctica de control legal de los contenidos que estos almacenan, recomiendan o transmiten. Se establece como norma general que se exime de responsabilidad a los prestadores de servicios si se cumplen dos condiciones: 1) que no se tenga conocimiento específico de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, y 2) que cuando se tenga ese conocimiento se actúe con diligencia para retirar los datos o hacer imposible el acceso a ellos. En particular, el contenido íntimo sexual publicado sin consentimiento implica responsabilidad cuando se tiene «conocimiento efectivo» de la existencia y la ilegalidad y no se actúa con diligencia para retirarlo o impedir el acceso.

En México (2010) se cuenta con la Ley Federal de Protección de Protección de Datos Personales en Posesión de los Particulares, que contempla de manera general a los derechos de Acceso, Rectificación, Cancelación y Oposición (derechos ARCO). Una de las diferencias principales es que la Ley Orgánica de Protección de Datos en España (2018) contiene un apartado especial denominado «Garantía de los derechos digitales» que tiene como base los derechos y libertades que se establecen en la era digital a partir de su Constitución, Tratados y Convenios Internacionales en donde España es parte. Se agota en cierta medida una de las responsabilidades de los Estados que, como ya se mencionó anteriormente, es la alfabetización digital.

Se informa en esta Ley acerca del derecho a la neutralidad de internet, acceso universal, seguridad digital, educación digital, protección de menores, rectificación, actualización de informaciones en medios de comunicación digitales, derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, derecho a la desconexión digital en el ámbito laboral, derecho a la intimidad frente al uso de dispositivos de video vigilancia y de grabación de sonidos en el lugar de trabajo, derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, derechos digitales en la negociación colectiva, derecho al olvido en búsquedas de Internet y en servicios de redes sociales o equivalentes, derecho de portabilidad en servicios de redes sociales y servicios equivalentes, además del derecho al testamento digital.

La Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (Endutih) 2021, que abarca personas de seis años o más que residen en el territorio nacional, registró en México 88:562.249 usuarios de internet en 2021.

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214

**Tabla 2. Usuarios de TIC en México de 2015 a 2021**

| | Usuarios de computadora | | Usuarios de internet | | Usuarios de telefonía celular | |
|---|---|---|---|---|---|---|
| **Año** | **Absolutos** | **%** | **Absolutos** | **%** | **Absolutos** | **%** |
| 2015 | 55.735.713 | 51,3 | 62.448.892 | 57,4 | 77.711.203 | 71,5 |
| 2016 | 51.708.327 | 47,0 | 65.520.817 | 59,5 | 81.027.569 | 73,6 |
| 2017 | 49.826.347 | 45,2 | 70.289.609 | 63,7 | 79.587.494 | 72,1 |
| 2018 | 49.935.658 | 44,7 | 73.142.199 | 65,5 | 81.865.019 | 73,3 |
| 2019 | 48.362.012 | 42,4 | 79.489.450 | 69,6 | 85.549.900 | 74,9 |
| 2020 | 43.534.080 | 37,5 | 82.978.847 | 71,5 | 87.218.465 | 75,1 |
| 2021 | 43.844.751 | 37,4 | 88.562.249 | 75,6 | 91.731.856 | 78,3 |

**Nota.** Tomado del Instituto Nacional de Estadística y Geografía (INEG, 2021).

La materialización de un internet seguro para todas las personas que no incurra en ninguna violación a los derechos humanos implicaría la adopción, aplicación y reforma progresiva de leyes, reglamentos, política y medidas relativas a la protección en línea.

## Violencia digital

La violencia digital es la extensión de la violencia *offline*. Es un fenómeno común, desgraciadamente, en donde las mujeres y niñas son las principales víctimas. La Asociación para el Progreso de las Comunicaciones definió la violencia en línea contra las mujeres como los actos de violencia por razones de género que son cometidos, instigados o agravados, en parte o en su totalidad, por el uso de tecnologías de la información y las comunicaciones (TIC), como teléfonos móviles, internet, plataformas de redes sociales y correo electrónico. Se destacan que estos actos ocasionan o pueden ocasionar daño o sufrimiento físico, sexual, psicológico o económico (Asociación para el Progreso de las Comunicaciones [APC], 2015). Es importante para un análisis concreto de los casos y su tratamiento la perspectiva de la interseccionalidad, entendida como una herramienta de análisis útil para visibilizar los diferentes privilegios y opresiones existentes.

Por su parte, en el Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos de 2018 se mencionó que las mujeres son las principales víctimas en todo el mundo de esta forma de violencia. Los estudios han comprobado que 90% de las personas afectadas por la distribución digital de imágenes íntimas sin consentimiento son mujeres (Naciones Unidas, 2018, p. 24).

Otro sector vulnerado ante este tipo de violencia es el LGBTIQ+, siendo víctimas comúnmente de ciberacoso, el cual se suele manifestar como hostigamiento contra la

diversidad sexual por no cumplir con los patrones heteronormativos de la sociedad. En España se tiene el registro de que el 57,4% de las víctimas de ciberacoso pertenecían a la comunidad LGBTIQ+ en 2014 (Martxueta y Etxeberria, 2014, p. 123).

La violencia en línea ha ido transformándose a medida que la internet y las herramientas tecnológicas avanzan y se relacionan «normalmente» en nuestras vidas. Es un fenómeno a escala, en muchas ocasiones comienza con intercambios en redes sociales y culmina en encuentros donde se comente violencia sexual, secuestros o, en algunas ocasiones, en trata de personas. La anonimidad abre la posibilidad de cometer abusos desde cualquier lugar a través de las TIC. Tiene a su favor la rápida expansión, la permanencia de los contenidos, la replicabilidad y el alcance, facilitando el contacto de los victimarios y las víctimas (Martxueta y Etxeberria, 2014, p. 123).

Claramente las víctimas de esta violencia se encuentran con repercusiones en su vida social que afectan gravemente el estado emocional. En casos de ciberhostigamiento, así como de difusión de contenido íntimo sexual, pueden experimentar depresión, ansiedad, estrés, miedo o ataques de pánico, e incluso llegar al suicidio. La injusticia social, jurídica y tecnológica lleva de la mano efectos perjudiciales para la vida misma.

El Frente Nacional para la Sororidad (FNS) ha trabajado arduamente por el reconocimiento del problema de la violencia digital en México, Argentina y en otras partes de Latinoamérica. Principalmente han señalado que los términos utilizados para nombrar a esta violencia sean correctos y se deje de revictimizar a las personas.

El primer término que es necesario entender es *sexting* o sexteo, una práctica que implica la generación e intercambio de material sexualmente explícito (United Nations Office on Drugs and Crime [UNODC], 2019). Se convirtió en una práctica común por quienes utilizan la tecnología como medio de expresión sexual. En algunas ocasiones se nombra al *sexting* como el delito, pero esto no es correcto. No tiene la culpa quien decide compartir imágenes, videos o audios propios de contenido íntimo sexual, sino quien decide compartirlas sin el consentimiento de la otra persona. Además de la responsabilidad que tienen el sector privado y el Estado de no contar con un mecanismo eficaz para la persecución de este delito llamado genéricamente violación a la intimidad sexual.

Entonces, la práctica en sí misma no tiene que ver con una conducta punible. Tampoco es correcto utilizar el término *pornovenganza,* ya que se oculta el componente no consensual de la conducta, y hablar de *venganza* es revictimizar a las personas que sufren esta agresión.

La llamada Ley Olimpia en México se compone por un conjunto de reformas legales con el fin de definir, prevenir y sancionar la violencia digital a través de la violación a la intimidad sexual. Ha sido una lucha colectiva de transformaciones sociales y jurídicas que busca crear espacios *online* seguros para todas las personas. Entre los logros están la sanción de la difusión no consentida de contenido íntimo y el reconocimiento de la violencia digital como una modalidad en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (LGAMVLV). Descrita a continuación:

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214

> Artículo 20 *Quáter***.** Violencia digital es 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.
>
> Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación (México, 2024).

En 2018 el Frente Nacional para la Sororidad, en el trabajo de investigación para lograr la tipificación de este delito en el Estado de Veracruz, en México, detectó que en el estado operan 45 mercados de explotación digital, particularmente en Facebook y Twitter, plataformas que han publicado hasta 3.055 videos sexuales sin consentimiento de mujeres y menores de edad. Estas publicaciones generan diferentes tipos de violencia digital como la ciberpersecución, la extorsión y la trata virtual de personas. Ante esto, las víctimas sufren vulneraciones en el aspecto emocional y psicológico, como ya se mencionó anteriormente, al ser sometidas a reproche social y burlas.

Como otra vertiente, la trata virtual ha sido especialmente analizada por el FNS. Olimpia Coral Melo, activista y fundadora del Frente, ha explicado que la *trata virtual de personas* comienza con el robo de la identidad de alguien, normalmente una mujer. Luego se crea un perfil apócrifo en el cual se lucra con la promesa de que la persona cumplirá con servicios sexuales. La situación se agrava cuando los delincuentes presentan imágenes e información personal de la víctima.

Desde otro ángulo del mismo fenómeno delictivo, Ana Gabriela Rojas, corresponsal de *BBC Mundo* en México, el 14 de enero de 2020 publicó el reportaje «Etnoporno, la explotación sexual de mujeres indígenas en videos pornográficos en México», donde narraba dos casos de este tipo. Mencionando, además, que las activistas se encontraban denunciando que es cada vez más común el *etnoporno,* un tipo de pornografía que usa como fetiche a mujeres y niñas indígenas, y que son por ello víctimas de abusos (Rojas, 2020).

Se necesita la contribución de autoridades, empresas privadas de las TIC, sector académico y sociedad civil en general para intervenir en las políticas nacionales e internacionales de ciberseguridad. Es indispensable la protección de los derechos humanos en la vida *online*.

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214 

## Desafíos de la regulación y responsabilidad: acercándonos a una posible solución

Uno de los problemas es que, al ser una suma de sistemas —un metasistema se le dice— con un protocolo común, nadie es propietario de la red, no habiendo por tanto un control centralizado. Su funcionamiento depende, en parte, de ingenieros que definen cuestiones técnicas para su implementación, desde el RFC de 1958 (Carpenter, 1996).

Como ya se ha señalado, los fabricantes de aditamentos que usan internet, los que almacenan datos, los que diseñan y poseen aplicaciones como redes sociales, los proveedores del servicio directo a los usuarios, los que prestan ese servicio a los anteriores y por supuesto los miles de millones de usuarios, ubicados todos los mencionados a lo largo y ancho del mundo, con diferentes regulaciones nacionales y hasta con distintas visiones culturales integran una «comunidad» con interacciones complejas. Aunado a lo anterior, el «control» de lo que se publica y se ve en la web ha pasado a algoritmos creados con diferentes intencionalidades, pero básicamente para definir los contenidos a los que tienen alcance los usuarios independientemente de su deseo y autorización expresa.

Utilicemos dos ejemplos: Facebook y WA. En el primer caso, con 2900 millones de usuarios, genera 4 *petabytes* —millones de *gigabytes*— de datos por día. Hay alrededor de 300 *petabytes* de datos almacenados en distintas partes, no siempre identificables. Cada 60 segundos se publican 510.000 comentarios, se actualizan 293.000 estados, se dan 4000 millones de *likes* y se suben 136.000 fotos (Wiener y Bronson, 2014). WA tiene en la actualidad más de 2000 millones de usuarios y cada día se envían más de 100.000 millones de mensajes a través de dicha aplicación (Moreno, 2020). Por lo anterior «Su control *a priori* resulta totalmente imposible, y exigir a los responsables de dichos *websites* que vigilen con carácter previo los contenidos que alojan supondría abocarles inmediatamente al colapso» (Martínez Otero, 2011, p. 13).

La abrumadora mayoría de los contenidos que circulan por internet son producidos por los propios usuarios, no por las empresas que participan en cada sistema integrante de la red. «Los proveedores de servicios son responsables por los contenidos que elaboren o que se hayan elaborado por cuenta suya. Por el contrario, no serán responsables por el ejercicio de actividades de intermediación» (Pérez Velasco y Conde Castejón, 2002, p. 123). La información de internet se trasmite preponderantemente por una red de *backbones* submarina gigante que cruza los océanos, auténticas autopistas de datos. Pertenecen a empresas privadas y gobiernos, aunque actualmente la mayor parte del control está en manos de Google, Facebook, Amazon y Microsoft.

Pero ¿no se puede hacer nada para evitar la violación de derechos de millones de personas diariamente? Consideramos que las siguientes medidas, implementadas de manera coordinada y colaborativa a nivel global, pueden contribuir significativamente a

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214

prevenir la violación de derechos en Internet y a proteger a millones de personas en su uso cotidiano de la red.

1. **Educación digital.** La comprensión de los derechos en línea, los riesgos, las medidas de protección disponibles y el uso responsable de los medios que nos proporciona la web para comunicarnos debe generalizarse en los sistemas educativos públicos y privados del mundo, dado que, como se ha dicho, buena parte de los contenidos que circulan en la red son producidos por los propios usuarios.
2. **Desarrollo de tecnologías éticas.** Fomentar la investigación y el desarrollo de tecnologías que incorporen principios éticos y respeten los derechos humanos desde su diseño, poniendo particular atención en el diseño y puesta en marcha de algoritmos que normalmente obedecen a intereses comerciales.
3. **Regulación y cumplimiento.** Contar con marcos regulatorios cuidadosamente elaborados y actualizados permanentemente que protejan los derechos en línea, garantizando su cumplimiento mediante sanciones efectivas, poniendo énfasis en la prevención.
4. **Transparencia y rendición de cuentas.** Exigir transparencia por parte de las plataformas digitales en cuanto a sus políticas de datos y moderación de contenido y asegurar que sean responsables por sus acciones.
5. **Participación ciudadana.** Integrar a la sociedad civil en el diseño e implementación de políticas relacionadas con Internet y los derechos digitales.
6. **Cooperación internacional.** Promover la cooperación entre países y organizaciones internacionales para abordar los desafíos transnacionales en materia de derechos en línea. Resaltando la importancia de una adecuada coordinación entre órganos de seguridad actuantes a nivel internacional y nacional.
7. **Desarrollo de herramientas de denuncia y protección.** Facilitar el acceso a mecanismos de denuncia y protección en línea para las personas afectadas por violaciones de derechos, asegurando que dichos mecanismos sean efectivos y accesibles.

## Conclusiones

Los estudios expuestos están lejos de arrojar resultados que concluyan exitosamente sobre la manera de regular y supervisar el flujo de datos inconmensurable que circula por la red en todo momento. Aun cuando las aproximaciones teóricas y los análisis son imprescindibles, es escasa la integración de decisiones políticas. De la profundidad y la seriedad con que se tomen en cada sociedad depende la implementación de líneas de acción eficaces.

La violación de derechos *online* a sectores vulnerables de la población, particularmente desde la perspectiva de género, es un hecho constante e impune en la mayor parte de los casos. Es posible, si no eliminar por completo, por lo menos reducir notablemente el número de víctimas por esta falta de regulación y supervisión a través de modificaciones a normas legales y establecimiento de compromisos serios por parte de todos los involucrados en el proceso. Se han tenido avances gracias a luchas colectivas y la transformación de asuntos de interés público en actuaciones jurídicas, pedagógicas y sociales que deben continuar para su garantía.

La búsqueda de mecanismos que obliguen a las empresas a notificar claramente, en un lugar visible y de forma permanente que no existe la comunicación *online* totalmente invulnerable y el compromiso de los gobiernos a legislar en ese sentido y en la búsqueda constante de seguridad del usuario puede atemperar tan grave lesión a los derechos de sectores vulnerables.

## Referencias bibliográficas

Aranda, V. T. (2004). *Historia y evolución de Internet*. Asociación de Autores Científico-Técnicos y Académicos. https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf

Arendt, H. (1958). *The human condition.* Chicago, EUA: The University of Chicago Press.

Asociación para el Progreso de las Comunicaciones. (2015). *De la impunidad a la justicia: Explorando soluciones corporativas y legales para la violencia hacia las mujeres relacionada con la tecnología*. https://www.genderit.org/sites/ default/files/csw_map_1_1.pdf

Carpenter, B. (1995). *Architectural principles of the Internet*. Internet Architecture Board.

España. (2002, 11 de julio). Ley de servicios de la sociedad de la información y de comercio electrónico. *Boletín Oficial del Estado*, 13758. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

España. (2018, 5 de diciembre). Ley orgánica de protección de datos personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 16673. https://www.boe.es/eli/es/lo/2018/12/05/3/con

Instituto Nacional de Estadística y Geografía. (2021). *Encuesta nacional sobre disponibilidad y uso de tecnologías de la información en los hogares: Base de datos 2021* [Conjunto de datos]. https://www.inegi.org.mx/app/descarga/?p=3193&ag=00

Martínez Otero, J. (2011). Mensaje publicitario y menores de edad: previsiones legales y códigos de autorregulación. En Fundación COSO, *Actas del 9.º Congreso Internacional de Ética y Derecho de la Información: La responsabilidad ética y social de las empresas informativas*.

DOI 10.29192/claeh.43.1.15
CUADERNOS DEL CLAEH · Segunda serie, año 43, n.º 119, 2024-1, ISSN 0797-6062 · ISSN [en línea] 2393-5979 · pp. 201-214

Martxueta, A., y Etxeberria, J. (2014). Claves para atender la diversidad afectivo-sexual en el contexto educativo desde un enfoque global escolar. *Revista Española de Orientación y Psicopedagogía*, *25*(3), 121-128. https://www.redalyc.org/pdf/3382/338233061009.pdf

México. (2010, 5 de julio). *Ley federal de protección de protección de datos*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

México. (2024, 26 de enero). *Ley general de acceso de las mujeres a una vida libre de violencia*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf

Moreno, M. (2020, 12 de febrero). *WhatsApp supera los 2.000 millones de usuarios*. Trecebits. https://www.trecebits.com/2020/02/12/whatsapp-supera-los-2-000-millones-de-usuarios/

Naciones Unidas. (2018). *Informe de la relatora especial de las Naciones Unidas sobre la violencia contra la mujer, sus causas y consecuencias: Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*. https://documents.un.org/doc/undoc/gen/g18/184/61/pdf/g1818461.pdf

Ortí, C. B. (2011). *Las tecnologías de la información y comunicación (TIC)*. Universidad de Valencia.

Pérez Velasco, M. M., y Conde Castejón, J. (2002). Regulación versus autorregulación en Internet y los nuevos servicios de comunicación. En M. Fernández Ordóñez, J. Cremades García, y R. Illescas Ortiz (Coords.), *Régimen jurídico de Internet* (pp. 119-128). Wolters Kluwer España.

Rojas, A. (2020, 14 de enero). *Etnoporno: la explotación sexual de mujeres indígenas en videos pornográficos en México*. BBC Mundo. https://www.bbc.com/mundo/noticias-america-latina48699964

Unión Internacional de Telecomunicaciones. (2019). *Measuring digital development: Facts and figures 2019*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

United Nations Office on Drugs and Crime. (2019). *Study on the effects of new information technologies on the abuse and exploitation of children: Cybercrime*. https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

Wiener, J., y Bronson, N. (2014, 22 de octubre). *Facebook's top open data problems*. Meta. https://research.facebook.com/blog/2014/10/facebook-s-top-open-data-problems/