

WEBINARIO

ESTRATEGIAS DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS PARA LUCHAR CONTRA LA VIOLENCIA DIGITAL EN IBEROAMÉRICA CON UN ENFOQUE DE GÉNERO

4 DE MARZO DE 2021



*Ponentes del webinar
"Estrategias de las autoridades
de protección de datos para
luchar contra la violencia en
Iberoamérica con un enfoque
de género"*



Contenido

¿Cuál es la situación actual respecto a la violencia de género digital?	5
Abordaje desde la óptica preventiva: Educación Digital	6
Cultura de la prevención para combatir la violencia digital	7
¿Introducir una materia ajena a la currícula tradicional?.....	9
Los datos colectivos como bienes comunes	10
El Canal Prioritario de la AEPD: los acuerdos con las plataformas de Internet	11
Estrategia regional de la RIPD con apoyo de la Unión Europea	13
La alianza entre organizaciones para una lucha en conjunto contra la violencia digital con una perspectiva de género	14
Estrategias institucionales y mecanismos de derechos humanos	16
Activismo en Latinoamérica: los retos de la región	17
La experiencia de violencia de género digital de Olimpia y su lucha por combatirla.....	18
Estereotipos sexistas y violencia contra mujeres en el ámbito informativo del deporte	20
Conclusiones: colaboración de las autoridades de protección de datos	21
Declaración de la Red Iberoamericana de Protección de Datos (RIPD) contra la Violencia Digital en mujeres y niñas	22

Autoridades de Protección de datos, organizaciones internacionales y sociedad civil, junto con la Red Iberoamericana de Protección de Datos, alertan sobre las diversas formas de violencia de género en Internet y las diversas estrategias dispuestas para erradicarla.

La RIPD se compromete a combatir de forma activa cualquier tipo de violencia digital que involucre tratamiento de datos personales, en especial la realizada contra las mujeres, niñas y adolescentes y emite una Declaración.



¿Cuál es la situación actual respecto a la violencia de género digital?

A pesar de sus enormes ventajas, en el ámbito de Internet y de las TIC tienden a reproducirse las estructuras sociales, más amplias incluso, en las que se manifiestan las diversas formas de violencia contra la mujer, al tiempo que aparecen otras nuevas, propias del entorno en línea. La extensión y el uso intensivo de dispositivos móviles e Internet, redes sociales, servicios como los de mensajería instantánea o de geolocalización y datos personales (fotos, videos, etc.) han servido de cauce para la proliferación de conductas de violencia contra la mujer, comprobándose que, en muchas ocasiones, Internet y sus servicios y aplicaciones se han utilizado con la finalidad de controlar, amedrentar, acosar, humillar y chantajear a las mujeres, constituyendo un instrumento cada vez más utilizado para dichos fines.

En este sentido, las características de las TIC han dado lugar a nuevas amenazas para la mujer víctima de violencia, derivadas, entre otras, de la velocidad con la que la información se difunde en este entorno,

la posibilidad de acceder a la información gracias a los motores de búsqueda y las dificultades para su eliminación. La viralidad, perdurabilidad y falta de olvido en el entorno en línea entrañan nuevas situaciones de riesgo, como pueden ser el acceso y la divulgación sin consentimiento de información privada y sensible, de fotografías o videos de carácter íntimo; la vigilancia y monitoreo de actividades en línea; daños a la reputación de la mujer, ya sea a través de lo que se escribe de ella o la utilización de prácticas como *deepfake*; las conductas conocidas como "sextorsión" y el acoso sexual en línea.

Por todo ello, las mujeres se ven especialmente afectadas por estos fenómenos de violencia en línea, sufriendo como consecuencia daños físicos, psicológicos y económicos. La Agenda 2030 de Naciones Unidas recoge 17 Objetivos de Desarrollo Sostenible (ODS), 169 Metas, 232 Indicadores, centrados en la persona, el planeta, la prosperidad, la paz y las alianzas. El ODS 5, "Lograr la igualdad de género y empoderar

a todas las mujeres y a las niñas", busca conseguir la igualdad real de mujeres y hombres. En concreto, la meta 5.b se refiere expresamente a la mejora en el uso de la tecnología instrumental, en particular la tecnología de la información y las comunicaciones, para promover el empoderamiento de las mujeres.

Para las entidades integrantes de la Red Iberoamericana de Protección de Datos, resulta de especial importancia atender cada uno de sus objetivos, entre los que destacan promover la cooperación, el diálogo y el uso compartido de la información para el desarrollo de iniciativas y políticas de protección de datos; fomentar políticas, tecnologías y metodologías que permitan garantizar el derecho fundamental a la protección de datos; e impulsar programas de capacitación entre sus miembros, así como la información a la ciudadanía sobre el uso y destino de sus datos personales, y de los derechos que pueden ejercer frente al manejo de los mismos.



Abordaje desde la óptica preventiva: Educación Digital

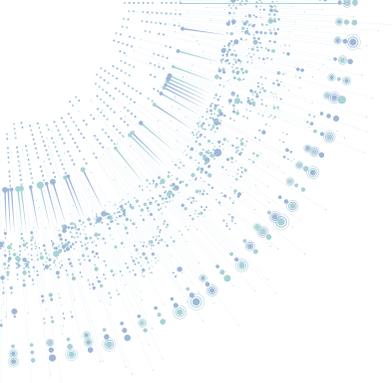
En palabras de Pilar García Freire, Jefa del Área Recursos Educativos Digitales del INTEF, del Ministerio de Educación y Formación Profesional de España, se busca proteger a los menores en su interacción con Internet, para una escuela conectada y cibersegura. Toda vez que la pandemia ha generado un aumento de la educación online, lo que supone una oportunidad y un riesgo a la vez.

La constitución Española, en el art. 18.4 reconoce el derecho fundamental a la protección de datos. Durante estos años ha habido una serie de reglamentos y leyes. En 2018, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales estableció en el art. 83 el derecho a la educación digital, garantizando en el sistema educativo español la plena inser-

ción de los alumnos en la sociedad digital, y un aprendizaje del uso crítico, seguro, y respetuoso de valores y derechos fundamentales. Para esto, las administraciones educativas deben incluir estas materias en los currículos, con especial énfasis en la violencia digital.

Bajo este artículo es que la Agencia Española de Protección de Datos celebró un convenio con el Ministerio de Educación, para prestar recursos educativos de calidad, de manera centralizada, para mayor eficiencia. En razón de esto, se crea AseguraTIC (aseguratic.intef.es), como una colaboración público-privada, cuyo principal objetivo es contribuir a la protección de los menores poniendo a disposición estos recursos educativos, para los menores, sus familias, educadores y administraciones educativas.

En este marco, se creó un buscador específico para facilitar el acceso a estos recursos, existiendo más de 385 recursos publicados, organizados por filtros para maximizar la facilidad de acceso. Hay diversos tipos de recursos, tales como videos, contenido interactivo, juegos, y otros, con temáticas de acoso en internet, adicción a la tecnología, redes sociales, seguridad, protección de datos, etc. Se destacan la guía de la Agencia Española de Protección de Datos para centros educativos, y la línea telefónica de ayuda en ciberseguridad del INCIBE (Instituto Nacional de Ciberseguridad de España), para apoyar a víctimas de violencia digital.



Cultura de la prevención para combatir la violencia digital

Una vez que los niños conozcan sus derechos, será mucho más difícil que sean víctimas de agresiones, y si lo sufren, podrán conocer las herramientas para prevenir y denunciar, así lo destaca Zulema Martínez, Comisionada Presidenta del INFOEM, Estado de México.

En sus palabras, en el Estado de México se habla de cultura de protección de datos personales y prevención de la violencia de género digital, porque se considera que el cambio debe hacerse a ese nivel. En México, la cultura está muy cargada en la masculinidad, y considera que se deben buscar sociedades más femeninas, promoviendo la empatía y así mejorar la calidad de vida. A raíz de un pronunciamiento del Sistema Nacional de Transparencia sobre la violencia digital promovido por el Comisionado

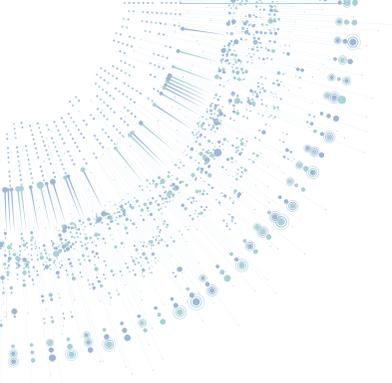
Luis Gustavo Parra Noriega, se adoptaron medidas en el EDOMEX (portal de Internet del Gobierno del Estado de México). Si bien se tienen referencias a las iniciativas como la Ley Olimpia, Ley Ingrid y otras, además se tomaron acciones adicionales, trabajando con las dependencias de gobierno que pudieran tomar acciones para difundir la cultura de protección de datos y prevención de la violencia digital.

Así, se hizo un vínculo con la secretaría de la mujer mexiquense —en un Estado con 8 millones de mujeres, un 51% de la población—, creando material educativo como infografías, para que las mujeres conozcan cómo proteger sus datos personales, y de qué maneras pueden ser agredidas, y que acciones pueden tomar ante esto. Además se ha trabajado con el sistema de protec-

ción de niños, niñas y adolescentes, y la secretaría de educación, para adecuar los protocolos existentes sobre violencia agregando la violencia digital, ofreciendo capacitaciones continuas, a través de juegos interactivos, y ahora a través de aplicaciones como cahoot, de manera de mantener el carácter didáctico.

En el Instituto Nacional de Acceso a la Información y Datos Personales, se tiene una iniciativa llamada "Comisionado infantil", donde los niños conversan con sus propias palabras de estos temas, el que se replicará este año en EDOMEX. También, se comparte material didáctico y multimedia y se dan charlas en las escuelas, así como capacitaciones para los servidores públicos.





¿Introducir una materia ajena a la currícula tradicional?

La ley peruana 29.733 de 2011 en materia de Protección de Datos Personales, y la creación de la Autoridad de Protección de Datos en 2013 instauran un mandato de promoción de la protección de datos personales, y en particular de una cultura de protección de los derechos de los niños, niñas y adolescentes.

Así, ese mandato de promoción ha supuesto una actividad constante de difusión, a entidades públicas y privadas. Las circunstancias del establecimiento de la autoridad han supuesto adecuar las condiciones de trabajo, a través de alianzas estratégicas. Por ello se han establecido alianzas con las direcciones regionales y

las unidades de gestión educativa del Ministerio de Educación de Perú, lo que ha permitido llegar de manera directa a miles de docentes en tres años, logro que ha supuesto el desafío de introducir una materia ajena a la currícula tradicional.

Además, se ha buscado llegar directamente a los niños y jóvenes para saber si el mensaje llega con un lenguaje adecuado para ellos, debiendo adecuar el mensaje, evitando anglicismos, y buscando una comunicación clara. Por ejemplo, se han usado recursos como concursos de arte en que los menores participan, en colaboración con el Ministerio de Cultura y privados. En esta línea, se han llegado a cerca de sie-

te mil alumnos de manera directa en Perú, constató Eduardo Luna, director de la Autoridad de Datos Personales de dicho país. Durante el año 2020 y el actual, el contexto de la pandemia y la virtualización de las clases implicó la colaboración con cápsulas de contenido para la plataforma educativa de la televisión pública, incluyendo contenidos con enfoque de género, buscando romper la cadena de violencia, que en Perú supone que más del 80% de niños y niñas ha sufrido algún tipo de violencia, incluyendo de carácter digital.



Los datos colectivos como bienes comunes

Hace más de 5 años, la Cooperativa Sulá Batsú ha desarrollado una línea de trabajo en Educación Popular para una Ciudadanía Digital. En palabras de Kemly Camacho, fundadora y coordinadora de la organización, esto no solo se refiere a que las personas aprendan sobre sus datos personales (usado en un término general), sino que también cómo sus usos, políticas y modelos de negocio los afectan en su vida cotidiana, y que tengan la capacidad de construir propuestas críticas respecto a estos usos, pasando a una relación bilateral.

Sulá Batsú es una empresa de la economía social solidaria, que trabaja para el desarrollo territorial local, a través de ciencias, artes, tecnología y ciencias sociales, a través del trabajo con las comunidades, y de políticas públicas. La cooperativa lleva 16 años de trabajo en Centroamérica.

Desde 2013, han desarrollado un programa de construcción de liderazgo femenino en el área de ciencias y tecnología,

que implica que las mujeres cuestionen la tecnología y la sociedad digital, y hagan nuevas propuestas desde una perspectiva feminista. Este programa, denominado "TIC-as" ha ganado numerosos reconocimientos internacionales.

Desde este programa se ha dialogado en torno a lo que han denominado los derechos de una ciudadanía digital: derecho a entender cómo funciona la tecnología, el derecho a saber informarse, el derecho al dato, el derecho al algoritmo, y el derecho a proponer la tecnología que requiere el lugar. Estos derechos son tanto respecto de saber cómo funcionan las tecnologías, como de proponer políticas públicas y opinar respecto de las decisiones que toman las empresas.

Con el apoyo de la Universidad de Washington y la WWW Foundation, se ha ido trabajando sobre la pregunta de cuáles datos quieren las mujeres, por qué y cómo los quieren obtener. En torno a eso, han desa-

rollado trabajo en el ámbito comunitario, escolar y laboral.

En cuanto al derecho al dato, se ha ido desarrollando una noción de los datos colectivos como bienes comunes, en oposición al extractivismo de datos, y el derecho a construir los algoritmos que van a tomar decisiones por las personas. Se está haciendo un cuestionamiento de las metodologías, los modelos de negocios, incluir otras poblaciones, etc, en la construcción tecnológica, de manera de tomar en cuenta la visión de las mujeres.

Para las mujeres indígenas, los datos no son transaccionales, sino que relacionales, están relacionados con sus cuerpos, y no se pueden "sacar", lo que se opone completamente al extractivismo de datos. Para poder negociar con las empresas de comunicaciones, y proteger los saberes y la cosmovisión indígena, estas poblaciones deben poder conocer las tecnologías.



El Canal Prioritario de la AEPD: los acuerdos con las plataformas de Internet.

La principal función de las agencias de protección de datos es proteger a las personas en el ejercicio de sus derechos, en un mundo donde la vida está cada vez más digitalizada, y las vulneraciones a la intimidad ponen incluso en riesgo la vida de las personas. Considera que la estrategia debe ser múltiple. Primero, intentaron llegar a la comunidad educativa a través de una línea de apoyo para padres, familias y profesores.

Resulta imprescindible regular por medio de leyes las competencias educativas en materias de prevención de la violencia digital. Como se señaló previamente, consiguieron que las comunidades autónomas tuvieran la función específica de educar en protección de datos y violencia de género en la ley orgánica de protección de datos.

En palabras de Mar España Martí, Directora de la Agencia Española de Protección de Datos, otro paso fundamental resulta vincularse con los ministerios con competencias en protección de derechos sociales, en especial con relación a niños, niñas y adolescentes. Así, por ejemplo, en España se está tramitando una nueva ley de protección a la infancia, y se está buscando incorporar el concepto de violencia digital dentro de las definiciones tradicionales de violencia, lo que sería la primera ocasión que se incorpora esta materia a nivel legislativo en Europa.

Además de la línea legislativa, se ha desarrollado una línea de acción institucional, a través de la colaboración público-privada. A pesar de tener desencuentros en ocasiones, deben buscar adhesiones en la causa

de la protección de derechos de las personas. Esta colaboración partió en ocasión del tratamiento de los delitos de odio, donde se incorporó la violencia digital, dado que podemos entender que este fenómeno tiene una connotación de odio y discriminación especial en contra de las mujeres, además de ser más prevalente.

La propuesta fue que, considerando que tienen potestades de dictar medidas cautelares de retiro de contenidos fuera de los procedimientos judiciales, aunque las empresas no tengan responsabilidad, proponer una alternativa de que se retire de manera voluntaria, dentro de las potestades que tienen por sus términos de servicio.

Han logrado acuerdos de cooperación voluntaria con Google, Facebook, Instagram

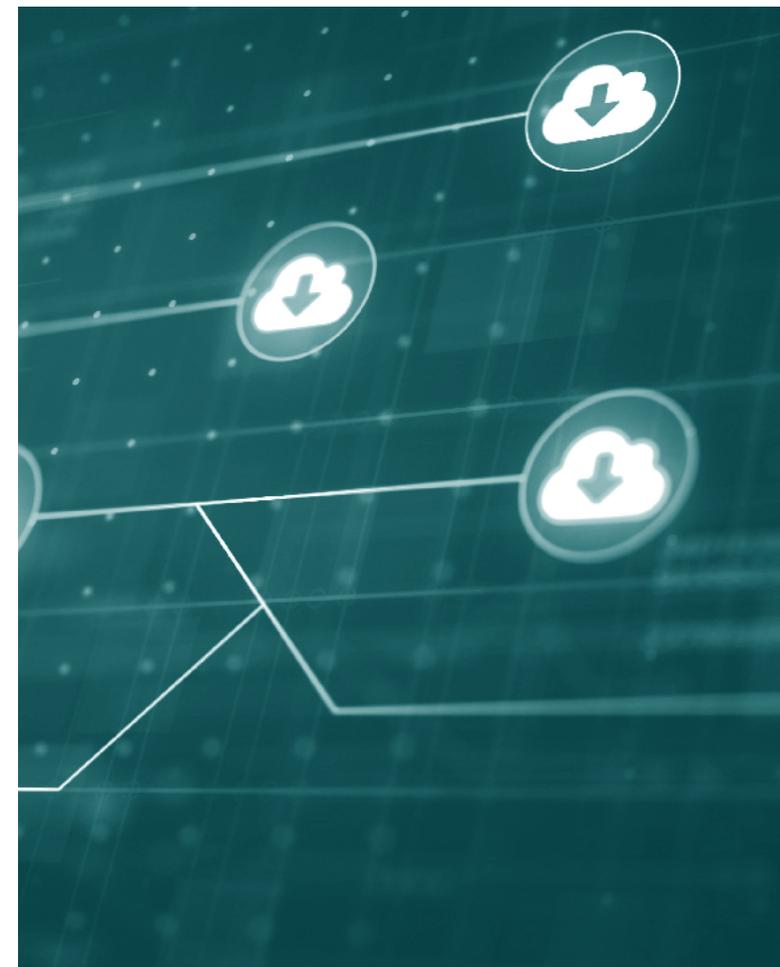


y Twitter, para que se retiren estos contenidos en menos de 72 horas. Desde octubre de 2019, el canal prioritario ha tratado cerca de 400 casos, donde lo importante es la correcta identificación del contenido, y que se trate de casos de violencia digital de exposición de contenidos sensibles.

Otra estrategia es la difusión de estas herramientas, para lo cual se han ideado campañas de difusión. Como la agencia no tiene presupuesto suficiente para pagar estas campañas, consiguieron la declaración de impacto público, por lo cual se pudo difundir de manera gratuita a través de la televisión.

Ahora, se está planificando una nueva campaña denominada “*un clic puede salvar tu vida*”, que busca educar a los jóvenes que un simple *like* o reenvío de un video puede tener consecuencias gravísimas. En la misma línea, también se han desarrollado campañas con *influencers* y *youtubers*, para llegar a los jóvenes a través del tipo de contenidos que consumen.

Una tercera línea es el “Pacto Digital”, en el cual han conseguido adhesiones de 100 entidades y organizaciones del mundo privado, las que se obligan a difundir entre sus empleados y clientes el canal prioritario y las demás iniciativas de la AEPD en materia de violencia digital.





Estrategia regional de la RIPD con apoyo de la Unión Europea

En las últimas décadas, los avances tecnológicos han generado grandes impactos sociales, culturales, económicos y políticos, así como una transformación de las relaciones humanas en cuanto se han disminuido los costos y tiempos para la comunicación. Al crear nuevos tipos de interacción social, también se han creado nuevas formas de violencia, que afectan especialmente a personas más vulnerables. El anonimato y la inmediatez que ofrece la red han contribuido a estos fenómenos.

Conforme al módulo de ciberacoso del INEGI de México, el 40% de las mujeres de 12+ años recibió insinuaciones o propuestas sexuales. También, han crecido los casos de mal uso de datos personales e información privada de mujeres y niñas.

En atención a estos fenómenos, las autoridades de protección de datos y privacidad de la región iberoamericana, en el séptimo encuentro de la RIPD de junio de 2019 determinaron crear el proyecto "Apoyo para

el Fortalecimiento de la estrategia de lucha contra la violencia de género contra niñas, adolescentes y mujeres en Internet" con el apoyo de Eurosocial+, a propuesta del INAI, el que fue aprobado en abril de 2020, con la participación de autoridades de protección de datos: a nivel local, el INFOEM de México, y a nivel internacional, las autoridades de Uruguay, Colombia, Perú y España.

Según Josefina Román, comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México, autoridad líder del proyecto, los resultados esperados son impulsar la creación de un modelo interinstitucional para prevenir y combatir los casos de violencia de género digital contra niñas y mujeres, a través de dos enfoques: uno de carácter preventivo, a través de programas educativos, dotando a las personas de herramientas y esquemas de apoyo legal para prevenir y combatir de manera efectiva la violencia digital. El otro enfoque es correctivo, para coordinar la implementación de acciones

específicas al resto de las autoridades involucradas en estos casos, tales como ministerios de educación, fiscalías, policías y otras.

Para esto, se requieren varios insumos: un estudio comparativo sobre las mejores prácticas de control de la violencia de género digital a nivel latinoamericano y europeo, lineamientos para la creación de una red latinoamericana de atención a situaciones de violencia de género en Internet; un protocolo o estrategia de lucha contra la violencia de género digital desde las competencias de las autoridades de datos, así como propuestas normativas al respecto.

Este proyecto representa una gran oportunidad para el trabajo conjunto entre expertos, autoridades de protección de datos y organizaciones de la sociedad civil, para buscar soluciones eficientes y eficaces en el combate y prevención de la violencia de género digital, el cual es coordinado por las expertas Jessica Matus, de Chile y Ana Karen Cortés, de Costa Rica.



La alianza entre organizaciones para una lucha en conjunto contra la violencia digital con una perspectiva de género

La importancia de la alianza entre las organizaciones de protección de datos y las organizaciones de promoción de los derechos de las mujeres es que permiten transversalizar y poner en el centro los temas de prevención de la violencia digital.

Desde el mecanismo de seguimiento de la Convención Belém do Pará, se han generado cada vez más nuevas formas de violencia. En el mundo digital se han ido reproduciendo estereotipos, prejuicios y formas de violencia tradicional, por lo cual debemos entender que existe un continuo entre la violencia en el mundo online y en el mundo físico, advierte Alejandra Mora Mora, Secretaria Ejecutiva de la Comisión Interamericana de Mujeres (CIM) de la Organización de los Estados Americanos (OEA), y recuerda también que la violencia digi-

tal tiene impactos en personas reales y las vulneraciones a la integridad sexual destruyen el futuro de las mujeres.

Algunos de los fenómenos de violencia digital detectados en la región son: el uso de la geolocalización para el control de la vida de las mujeres; la transmisión de fotos y contenidos íntimos, incluyendo contenidos modificados.

Es importante hablar de estas formas de violencia y su prevención, pero también de la necesidad de su sanción, para evitar la impunidad. Así como hace 25 años se decía que la violencia doméstica no era delito si no que era algo del ámbito privado, ahora se dice que la violencia digital no se puede perseguir, por ello es importante trabajar en la ubicación de los contenidos y la identificación de los responsables.

Otro espacio de desafío es la violencia contra la participación de las mujeres en la política, donde están participando cada vez más, y donde se están dando formas de violencia, difamación y otras contra la participación de las mujeres más allá de la interpelación política, sino que también contra su cuerpo, su sexualidad y su persona.

Aunado a ello, existe un desafío en la protección de las activistas por los derechos de la mujer. Estas mujeres, que muchas veces luchan contra verdaderas mafias, tienen riesgos especiales de violencia, también en el ámbito digital.

Hay que entender que todas las tecnologías deben servir para el acceso y disfrute de oportunidades y derechos, y no para destruir vidas, y vulnerar derechos,



especialmente cuando a las mujeres les ha costado mucho esfuerzo el igual goce de los derechos.

Cinco son las recomendaciones que entrega la máxima autoridad de la CIM: (1) no puede haber desarrollo tecnológico sin enfoque de género; (2) mientras no se tengan datos desagregados por género de la prevalencia de las formas de violencia y sus consecuencias, no se podrá tratar estos problemas de manera objetiva, para lo cual se

requiere que las plataformas transparenten datos; (3) garantizar espacios para que las mujeres puedan solicitar información y discutir estos temas de manera segura, libre de discriminación y confidencial; (4) proporcionar asistencia especializada a las mujeres en la denuncia y seguimiento de estos procesos, y; (5) asegurar el acceso a la información de las aplicaciones y plataformas, conforme a los estándares internacionales del más alto nivel, considerando que los derechos humanos son universales.



Estrategias institucionales y mecanismos de derechos humanos

¿Cuáles son las estrategias que debemos tener para asegurar la protección de datos personales con enfoque de género y erradicar la violencia de género en el ámbito digital? El Instituto de las Mujeres de México -INMUJERES-, como organización es un mecanismo de derechos humanos, cuyo rol es promover políticas de Estado, no de gobierno, y que trasciende a los tres poderes del Estado y los tres órdenes de gobierno.

Por otro lado, los mecanismos de derechos humanos son estructuras bastante pequeñas en recurso y personal, pero con una tarea bastante grande, como es generar instrumentos, protocolos, y guías técnicas para que las instituciones, en el ámbito de su competencia, protejan los derechos de las mujeres en el mundo digital.

La propuesta de INMUJERES, en su calidad de mecanismos de derechos, busca aterrizar estas materias a nivel municipal, fe-

derativo y nacional, armonizando reglas a nivel institucional y normativo, de manera que la protección de los derechos no dependa de la voluntad política de turno. La idea es que esta protección de derechos parta de una manera propositiva, de promoción de derechos antes que reactiva, a través de sanciones. Para esto, se debe tener un enfoque de género, generacional, intercultural y territorial, a nivel de lenguaje incluyente, etc.

Otra materia relevante es la brecha de género en el acceso a las tecnologías digitales. La falta de acceso a la vida digital es también una forma de violencia. Por ejemplo, en lugares rurales o de escasos ingresos, en que hay un solo dispositivo, en muchos casos solo se le da acceso a los niños, privando del acceso a la educación vía internet a las mujeres, señaló Celia Aguilar Setién, Directora General de Estadísticas, Información y Formación de Género de INMUJERES.

El enfoque intercultural es importante también. El acceso a smartphones en comunidades indígenas y rurales se ha vuelto imprescindible como línea de conexión con las personas migrantes de estas comunidades y de acceso a las remesas. En estas situaciones especiales, puede haber mayor incidencia de violencia y menor acceso al conocimiento de las normativas y herramientas para su denuncia y prevención.

La capacidad de los mecanismos de derechos es poder incidir en las múltiples soberanías (32 entidades federativas y miles de municipios), sus legislaciones, organizaciones y programas, de manera de promover los derechos humanos, reconocidos a nivel constitucional, de manera de hacer efectivas las políticas de protección de género.



Activismo en Latinoamérica: los retos de la región

Un proyecto de activismo de Latinoamérica es Acoso.online, dedicado a compilar información de manera fidedigna y profesional sobre violencia de género en Internet, en particular respecto de la difusión no consentida de imágenes íntimas.

Esta iniciativa comenzó en 2017, cuando a sus integrantes que trabajan en derechos humanos y tecnología, les llegaban solicitudes de ayuda sobre difusión de contenidos íntimos. Así, se fueron dando cuenta que había escasa información en español, por parte de gobiernos y plataformas de Internet, y que faltaba un enfoque de género, porque la información solía ser estigmatizadora contra las víctimas.

Más allá de las leyes, Paz Peña Ochoa, consultora chilena experta en tecnologías, derechos humanos y género, advierte que hace falta mucho trabajo a nivel de políticas públicas para terminar con la violencia de género en línea.

A nivel formal, si bien no reciben casos particulares, de todos modos han conocido

de casos donde han visto los graves impactos en el mundo físico, personas que han debido cambiarse de domicilio, de nombre, hacerse cargo de los costos legales y psicológicos, casos de suicidios, entre otras terribles consecuencias.

Primero, han notado que las víctimas se encuentran en una situación de abandono por parte de los gobiernos. Por ejemplo, en el caso de Chile, con la pandemia las cifras de violencia de género y violencia digital han aumentado; el gobierno levantó una línea de ayuda, la cual está encargada a una empresa de call center, sin mayor formación especializada en violencia de género. También, al momento de recurrir a las policías, las víctimas se ven cuestionadas, o no son tomadas en cuenta sus denuncias, lo cual replica la estructura patriarcal del Estado.

Por otro lado, hay un abandono de las víctimas por parte de las plataformas. En el año 2017 Acoso.Online realizó un estudio sobre los términos de servicio y las herramientas de las grandes plataformas de Internet respecto de la violencia de género, y descu-

brieron que muchas veces estos términos y herramientas no estaban disponibles en español ni portugués, pese a su gran adopción en Latinoamérica, y que no había transparencia respecto al avance de las denuncias. Si bien se ha mejorado con el tiempo, las plataformas siguen en deuda en la materia.

Por último, hay mucha ignorancia en las comunidades cercanas a las víctimas, como son las universidades e instituciones educativas. Muchas veces la violencia digital se da en el ámbito educativo, y las instituciones consideran que es un problema privado en el que no deben intervenir, lo cual supone que las víctimas abandonen sus estudios o sufran grandes costos psicológicos. Hace falta que los códigos de conducta en el ámbito educativo aborden seriamente estos temas.

Lo anterior también se replica en el ámbito laboral, materia que están investigando actualmente por la masificación del teletrabajo a partir de la pandemia, donde hay muy poca información en la materia.



La experiencia de violencia de género digital de Olimpia y su lucha por combatirla.

Olimpia Coral es la impulsora de la “Ley Olimpia” para combatir la violencia digital contra las mujeres y fundadora del Frente Nacional para la Sororidad en México.

Hace unos años, advierte, se utilizaba el término pornovenganza, que está mal por dos motivos. Primero, porque no es porno, con ese término se normaliza la cultura que objetiviza, criminaliza y sujeta los cuerpos femeninos al placer sexual masculino. Tampoco es venganza porque así pareciera justificar la acción de violencia, revictimizando a las mujeres.

Considera que las reformas legislativas no son la panacea, no van a solucionar todos los problemas. Una reforma sin educación, sin prevención, sin conciencia de que el espacio digital es una continuación de los espacios offline no será suficiente.

El frente nacional para la sororidad comenzó a trabajar el 2014, luego de que ella misma fue víctima de violencia de género digital. En esa oportunidad se sintió triste, sola, expuesta, y cuando buscó salir adelante, y la ayuda del Estado, se encontró con la respuesta de los funcionarios, primeros en revictimizar, cuestionar la víctima para, luego, decir que no pueden hacer nada.

En esa época, se le señaló que únicamente se le podría haber ayudado si hubiera sido menor de edad, constituyendo éste un caso de pornografía infantil, por producción, difusión o promoción de contenidos íntimos. Para los mayores de edad, en algunos casos se podían aplicar tipos penales de faltas a la moral, lo cual es un enfoque incorrecto, porque nuevamente cuestiona las decisiones de las mujeres en su vida sexual.

Lo que ha buscado, por un lado, es incorporar la violencia digital contra las mujeres dentro de la Ley de Acceso de las Mujeres a una Vida Libre de Violencia, incluyendo las formas de violencia que dañan la intimidad sexual, como la sextorsión, o la difusión no consentida de imágenes íntimas, la trata virtual de personas con fines de explotación; y por otro lado, las que afectan la privacidad, como el ciberacoso, y otras formas que no dañan la intimidad sexual.

Otra línea de trabajo dice relación con la formación de una fiscalía especializada en delitos digitales. Para esto, se han tenido que combatir con diversos prejuicios: que lo digital no es real; que no se discute lo sexual en público, y por qué razón se va a defender a las víctimas si ellas se expusieron, revictimizándolas en el proceso.



Considera que no hay posibilidad de una Internet segura para las mujeres mientras se mantengan las estructuras patriarcales. Recuerda el caso de Facebook, que partió como un álbum de fotos de mujeres obtenidas sin su consentimiento en Harvard.

Asimismo, señala que mientras no se erradiquen estas estructuras machistas no se van a eliminar estos problemas, no basta con reformas legales si no se hacen primero reformas a nivel educativo que cambien estos paradigmas. También, se debe pasar a un paradigma de derechos digitales, mayor uso de tecnologías en la investigación,

y mayor responsabilidad de las plataformas de Internet, en las cuales hay usos de datos, fotografías, información, en una suerte de colonialismo digital, y un consentimiento manipulado.

Concluye que así como en los tiempos de nuestras abuelas el voto de las mujeres era algo que aún no se conquistaba, pero que ahora cuentan con orgullo como un tema superado, quiere lograr que en algún momento puedan decir lo mismo a sus nietas respecto de la desaparición de la difusión sin consentimiento de contenido íntimo.





Estereotipos sexistas y violencia contra mujeres en el ámbito informativo del deporte.

Versus es una organización mexicana que trata formas distintas de violencia de género. Se enfoca en la omisión de las mujeres en contenidos informativos en el deporte, donde la invisibilización y la aplicación de estereotipos sexistas contra mujeres y personas LGBTQ es una forma de violencia simbólica.

Las representaciones mediáticas juegan un rol importante en la construcción de la realidad. La sexualización de las atletas, validada en los medios de comunicación, se traduce en consecuencias en el mundo real.

Andrea Martínez de la Vega, representante de la organización, cita el caso de una jugadora de las Chivas de Guadalajara, goleadora histórica del equipo, respecto de

quien sólo se publica información en torno a su físico, con lo cual se ha afectado finalmente su actividad profesional.

Como organización, realizaron un estudio sobre la representación de las mujeres en el deporte en medios digitales en el contexto de la pandemia. Este ejercicio de observación y análisis lo han compartido en varios espacios de diálogo y aprendizaje conjunto, y en general han tenido buena recepción, donde han considerado que el deporte es un espacio con gran potencial de impacto cultural, por lo que las representaciones importan.

Pero no en todos los espacios han encontrado la misma recepción, por ejemplo, en los medios han observado una resistencia

al cambio, por tratarse de espacios bastante masculinizados, donde existen pocas mujeres en las redacciones y en los lugares de decisión editorial.

En la actualidad están expandiendo el ejercicio de observación de las representaciones de mujeres en los deportes en los medios, pasando de ocho semanas a un año, y de medios digitales a incluir medios impresos, de modo de contar datos duros, y sensibilizar de mejor manera el tema. También están trabajando desde la visibilización con campañas educativas dirigidas a las audiencias, las que tienen un papel fundamental, buscando formar consumidores críticos de contenidos.



Conclusiones: colaboración de las autoridades de protección de datos

Es fundamental recalcar la necesidad de la colaboración. Desde la práctica, es un común denominador en la actividad de las autoridades de protección de datos latinoamericanas la descoordinación o ausencia de colaboración con las policías y órganos de investigación, en especial respecto de casos que ya son delito en los ordenamientos jurídicos, y de mujeres, niños, niñas, adolescentes y sujetos de especial protección. Esta coordinación es particularmente importante para adelantarse respecto de casos transnacionales, que puedan afectar no solo la protección de datos, sino que otros derechos humanos de estas personas.

Andrés Barreto González, Superintendente de Industria y Comercio de Colombia, entidad que preside la RIPD, indicó que la declaración de la Red Iberoamericana contra la violencia digital de mujeres y niños busca una protección de datos que, desde las diferentes competencias de cada organización, permita combatir cualquier tipo de violencia. La gravedad de estas conductas, y la

imposibilidad de controlarlas puede revictimizar y vulnera derechos como la protección de datos, la intimidad, y puede constituir delitos, que deben ser atacadas mediante la cooperación judicial internacional.

Según el estudio de ONU Mujeres de 2015, el 73% de las mujeres ha estado expuesta o experimentado violencia en línea, de las cuales el 90% ha sido víctima de difusión de contenido íntimo no autorizado. La cruzada para proteger el espacio digital de las mujeres debe suponer la participación plural de diversos actores, no vale la pena discutir entre autoridades, academia y organizaciones de la sociedad civil, un mundo o una norma perfecta, pero el producto que resulte, deberá surgir de un diálogo conjunto, que contenga estas visiones plurales.

Se deben buscar instrumentos fuertes homólogos a los europeos. En ese sentido, la autoridad colombiana advierte que proteger los negocios no puede ser una excusa para permitir la violación de derechos, para no

transparentar donde están los servidores con los datos, o para que no haya corresponsabilidad entre los gigantes tecnológicos que usan nuestros datos o imágenes. Esto es parte de una cruzada digital para tener un mundo digital más nivelado en materia de protección de datos y de los consumidores.

Seguir construyendo espacios como éste, donde existan distintas visiones. No es necesario criminalizar todo, porque sería imposible, pero es necesario proteger la intimidad, los datos personales, lograr un uso responsable de las tecnologías, y la generar un marco de corresponsabilidad entre los diversos actores será el camino para alcanzar un sano y adecuado disfrute de las tecnologías y la protección de los derechos.

Por último, considera que la libertad de expresión no debe verse en contradicción contra los derechos a la intimidad y protección de datos, la libertad de expresión no es un derecho absoluto que permita vulnerar los derechos de otras personas.

Declaración de la Red Iberoamericana de Protección de Datos (RIPD) contra la Violencia Digital en mujeres y niñas

Conscientes de la responsabilidad que les atañe como autoridades de protección de datos de la región iberoamericana y la necesidad de incidir decisivamente en el objetivo de poner fin al flagelo de la Violencia de Género en Internet, se declara:

PRIMERO. La "violencia digital" o "ciberviolencia", entendida con el alcance en que ha sido definida por algunos de los textos anteriormente citados, constituye, entre otras, una flagrante vulneración del derecho fundamental a la protección de datos personales, en la medida en que las imágenes, los videos, las fotos y la voz constituyen datos personales que están siendo objeto de un indebido tratamiento, y, en esa medida, debe ser erradicada.

SEGUNDO. Reconocemos que, si bien es cierto que todas las personas estamos expuestas a sufrir violencia en el entorno digital y mediático, sin embargo, las mujeres, niñas y adolescentes están afectadas de forma desproporcionada por la hipersexualización a la que históricamente han estado sujetas y, por ello, sufren en mayor medida las consecuencias extremadamente graves de este fenómeno, aunado al perjuicio que ocasionan los estereotipos y roles de género arraigados en los países Iberoamericanos. Este fenómeno no es más que una prolongación de la violencia que vive a diario esta parte de la población en el espacio virtual, mismo que puede provocar daños físicos y psicológicos permanentes en quien es víctima de este flagelo.

TERCERO. Consideramos que los Estados Iberoamericanos, desde una perspectiva global y regional, deben avanzar en la tarea de incorporar en sus respectivos marcos legislativos y en sus políticas públicas las distintas formas de violencia digital contra las mujeres, niñas y adolescentes, estableciendo mecanismos de tutela judicial y administrativa y servicios de información y apoyo de sus derechos legales y de las ayudas disponibles.

CUARTO. Estamos convencidos que, para hacer frente a este fenómeno de forma efectiva, resulta necesaria una estrategia de responsabilidad compartida en el que todas las instituciones competentes, las legislaciones nacionales y las organizaciones implicadas trabajen en común desde un enfoque integral -preventivo y reactivo-, a fin de contar con los correspondientes canales de denuncia, atención inmediata a las víctimas y castigo a las personas responsables para mitigar los efectos de la violencia digital. Esta estrategia deberá diseñarse teniendo en cuenta las voces de las mujeres víctimas de esta violencia y de sus asociaciones más representativas.

QUINTO. Consideramos que los Estados Iberoamericanos deberán impulsar instrumentos y herramientas que permitan a sus respectivas Autoridades de Protección de Datos combatir de forma efectiva y urgente estas conductas en internet, dotándolas, si fuese necesario, del marco legal adecuado para ello, incorporando en la legislación interna la tipificación de este delito de violencia digital, además de los correspondientes recursos materiales y personales. En este sentido, se considera una buena práctica el llamado "Canal Prioritario" creado por la Agencia Española de Protección de Datos para solicitar la eliminación urgente (en menos de 72 horas) de contenidos sexuales o violentos en internet contra mujeres, niñas y adolescentes.

SEXTO. Hacemos un llamado a la industria digital a generar un diálogo permanente que permita identificar áreas de colaboración y trabajo, que generen esfuerzos conjuntos contra la violencia digital y líneas de acción para mitigar los riesgos y atender los fenómenos derivados de ella, en conjunto con las autoridades competentes, la sociedad civil y la RIPD. En particular, exhortamos a promover medidas de prevención, como la adopción de normas de autorregulación para evitar la generación nociva de estereotipos de género y la propagación de imágenes degradantes de mujeres, o de aquéllas en las que se asocia el sexo con la violencia.

Un punto indispensable en esta batalla es la realización de ajustes no solo en los algoritmos de búsqueda sino también en los de almacenamiento de la información, puesto que la traza digital que genera una persona puede ser fácilmente accedida por los ciberdelincuentes. Los términos y condiciones de los servicios de redes sociales, correos y demás deben revisarse de tal forma que se pueda aplicar el derecho al olvido y así minimizar la traza digital y, con ello, el riesgo de ciberacoso en todas las

modalidades expuestas anteriormente, evitando que los perfiles que realizan los algoritmos sobre las personas no sean objeto de comercialización ni de fácil acceso para los ciberatacantes.

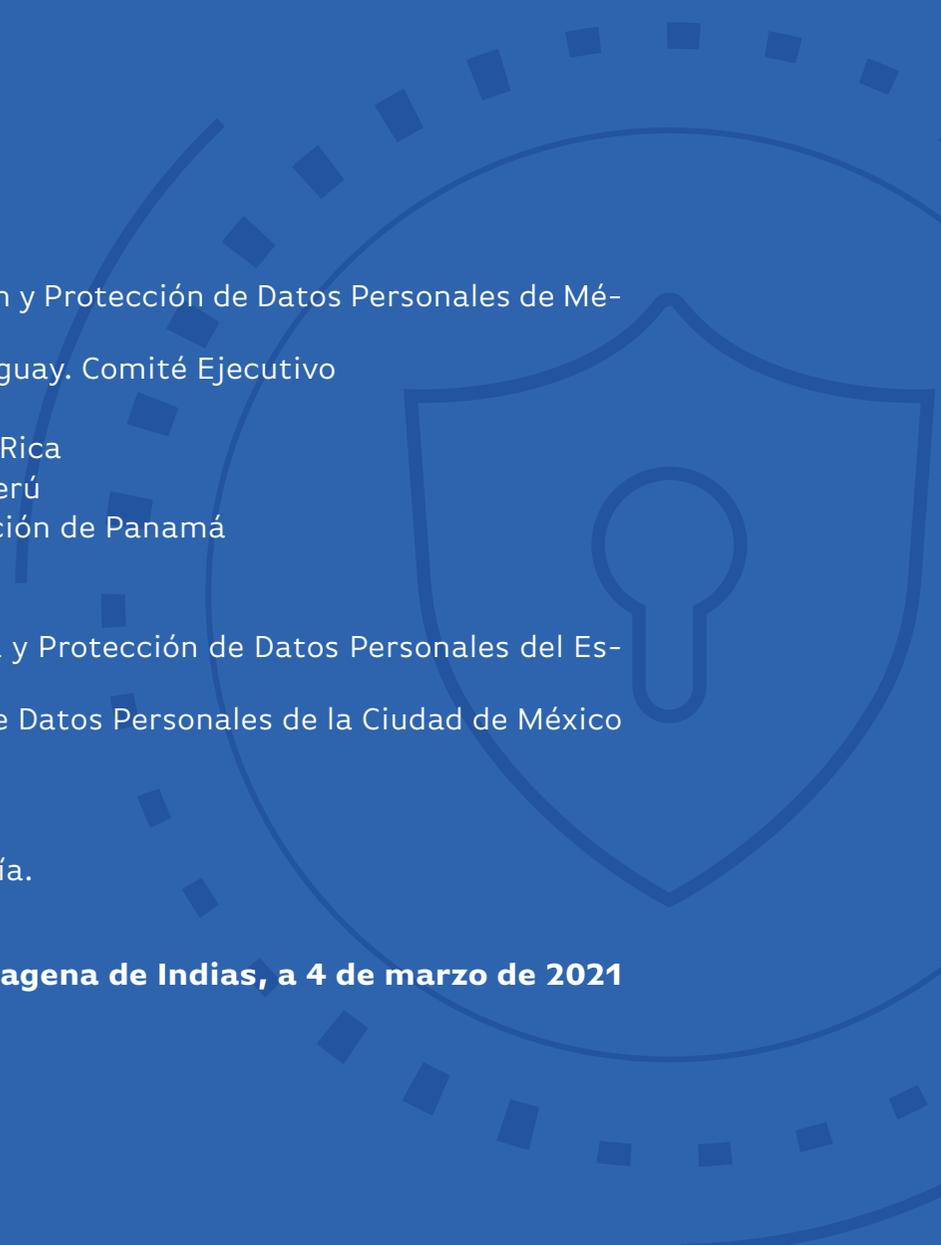
Las redes sociales digitales también deberían contar con canales prioritarios para que las personas afectadas soliciten la eliminación urgente (en menos de 72 horas) de contenidos sexuales o violentos en internet contra mujeres, niñas y adolescentes.

SÉPTIMO. Invitamos a la ciudadanía y a las organizaciones de la sociedad civil, para que se trabaje en conjunto a favor del desarrollo de una cultura de protección y cuidado de la información personal a través de la educación digital y campañas de concienciación y sensibilización sobre esta problemática en conjunto con el sistema educativo de cada país, así como fomentar la denuncia en instancias jurisdiccionales ante posibles hechos que constituyan violencia digital.

En consecuencia, quienes integramos la RIPD asumimos el firme compromiso de combatir de forma activa, y dentro de nuestras competencias legales, cualquier tipo de violencia digital que involucre tratamiento de datos personales, en especial la realizada contra las mujeres, niñas y adolescentes, impulsando iniciativas que contribuyan a concienciar y sensibilizar a la ciudadanía y a las organizaciones responsables de sus derechos, pero también de sus responsabilidades en el ámbito digital, en estrecha colaboración con las organizaciones y asociaciones de defensa de los derechos de las mujeres. La suma de estos esfuerzos permitirá la visibilización de este preocupante fenómeno y ampliará el espectro de la protección de la intimidad sexual de las mujeres, adolescentes y niñas en todas las edades, lo que marcará un precedente de progresividad respecto al reconocimiento de la dignidad de las personas y su protección en los medios digitales.

Suscriben la presente Declaración, las siguientes Autoridades Miembros de la RIPD:

Superintendencia de Industria y Comercio de Colombia. Presidencia
Agencia Española de Protección de Datos. Secretaría Permanente
Agencia de Acceso a la Información Pública de Argentina. Comité Ejecutivo



Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México. Comité Ejecutivo
Unidad Reguladora y de Control de Datos Personales de Uruguay. Comité Ejecutivo
Agencia Andorrana de Protección de Datos
Agencia de Protección de Datos de los Habitantes de Costa Rica
Autoridad Nacional de Protección de Datos Personales de Perú
Autoridad Nacional de Transparencia y Acceso a la Información de Panamá
Comisión Nacional de Protección de Datos de Portugal
Consejo para la Transparencia de Chile
Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM)
Instituto de Acceso a la Información Pública y Protección de Datos Personales de la Ciudad de México (INFOCDMX)
Agencia Vasca de Protección de Datos;
Autoridad Catalana de Protección de Datos.
Consejo de Transparencia y Protección de Datos de Andalucía.

En Cartagena de Indias, a 4 de marzo de 2021

WEBINARIO

ESTRATEGIAS DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS PARA LUCHAR CONTRA LA VIOLENCIA DIGITAL EN IBEROAMÉRICA CON UN ENFOQUE DE GÉNERO

4 DE MARZO DE 2021



Financiado por
la Unión Europea



Cooperación
Española
CONOCIMIENTO/INTERCONECTA