Medidas de protección frente a la violencia digital

Regulación y mecanismos en la legislación comparada

Autoras

Daniela Santana Silva
dasantana@bcn.cl

Pamela Cifuentes Vidal
pcifuentes@bcn.cl

Nº SUP: 156654

Resumen

El presente informe analiza, en perspectiva comparada, las medidas jurídicas destinadas a detener o reducir la circulación de determinados contenidos digitales nocivos, en particular la difusión no consentida de imágenes íntimas, el ciberacoso y el ciberabuso en mujeres. Para ello, examina la Ley Modelo Interamericana para Prevenir, Sancionar y Erradicar la Violencia Digital contra las Mujeres basada en Género (MESECVI, 2025) y la legislación de Australia, México y Reino Unido.

Los casos analizados contemplan mecanismos de retiro o eliminación del contenido, aunque difieren en la autoridad encargada de disponerlos o exigir su cumplimiento. En México, la ordenan el Ministerio Público o el juez en el marco de una investigación. En Australia, la dispone una autoridad administrativa especializada, el *eSafety Commissioner*. En el Reino Unido, la obligación recae directamente sobre las plataformas, bajo la supervisión del regulador Ofcom. La Ley Modelo combina la intervención administrativa y la judicial, y exige control judicial para las medidas que restrinjan derechos fundamentales.

También existen diferencias en los plazos de actuación y cumplimiento. Australia exige cumplir las órdenes en 24 horas y el Reino Unido fija un máximo de 48 horas desde la denuncia de la víctima. México y la Ley Modelo, en cambio, exigen una actuación inmediata sin fijar un plazo determinado. El régimen británico contempla, además, medidas de exclusión de resultados de búsqueda y mecanismos destinados a prevenir la recirculación del contenido mediante tecnologías de *hash matching,* cuya aplicación debe entenderse conforme a las fechas de entrada en vigor previstas para dichas obligaciones.

Respecto de la preservación de la evidencia digital, solo México y la Ley Modelo establecen de forma expresa el deber de conservar el contenido retirado para fines probatorios. En Australia y el Reino Unido existen facultades de investigación y obligaciones generales de registro, pero no un deber específico de resguardar el material cuya retirada se ordena.

Contenido del informe

Introducción....2
I. Fórmulas de protección frente a contenidos digitales nocivos....4
1. Retiro o eliminación del contenido....5
2. Bloqueo o restricción del acceso....5
3. Reducción de visibilidad y exclusión de resultados de búsqueda....6
4. Suspensión o bloqueo de cuentas....6
5. Prevención de la recirculación mediante tecnologías de hashing....7
6. Preservación de la evidencia digital....7
II. Medidas de protección en la legislación comparada....8
1. Ley Modelo Interamericana....8
a. Tipo de medida....9
b. Autoridad facultada....9
c. Etapa o momento en que puede disponerse....9
d. Presupuesto o estándar requerido....9
e. Destinatario de la orden....9
f. Plazo de cumplimiento....10
g. Mecanismos de revisión o impugnación....10
h. Preservación de la evidencia digital....10
2. Australia....10
2.1 Ciberacoso dirigido a un niño, niña o adolescente (NNA) (cyber-bullying material targeted at an Australian child)....11
a. Tipo de medida....11
b. Autoridad facultada....11
c. Etapa o momento en que puede disponerse....11
d. Presupuesto o estándar requerido....12
e. Destinatario de la orden....12
f. Plazo de cumplimiento....12
g. Mecanismos de revisión o impugnación....12
h. Preservación de la evidencia digital....13
2.2 Ciberabuso dirigido a una persona adulta australiana (*cyber-abuse material targeted at an Australian adult*)....13
a. Tipo de medida....13
b. Autoridad facultada....14
c. Etapa o momento en que puede disponerse....14
d. Presupuesto o estándar requerido....14
e. Destinatario de la orden....15
f. Plazo de cumplimiento....15
g. Mecanismos de revisión o impugnación....15
h. Preservación de la evidencia digital....15

2.3 Difusión no consentida de imágenes íntimas (*non-consensual sharing of intimate images*)..... 15
a. Tipo de medida..... 16
b. Autoridad facultada..... 16
c. Etapa o momento en que puede disponerse..... 16
d. Presupuesto o estándar requerido..... 17
e. Destinatario de la orden..... 17
f. Plazo de cumplimiento..... 17
g. Mecanismos de revisión o impugnación..... 17
h. Preservación de la evidencia digital..... 18
3. México..... 18
a. Tipo de medida..... 18
b. Autoridad facultada..... 19
c. Etapa o momento en que puede disponerse..... 19
d. Presupuesto o estándar requerido..... 19
e. Destinatario de la orden..... 19
f. Plazo de cumplimiento..... 20
g. Mecanismos de revisión o impugnación..... 20
h. Preservación de la evidencia digital..... 20
4. Reino Unido..... 20
a. Tipo de medida..... 21
b. Autoridad facultada..... 21
c. Etapa o momento en que puede disponerse..... 22
d. Presupuesto o estándar requerido..... 22
e. Destinatario de la orden o medida..... 22
f. Plazo de cumplimiento..... 22
g. Mecanismos de revisión o impugnación..... 23
h. Preservación de la evidencia digital..... 23
III. Consideraciones finales..... 23
Referencias..... 25

Introducción

A solicitud parlamentaria, el presente informe tiene por objeto entregar antecedentes de legislación comparada sobre las medidas de protección frente a contenidos digitales nocivos, en particular aquellos vinculados con violencia digital, difusión no consentida de imágenes íntimas, ciberacoso, con especial énfasis en las órdenes de retiro, bloqueo o eliminación de contenidos y en la preservación de la evidencia digital.

En primer lugar, el informe describe las distintas fórmulas de protección identificadas en la literatura especializada, las que no necesariamente se encuentran presentes en todos los ordenamientos analizados. Estas son el: retiro del contenido, el bloqueo o restricción del acceso, la reducción de visibilidad y la exclusión de resultados de búsqueda, la suspensión de cuentas, la prevención de la recirculación mediante tecnologías de *hashing* y la preservación de la evidencia digital.

En segundo lugar, se analiza la Ley Modelo Interamericana como estándar regional de referencia y la legislación de Australia, México y Reino Unido. Estos países fueron seleccionados porque representan

modelos institucionales distintos: la intervención del Ministerio Público y los tribunales, la actuación de una autoridad administrativa especializada y la imposición de deberes directos a las plataformas bajo la supervisión de un regulador. Para cada caso, la información se organiza en torno a ocho parámetros de análisis:

- Tipo de medida, esto es, la forma de intervención que puede adoptarse sobre el contenido, el servicio o la cuenta.
- Autoridad competente para ordenar, adoptar o supervisar la medida.
- Etapa o momento en que puede disponerse, incluida su relación con una denuncia o investigación.
- Supuesto habilitante o estándar jurídico requerido para su adopción.
- Destinatario de la orden, sea el proveedor del servicio, el proveedor de alojamiento o el usuario que publicó el contenido.
- Plazo de cumplimiento exigido al destinatario.
- Mecanismos de revisión o impugnación de la medida.
- Preservación de la evidencia digital.

Finalmente, el informe incluye un apartado de conclusiones que sintetiza las principales similitudes y diferencias entre los modelos analizados.

El tema abordado y los contenidos del presente informe se encuentran delimitados por los parámetros propios de la Asesoría Técnica Parlamentaria, por el plazo de entrega convenido y por la información normativa, técnica y doctrinaria disponible. No constituye un documento académico y se enmarca en criterios de neutralidad, pertinencia, síntesis y oportunidad en su elaboración. Lo destacado y las traducciones son propias.

I. Fórmulas de protección frente a contenidos digitales nocivos

La difusión de contenidos mediante plataformas digitales presenta características que pueden intensificar y prolongar el daño provocado a las víctimas. En particular, la posibilidad de reproducción, descarga y redistribución del material permite que una misma publicación se replique rápidamente en distintas plataformas y sitios de internet.

En un estudio publicado por Antoinette Huber y Zara Ward en el *European Journal of Criminology*, sobre la distribución y retiro de imágenes íntimas difundidas sin consentimiento (*Non-consensual intimate image distribution: Nature, removal, and implications for the Online Safety Act*), las autoras analizaron información recopilada en colaboración con la Revenge Porn Helpline del Reino Unido. En los 35 casos en los que fue posible examinar las URL públicas involucradas, identificaron 16.937 imágenes distribuidas en 325 sitios y plataformas, equivalentes a un promedio de 484 imágenes por víctima. A partir de estos resultados, Huber y Ward destacan la importancia de contar con mecanismos de denuncia accesibles y procedimientos que permitan un rápido retiro del contenido (Huber & Ward, 2025: 41-42).

Por tanto, las medidas de protección frente a contenidos digitales nocivos no se limitan a su eliminación. Las respuestas disponibles pueden actuar sobre distintos elementos de su circulación: hacer desaparecer el contenido de un determinado servicio; impedir su acceso; reducir su visibilidad; intervenir sobre la cuenta desde la cual se difunde; o impedir que copias previamente identificadas vuelvan a

publicarse. A estas medidas, destinadas principalmente a detener o reducir el daño, se agrega una cuestión distinta pero estrechamente relacionada con la investigación penal: la preservación de la evidencia digital. A continuación, analicemos brevemente cada una de ellas.

1. Retiro o eliminación del contenido

El retiro o *takedown* supone que determinado contenido deja de encontrarse disponible en el servicio en el cual estaba alojado. En materia de violencia digital, esta medida puede adquirir una función protectora inmediata, especialmente cuando la continuidad de la publicación facilita nuevas descargas o redistribuciones.

La evidencia recogida por Huber y Ward muestra que la eficacia del retiro de contenido depende, entre otros factores, de que existan vías claras para denunciar el contenido y de la cooperación de los distintos intermediarios. En los casos examinados por las autoras, la Revenge Porn Helpline recurrió, según las características del sitio, al correo electrónico, formularios de denuncia, canales de confianza o, cuando el sitio no respondía, directamente al proveedor de alojamiento. Mediante estas fórmulas se alcanzó una tasa de retiro cercana al 96 % respecto de las imágenes analizadas (Huber & Ward, 2025: 40–42).

La literatura reciente propone, además, distinguir entre retirar contenido definitivamente y retirar contenido de manera provisional mientras se verifica la denuncia. Harlan, Jo y Crockett, en un estudio comparado sobre los mecanismos de denuncia y retiro de imágenes íntimas no consentidas en Facebook, Instagram, Snapchat, TikTok, Reddit, X y Google Search, analizan estos sistemas desde una perspectiva centrada en la víctima y sostienen que el procedimiento de retirar contenido debe minimizar la carga y la reexposición de la persona afectada. En este marco, proponen que exista un umbral bajo para retirar provisoriamente el contenido: la declaración de la persona que afirma aparecer en una imagen difundida sin su consentimiento podría justificar su indisponibilidad temporal mientras la plataforma efectúa las verificaciones correspondientes. Si posteriormente se determina que el contenido no reúne esas características, este podría ser restablecido, sujeto a un mecanismo adecuado de revisión o apelación (Harlan et al., 2026: 11–12).

Esta propuesta se expresa en el denominado enfoque "*remove first, verify later*", conforme al cual mantener visible el contenido mientras se desarrolla la revisión puede prolongar y agravar el daño. En consecuencia, las autoras recomiendan priorizar el retiro inmediato del contenido durante dicho período, en lugar de limitarse a reducir su circulación mientras se adopta una decisión definitiva (Harlan et al., 2026: 20).

2. Bloqueo o restricción del acceso

El bloqueo produce un efecto diferente del retiro de contenido. En este supuesto, el contenido puede continuar alojado en el servidor o sitio de origen, pero se adoptan medidas destinadas a impedir o dificultar que los usuarios puedan acceder a él.

Esta fórmula adquiere particular importancia cuando el proveedor que aloja el contenido no lo elimina, especialmente si se encuentra radicado fuera de la jurisdicción de la autoridad que pretende intervenir. El informe de la *Women and Equalities Committee* de la Cámara de los Comunes británica constató que, aun cuando muchas plataformas retiran voluntariamente contenidos de imágenes íntimas no

consentidas, parte del material permanece disponible, particularmente en sitios alojados en el extranjero. Frente a estas situaciones, el Comité planteó el bloqueo del acceso como una respuesta alternativa cuando el retiro de contenido no es efectivo (Women and Equalities Committee, 2025: 1–2).

3. Reducción de visibilidad y exclusión de resultados de búsqueda

Howard y Kira utilizan el término reducción de visibilidad (*demotion*) para referirse, de manera general, a políticas mediante las cuales determinadas categorías de contenido se hacen menos visibles para las personas usuarias. Ello puede realizarse mediante distintas técnicas, entre ellas reducir la posición del contenido en sistemas de recomendación (*downranking*), excluirlo de las recomendaciones, impedir que aparezca en una búsqueda (*delisting*) o disminuir su posición dentro de los resultados de búsqueda (*downlisting*). En todos estos casos, el contenido puede permanecer publicado, pero se limita deliberadamente su amplificación y, con ello, el número y frecuencia de usuarios que pueden quedar expuestos a él (Howard & Kira, 2026: 484-488).

Dentro de estas técnicas, el *delisting* se refiere específicamente a impedir que un contenido aparezca en los resultados de una búsqueda, sin que ello implique necesariamente su eliminación del sitio en que se encuentra alojado. El informe de la *Women and Equalities Committee* del Parlamento británico ofrece una aplicación concreta de esta medida respecto de imágenes íntimas no consentidas (NCII, por sus siglas en inglés, Non-Consensual Intimate Images). Según el informe, Microsoft/Bing ha utilizado la base de datos de StopNCII para impedir que determinadas imágenes sean mostradas en los resultados de búsqueda de imágenes de Bing. Asimismo, una vez verificado que el contenido infringe su política sobre NCII, Microsoft puede retirar los enlaces denunciados de los resultados de búsqueda y, cuando el contenido se encuentra alojado en alguno de sus propios servicios, retirar también el acceso al mismo (Women and Equalities Committee, 2025: 44).

La reducción de visibilidad presenta, además, una dimensión de proporcionalidad. Howard y Kira sostienen que, frente a contenidos cuyo nivel de daño no justifica necesariamente una eliminación total, la *demotion* puede constituir una intervención menos intensa. Desde esta perspectiva, la determinación de la medida adecuada exige ponderar el beneficio de prevenir el daño y el costo que la intervención produce sobre la libertad de expresión; por ello, una reducción de visibilidad puede resultar menos gravosa que la eliminación, aunque su procedencia dependerá de las características concretas del contenido y de la intensidad del riesgo involucrado (Howard & Kira, 2026: 507-508).

4. Suspensión o bloqueo de cuentas

Las medidas también pueden recaer sobre la cuenta o perfil utilizado para efectuar la conducta, y no exclusivamente sobre una publicación determinada. De esta manera, una plataforma puede suspender temporalmente una cuenta o proceder a su desactivación permanente cuando es utilizada para realizar o reiterar conductas contrarias a sus normas.

Desde una perspectiva centrada en las víctimas de NCII, Harlan, Jo y Crockett plantean que las plataformas debieran transparentar los criterios conforme a los cuales las cuentas de quienes publican estos contenidos son eliminadas o deshabilitadas permanentemente, vinculando estas medidas con la prevención de nuevas conductas de creación y distribución de material íntimo no consentido (Harlan et al., 2026: 23).

No obstante, este tipo de medida presenta una intensidad mayor que la intervención sobre una publicación individual. En sus Directrices sobre gobernanza de plataformas digitales, UNESCO incluye entre las posibles respuestas la limitación de la amplificación, la desmonetización, el retiro de contenidos, pero precisa que la eliminación o retiro y la suspensión o bloqueo de cuentas deben utilizarse como último recurso y en los casos más extremos, de acuerdo con un criterio de proporcionalidad (UNESCO, 2023: 45).

5. Prevención de la recirculación mediante tecnologías de hashing

El retiro de una publicación determinada puede resultar insuficiente cuando el mismo archivo vuelve a ser cargado o distribuido en otros servicios. Frente a ello, se han desarrollado mecanismos destinados no solo a eliminar el contenido ya publicado, sino también a evitar su reaparición.

Entre ellos se encuentra el denominado *hash matching*. Mediante esta tecnología se genera una representación o "huella" digital del archivo que permite identificar posteriormente copias coincidentes y actuar frente a nuevos intentos de publicación.

Según Harlan, Jo y Crockett, el intercambio de *hashes* de NCII previamente verificado entre plataformas puede acelerar la detección de nuevas copias y evitar que el mismo contenido vuelva a circular. Las autoras destacan, sin embargo, que la utilización e intercambio de estos identificadores continúa siendo voluntaria e irregular entre distintas plataformas (Harlan et al., 2026: 20). Por ello, proponen extender sistemas interoperables de *hash matching*, de manera que la víctima pueda generar o registrar el identificador del contenido una sola vez, sin verse obligada a localizar y denunciar separadamente cada nueva copia en las diferentes plataformas (Harlan et al., 2026: 20).

Esta técnica responde a una dificultad propia del entorno digital: aun después de un retiro exitoso, el material puede reaparecer. Huber y Ward advierten precisamente sobre la existencia de sitios que desaparecen y posteriormente vuelven a estar disponibles, así como sobre la dificultad que ello genera para las víctimas al intentar determinar si sus imágenes han sido definitivamente retiradas; frente a este fenómeno, las autoras identifican el hashing como una herramienta con potencial preventivo si su utilización se extendiera entre plataformas (Huber & Ward, 2025: 45).

6. Preservación de la evidencia digital

La eliminación o bloqueo del contenido presenta una cuestión adicional cuando los hechos son objeto de investigación penal. En estos casos concurren dos objetivos diferentes: por una parte, evitar la continuidad de la exposición y del daño a la víctima; por otra, conservar los elementos necesarios para acreditar posteriormente los hechos investigados.

Ambos objetivos no son necesariamente incompatibles. Si bien referida específicamente a contenidos de abuso sexual de menores y retransmisiones de actos terroristas, UNESCO señala que las plataformas deben actuar rápidamente para retirarlos de circulación, pero, simultáneamente, garantizar que aquellos materiales que puedan resultar vitales para la investigación y el enjuiciamiento de delitos sean conservados y salvaguardados de manera segura para su utilización por las autoridades competentes (UNESCO, 2023: 44).

Esta distinción adquiere especial importancia en materia de violencia digital. La preservación de la evidencia no exige, por sí misma, que el contenido continúe públicamente accesible. En consecuencia, desde una perspectiva más funcional, puede distinguirse entre la indisponibilidad pública del material y la conservación segura de los datos necesarios para la investigación penal.

La experiencia recogida por la Cámara de los Comunes británica ilustra las dificultades que pueden surgir cuando ambas funciones no se encuentran adecuadamente coordinadas. La *Revenge Porn Helpline* informó al Comité que, en ocasiones, la policía había solicitado no retirar contenidos NCII para que estos permanecieran en línea durante el proceso judicial. Frente a ello, representantes policiales reconocieron la falta de un modelo uniforme de investigación y señalaron que mantener las imágenes disponibles podía producir una revictimización constante; asimismo, se indicó que en otros casos el contenido era retirado antes de iniciarse la investigación, evidenciando una práctica inconsistente (Women and Equalities Committee, 2025: 36-37).

El Comité recomendó, por ello, que el *College of Policing*, *Ofcom* y la *Revenge Porn Helpline* desarrollaran conjuntamente directrices para mejorar la respuesta policial, incluyendo los pasos necesarios para procurar que los contenidos sean retirados y bloqueados con carácter prioritario (Women and Equalities Committee, 2025: 38).

II. Medidas de protección en la legislación comparada

Este apartado examina cómo las fórmulas descritas en la sección anterior se incorporan en instrumentos normativos concretos. Se analiza, en primer término, la Ley Modelo Interamericana del MESECVI, como estándar regional de referencia, y luego la legislación de Australia, México y Reino Unido.

Para facilitar la comparación, cada caso se estructura en torno a los mismos ocho parámetros : tipo de medida, autoridad facultada, etapa, presupuesto, destinatario, plazo de cumplimiento, mecanismos de revisión y preservación de la evidencia digital.

1. Ley Modelo Interamericana

El 10 de diciembre de 2025, el Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI) publicó la Ley Modelo Interamericana para Prevenir, Sancionar y Erradicar la Violencia Digital contra las Mujeres basada en Género. El instrumento fue elaborado por el Comité de Expertas del MESECVI, con el apoyo de la República de Italia, a partir de un proceso participativo en el que intervinieron Estados parte de la Organización de los Estados Americanos (OEA), organismos internacionales y regionales, instituciones de derechos humanos, organizaciones de la sociedad civil y la academia (MESECVI, s.f.).

La Ley Modelo contempla diversas medidas destinadas a prevenir y detener la circulación de contenidos que constituyan violencia digital contra las mujeres basada en género, así como mecanismos dirigidos a proteger a las víctimas y preservar la evidencia digital. En particular, establece medidas de moderación de contenidos y servicios, procedimientos para el cumplimiento de órdenes de autoridades competentes y un régimen de medidas precautelares y cautelares.

a. Tipo de medida

La Ley Modelo contempla distintas formas de intervención sobre los contenidos y servicios digitales. Entre ellas se encuentran la suspensión, restricción y eliminación de contenidos o servicios, la suspensión temporal y progresiva del acceso a determinados servicios, la desactivación de funciones de monetización o promoción del contenido identificado como violencia digital y, en determinados casos, el cierre de cuentas (artículo 26). Asimismo, las autoridades judiciales o administrativas pueden ordenar la remoción temporal y controlada de contenidos, la restricción de perfiles, accesos, funcionalidades o interacciones digitales y otras medidas destinadas a prevenir la continuidad del daño o la revictimización (artículo 41).

La regulación contempla además una medida específica para los casos que involucren material de violencia o explotación sexual de niñas y adolescentes, estableciendo el cierre inmediato de la cuenta involucrada y la eliminación del contenido ilícito o nocivo (artículo 26).

b. Autoridad facultada

Las medidas pueden ser adoptadas por distintas autoridades según su naturaleza.

Las medidas precautelares pueden ser adoptadas por los órganos competentes para recibir denuncias o solicitadas por estos a la autoridad judicial o administrativa correspondiente, cuando exista evidencia de daño inminente o riesgo de pérdida o alteración de elementos de prueba (artículo 40).

Por su parte, las medidas cautelares son impuestas durante el proceso por el tribunal competente, a petición del Ministerio Público, de la víctima, de su representante legal o de los órganos competentes (artículo 40).

En cuanto a las medidas que impliquen el bloqueo o restricción de derechos fundamentales, estas deben ser autorizadas y/o revisadas por una autoridad judicial competente (artículo 41).

c. Etapa o momento en que puede disponerse

La Ley Modelo permite adoptar medidas antes del inicio de un proceso judicial o administrativo, cuando exista evidencia de un daño inminente a la integridad de la víctima o riesgo de pérdida o alteración de elementos de prueba. Estas medidas son calificadas como precautelares (artículo 40). Las medidas cautelares, en cambio, pueden adoptarse durante el proceso judicial y deben resolverse inmediatamente cuando sean solicitadas dentro del plazo legal correspondiente (artículo 40).

d. Presupuesto o estándar requerido

La adopción de las medidas precautelares y cautelares debe ajustarse a los principios de legalidad, necesidad y proporcionalidad y observar los estándares del derecho internacional de los derechos humanos (artículo 40). Para las medidas que impliquen bloqueo o restricción de derechos fundamentales se exige, adicionalmente, autorización y/o revisión judicial y el respeto del principio de responsabilidad ulterior (artículo 41).

Respecto de las medidas de moderación de contenidos, el artículo 26 establece que su adopción procede cuando se determine la existencia de manifestaciones de violencia digital contra las mujeres basada en género, y dispone la aplicación escalonada y proporcional de las sanciones.

e. Destinatario de la orden

El artículo 30 de la ley establece que, cuando el punto de contacto designado ante las autoridades del Estado o el representante legal del intermediario reciba una orden emitida por una autoridad judicial o administrativa nacional competente, deberá darle cumplimiento respecto de los contenidos comprendidos en el ámbito de aplicación de la Ley Modelo o proporcionar la información específica solicitada.

f. Plazo de cumplimiento

Cuando se trate de una orden emitida por una autoridad competente, el intermediario debe actuar sin dilación y dar cumplimiento inmediato a las medidas requeridas (artículo 30). En los casos de material de violencia o explotación sexual de niñas y adolescentes, el artículo 26 establece igualmente una actuación inmediata respecto del cierre de la cuenta y la eliminación del contenido.

g. Mecanismos de revisión o impugnación

Las medidas precautelares y cautelares quedan sujetas a control judicial inmediato y las decisiones deben ser debidamente motivadas y notificadas a las partes involucradas (artículos 40 y 42). Asimismo, los tribunales competentes tienen atribuciones para la imposición, revisión, impugnación y ejecución de las medidas precautelares y para la emisión, revisión y suspensión de las medidas cautelares (artículo 42).

h. Preservación de la evidencia digital

La conservación de la evidencia constituye expresamente uno de los objetivos de las medidas precautelares y cautelares. En particular, el artículo 41 permite ordenar la remoción temporal y controlada de contenidos digitales que puedan constituir violencia digital contra las mujeres, asegurando simultáneamente la conservación de dicho material como prueba, conforme a los protocolos establecidos. De esta manera, la regulación diferencia entre la indisponibilidad pública del contenido y su conservación para efectos probatorios (artículo 41).

2. Australia

En Australia, la respuesta jurídica frente a los contenidos digitales nocivos está en la Ley de Seguridad en Línea (*Online Safety Act* - OSA) de 2021, cuyo texto vigente es la compilación n.º 4, del 12 de septiembre de 2026. A diferencia de otros modelos, la ley no confía la retirada de contenidos a los tribunales ni al Ministerio Público. La encarga a una autoridad administrativa especializada, el Comisionado de Seguridad en Línea (*eSafety Commissioner*), y organiza un procedimiento de quejas y órdenes de retirada (*removal notices*) distinto para cada tipo de contenido. En este apartado se analizan tres: el ciberacoso dirigido a menores de edad (Parte 5), la difusión no consentida de imágenes íntimas (Parte 6) y el ciberabuso dirigido a personas adultas (Parte 7).

Para los tres regímenes, la ley entiende que un contenido ha sido “retirado” (*removed*) de un servicio cuando ningún usuario final en Australia puede acceder a él ni recibirlo (sección 12, OSA). Por “menor” se entiende a quien no ha cumplido 18 años y por “adulto” a quien tiene 18 años o más. En ambos casos, la persona debe residir habitualmente en Australia para quedar protegida (sección 5, OSA).

2.1 Ciberacoso dirigido a un niño, niña o adolescente (NNA) (cyber-bullying material targeted at an Australian child)

La sección 6 de la OSA define este material como el contenido difundido en un servicio de redes sociales, un servicio electrónico relevante o un servicio de Internet designado, respecto del cual una persona razonable común concluiría:

- que es probable que el material tuviera la intención de producir un efecto sobre un NNA australiano en particular; y
- que el material probablemente tendría sobre ese NNA el efecto de amenazarlo, intimidarlo, acosarlo o humillarlo gravemente.

El efecto puede ser directo, si el niño, niña o adolescente accede al material, o indirecto, si acceden a él terceras personas (sección 6(2), OSA). No se considera ciberacoso el contenido que publica una persona con autoridad sobre el menor cuando actúa en ejercicio legítimo de esa autoridad y de forma razonable (sección 6(4), OSA).

a. Tipo de medida

La ley contempla tres instrumentos:

- Una orden de retirada (*removal notice*) dirigida al proveedor del servicio, que le exige retirar el material (sección 65(1)(f), OSA).
- Una orden de retirada dirigida al proveedor de alojamiento (*hosting service provider*), que le exige adoptar todas las medidas razonables para dejar de alojar el material (sección 66(1)(g), OSA).
- Un aviso al usuario final (*end-user notice*), dirigido a quien publicó el material. Puede exigirle retirarlo, abstenerse de publicar nuevo material de ciberacoso contra el mismo niño y pedirle disculpas en la forma y el plazo que fije el aviso (sección 70(1), OSA).

La orden debe identificar el material, en la medida en que sea razonablemente posible, de un modo que permita a su destinatario cumplirla (secciones 65(2), 66(2) y 70(2), OSA). Además, con el consentimiento del denunciante, el Comisionado puede enviar al proveedor una notificación no vinculante en la que identifica el material y declara que lo considera ciberacoso. Si en los últimos 12 meses ha habido dos o más casos de este material contrarios a las condiciones de uso del servicio, puede también publicar una declaración al respecto en su sitio web (sección 73, OSA).

Esta parte de la ley no establece mecanismos de exclusión de resultados de búsqueda ni un sistema de identificación mediante *hashes* para impedir técnicamente que el contenido vuelva a circular.

b. Autoridad facultada

La facultad corresponde exclusivamente al Comisionado de Seguridad en Línea, que actúa por vía administrativa y sin necesidad de autorización judicial (secciones 65(1), 66(1) y 70(1), OSA). El Comisionado puede investigar las quejas como estime conveniente y obtener información de las personas que considere pertinentes (sección 31, OSA). Para ello dispone de las facultades de investigación de la Parte 14 (sección 198, OSA).

c. Etapa o momento en que puede disponerse

El procedimiento empieza con una queja ante el Comisionado (sección 30, OSA), que pueden presentar:

- el propio NNA (sección 30(1), OSA);
- su padre, madre o tutor, o una persona que el NNA haya autorizado (sección 30(2), OSA);
- quien, siendo ya adulto, fue víctima siendo menor de edad, siempre que lo haga dentro de un plazo razonable desde que tomó conocimiento del hecho y dentro de los 6 meses siguientes a cumplir 18 años (sección 30(3), OSA).

Para una orden dirigida al proveedor del servicio o al proveedor de alojamiento, la ley exige además un paso previo ante la plataforma. El material debe haber sido denunciado antes ante el proveedor, y este no debe haberlo retirado en 48 horas o en el plazo mayor que permita el Comisionado (secciones 65(1)(b)-(c) y 66(1)(b)-(c), OSA). Esa denuncia previa se acredita con el comprobante o número de reclamo que emita el servicio. Si el servicio no los emite, se acredita con una captura de pantalla, una declaración jurada u otro medio que determine el Comisionado (sección 30(4)-(7), OSA). El aviso al usuario final no requiere esa denuncia previa ante la plataforma (sección 70(1), OSA).

d. Presupuesto o estándar requerido

El Comisionado debe estar convencido (*satisfied*) de que el material es o fue ciberacoso dirigido a un niño australiano (secciones 65(1)(e), 66(1)(e) y 70(1)(c), OSA). Esa calificación se hace con el criterio objetivo de la persona razonable común de la sección 6 y exige un efecto grave: amenaza, intimidación, acoso o humillación seria (sección 6(1)(b), OSA). Para la orden al proveedor de alojamiento, se exige además que el material esté efectivamente alojado por él (sección 66(1)(f), OSA).

e. Destinatario de la orden

La orden puede dirigirse:

- al proveedor de un servicio de redes sociales, de un servicio electrónico relevante o de un servicio de Internet designado (sección 65, OSA);
- al proveedor de alojamiento (sección 66, OSA);
- al usuario final que publicó el material (sección 70, OSA).

f. Plazo de cumplimiento

Las órdenes dirigidas al proveedor del servicio y al proveedor de alojamiento deben cumplirse dentro de las 24 horas siguientes a su notificación, o en el plazo mayor que permita el Comisionado (secciones 65(1)(g) y 66(1)(h), OSA). Para el aviso al usuario final, la ley no fija un plazo: lo determina el propio aviso (sección 70(1)(e)(ii) y (g)(ii), OSA).

El incumplimiento de una orden de retirada es una infracción civil sancionada con 500 unidades de multa (sección 67, OSA). Puede dar lugar a una amonestación formal (sección 68, OSA), a avisos de infracción (sección 163(1)(e), OSA), a compromisos exigibles (sección 164, OSA) y a medidas cautelares o *injunctions* (sección 165, OSA). El incumplimiento del aviso al usuario final no tiene multa civil. Solo puede exigirse mediante una *injunction* (sección 71, OSA) y dar lugar a una amonestación formal (sección 72, OSA).

g. Mecanismos de revisión o impugnación

Si el Comisionado decide no emitir la orden, debe comunicarlo por escrito a quien presentó la queja (secciones 65(3) y 66(3), OSA).

Las decisiones pueden impugnarse ante el Tribunal de Revisión Administrativa (*Administrative Review Tribunal*):

- La orden al proveedor del servicio puede ser impugnada por el proveedor y por el usuario que publicó el material (sección 220(2)-(3), OSA).
- La orden al proveedor de alojamiento pueden impugnarla ese proveedor y el usuario que publicó el material (sección 220(6)-(7), OSA).
- El aviso al usuario final también es impugnable (sección 220(10), OSA).
- La negativa a emitir una orden pueden impugnarla el denunciante o la persona afectada, o un tercero con su consentimiento (sección 220(4)-(5) y (8)-(9), OSA).

La ley obliga además al Comisionado a establecer y publicar un sistema de revisión interna de estas decisiones, que le permite confirmarlas, modificarlas o revocarlas (sección 220A, OSA).

h. Preservación de la evidencia digital

La Parte 5 no contiene una obligación expresa de resguardar o conservar el contenido cuya retirada se ordena. La retirada se define por la imposibilidad de acceso desde Australia (sección 12, OSA), no por la destrucción del material.

Para la investigación, el Comisionado puede:

- exigir al proveedor información sobre la identidad o los datos de contacto del usuario final (sección 194, OSA);
- citar a personas para que comparezcan, respondan preguntas o entreguen documentos (sección 199, OSA);
- exigir que se le exhiban documentos y permitir que los copie (sección 203, OSA).

Estas facultades sirven para obtener pruebas, pero no configuran un deber específico de conservar el contenido retirado.

2.2 Ciberabuso dirigido a una persona adulta australiana (*cyber-abuse material targeted at an Australian adult*)

La sección 7 de la OSA define este material como el contenido difundido en uno de los servicios mencionados respecto del cual:

una persona razonable común (*an ordinary reasonable person*) concluiría que es probable que el material tuviera la intención de causar un daño grave a un adulto australiano en particular; y una persona razonable común en la posición de ese adulto consideraría el material, en todas las circunstancias, amenazante, acosador u ofensivo.

La ley define el daño grave (*serious harm*) como un daño físico grave o un daño grave a la salud mental, temporal o permanente. Este último incluye el daño psicológico grave y la angustia grave, pero no las simples reacciones emocionales corrientes, como la angustia, el pesar, el miedo o la ira (sección 5, OSA). Para decidir si un material es “ofensivo”, se consideran los estándares de moralidad y decencia generalmente aceptados, el mérito literario, artístico o educativo del material y su carácter general (sección 8, OSA).

a. Tipo de medida

La ley contempla tres órdenes de retirada:

- Una orden dirigida al proveedor del servicio, que le exige adoptar todas las medidas razonables para retirar el material (sección 88(1)(f), OSA).
- Una orden dirigida al usuario final que lo publicó, que le exige adoptar todas las medidas razonables para retirarlo (sección 89(1)(g), OSA).
- Una orden dirigida al proveedor de alojamiento, que le exige adoptar todas las medidas razonables para dejar de alojarlo (sección 90(1)(g), OSA).

El material debe identificarse en la orden de modo suficiente para que pueda cumplirse (secciones 88(2), 89(2) y 90(2), OSA). El Comisionado puede también enviar notificaciones no vinculantes y publicar declaraciones sobre casos reiterados (sección 93, OSA).

A diferencia del régimen de NNA, el usuario final no puede ser obligado a abstenerse de publicar nuevo material ni a pedir disculpas. La ley tampoco prevé aquí exclusión de resultados de búsqueda ni identificación mediante *hashes*.

b. Autoridad facultada

La facultad corresponde al Comisionado de Seguridad en Línea, por vía administrativa (secciones 88(1), 89(1) y 90(1), OSA). Puede investigar las quejas con las facultades generales de la sección 37 y las de la Parte 14 (secciones 37 y 198, OSA).

c. Etapa o momento en que puede disponerse

El procedimiento empieza con una queja ante el Comisionado, que puede presentar el propio adulto o una persona que él haya autorizado (sección 36(1)-(2), OSA). Para cualquiera de las tres órdenes, la ley exige además que:

- el material haya sido denunciado antes ante el proveedor del servicio; y
- el proveedor no lo haya retirado en 48 horas o en el plazo mayor que permita el Comisionado (secciones 88(1)(c)-(d), 89(1)(c)-(d) y 90(1)(c)-(d), OSA).

La denuncia previa se acredita del mismo modo que en el régimen de menores: con el comprobante o número de reclamo, o con una captura de pantalla, una declaración jurada u otro medio que determine el Comisionado (sección 36(3)-(6), OSA).

d. Presupuesto o estándar requerido

El Comisionado debe estar convencido de que el material es o fue ciberabuso dirigido a un adulto australiano (secciones 88(1)(b), 89(1)(b) y 90(1)(b), OSA). Este estándar es más exigente que el aplicable a los menores por dos razones. Primero, requiere una probable intención de causar un daño grave, y el concepto de daño grave excluye las reacciones emocionales corrientes (secciones 5 y 7(1)(b), OSA). Segundo, el material debe resultar, además, amenazante, acosador u ofensivo para una persona razonable en la posición de la víctima (sección 7(1)(c), OSA).

Para la orden al usuario final, el material debe haber sido publicado por él (sección 89(1)(f), OSA). Para la orden al proveedor de alojamiento, el material debe estar alojado por ese proveedor (sección 90(1)(f), OSA).

e. Destinatario de la orden

La orden puede dirigirse:

- al proveedor de un servicio de redes sociales, de un servicio electrónico relevante o de un servicio de Internet designado (sección 88, OSA);
- al usuario final que publicó el material (sección 89, OSA);
- al proveedor de alojamiento (sección 90, OSA).

f. Plazo de cumplimiento

Las tres órdenes deben cumplirse dentro de las 24 horas siguientes a su notificación, o en el plazo mayor que permita el Comisionado (secciones 88(1)(g), 89(1)(h) y 90(1)(h), OSA).

El incumplimiento se sanciona con 500 unidades de multa (sección 91, OSA) y puede dar lugar a una amonestación formal (sección 92, OSA) y a avisos de infracción (sección 163(1)(i), OSA).

g. Mecanismos de revisión o impugnación

Si el Comisionado decide no emitir la orden, debe comunicarlo por escrito al denunciante (secciones 88(3), 89(3) y 90(3), OSA).

Las decisiones pueden impugnarse ante el Tribunal de Revisión Administrativa (*Administrative Review Tribunal*):

- La orden al proveedor del servicio pueden impugnarla el proveedor y el usuario que publicó el material (sección 220(2)-(3), OSA).
- La orden al proveedor de alojamiento pueden impugnarla ese proveedor y el usuario que publicó el material (sección 220(6)-(7), OSA).
- La orden al usuario final también es impugnable (sección 220(10A), OSA).
- La negativa a emitir una orden pueden impugnarla el denunciante o la persona afectada, o un tercero con su consentimiento (sección 220(4)-(5) y (8)-(9), OSA).

Todas estas decisiones admiten también la revisión interna de la sección 220A de la OSA.

h. Preservación de la evidencia digital

Como en los otros dos regímenes, la Parte 7 no establece una obligación expresa de resguardar o conservar el contenido cuya retirada se ordena. Para la investigación rigen las facultades de obtener datos de identidad del usuario final (sección 194, OSA), citar a declarar (sección 199, OSA) y exigir la exhibición de documentos (sección 203, OSA).

2.3 Difusión no consentida de imágenes íntimas (*non-consensual sharing of intimate images*)

La sección 15 de la OSA define la imagen íntima como una imagen fija o en movimiento que muestra, o parece mostrar, alguna las siguientes situaciones en circunstancias en que una persona razonable común esperaría tener privacidad:

- las zonas genital o anal de la persona, desnudas o cubiertas por ropa interior;
- los senos, si se trata de una mujer o de una persona transgénero o intersexual;

- a la persona desvestida, usando el baño, duchándose, bañándose o realizando un acto sexual que normalmente no se realiza en público;
- a la persona sin la vestimenta de significado religioso o cultural que usa habitualmente en público.

Las imágenes que parecen mostrar a la persona (*depicts, or appears to depict*) incluyen el contenido simulado o manipulado (sección 15(2)-(4), OSA).

La sección 75 prohíbe al usuario final publicar, o amenazar con publicar, una imagen íntima de otra persona sin su consentimiento, cuando la persona retratada o quien publica la imagen reside habitualmente en Australia. La infracción se sanciona con 500 unidades de multa (sección 75(1)-(2), OSA).

a. Tipo de medida

La ley contempla cuatro instrumentos:

- Una orden de retirada dirigida al proveedor del servicio, que le exige adoptar todas las medidas razonables para retirar la imagen (sección 77(1)(e), OSA).
- Una orden de retirada dirigida al usuario final que la publicó (sección 78(1)(f), OSA).
- Una orden de retirada dirigida al proveedor de alojamiento, que le exige adoptar todas las medidas razonables para dejar de alojarla (sección 79(1)(f), OSA).
- Una instrucción correctiva (*remedial direction*) dirigida a quien infringió la prohibición de la sección 75. Le exige adoptar las medidas que se indiquen para no volver a infringirla (sección 83(2), OSA).

La imagen debe identificarse en la orden de modo suficiente para que pueda cumplirse (secciones 77(2), 78(2) y 79(2), OSA). El Comisionado puede también enviar al proveedor notificaciones no vinculantes y publicar declaraciones sobre casos reiterados (sección 85, OSA).

b. Autoridad facultada

Todas estas medidas corresponden al Comisionado de Seguridad en Línea, por vía administrativa (secciones 77(1), 78(1), 79(1) y 83(2), OSA). Puede investigar las quejas con las facultades generales de la sección 34 y las de la Parte 14 (secciones 34 y 198, OSA).

c. Etapa o momento en que puede disponerse

El procedimiento puede comenzar de dos maneras:

- Con una queja (*complaint*) por infracción de la sección 75. Puede presentarla la persona que aparece en la imagen o un tercero en su nombre: alguien a quien ella haya autorizado, o su padre, madre o tutor si es menor de 16 años o está incapacitada para administrar sus asuntos (sección 32(1) y (3), OSA). Si el denunciante no puede identificar al autor, debe declararlo así (sección 32(2) y (5), OSA).
- Con un aviso de oposición (*objection notice*). Puede presentarlo la persona que aparece en la imagen, o un tercero en su nombre, siempre que la persona retratada o quien publicó la imagen resida habitualmente en Australia o que la imagen esté alojada en Australia (sección 33(1) y (3), OSA). Este aviso procede aunque la persona haya consentido antes la publicación (sección 33(2) y (5), OSA). Una vez recibido, el Comisionado puede evaluar si emite una orden de retirada (sección 35, OSA).

A diferencia de los regímenes de ciberacoso a menores y ciberabuso a adultos, aquí no es necesario haber denunciado antes el contenido ante la plataforma ni esperar un plazo antes de acudir al Comisionado (secciones 77 a 79, OSA).

d. Presupuesto o estándar requerido

Si el procedimiento empezó con una queja, el Comisionado debe estar convencido de que la persona retratada no consintió la difusión de la imagen en el servicio (secciones 77(1)(c), 78(1)(d) y 79(1)(c), OSA). En cualquier caso, la difusión no debe ser una "difusión exenta" (*exempt provision*) (secciones 77(1)(d), 78(1)(e) y 79(1)(e), OSA).

Una difusión es exenta cuando la imagen se difunde:

- porque es necesaria para hacer cumplir la ley o investigar una infracción (sección 86(1)(d), OSA);
- para un procedimiento judicial (sección 86(1)(e), OSA);
- con fines médicos o científicos genuinos (sección 86(1)(f), OSA);
- en condiciones que una persona razonable común consideraría aceptables. Para evaluarlo se consideran la naturaleza de la imagen, el contexto, la edad y la vulnerabilidad de la persona retratada, la afectación de su privacidad y su relación con quien la publicó (sección 86(1)(g), OSA).

Para la instrucción correctiva, basta con que la persona haya infringido o esté infringiendo la sección 75 (sección 83(1), OSA).

e. Destinatario de la orden

La orden puede dirigirse:

- al proveedor de un servicio de redes sociales, de un servicio electrónico relevante o de un servicio de Internet designado (sección 77, OSA);
- al usuario final que publicó la imagen (sección 78, OSA);
- al proveedor de alojamiento (sección 79, OSA).

La instrucción correctiva se dirige a quien infringió la prohibición de publicar sin consentimiento (sección 83, OSA).

f. Plazo de cumplimiento

Las tres órdenes de retirada deben cumplirse dentro de las 24 horas siguientes a su notificación, o en el plazo mayor que permita el Comisionado (secciones 77(1)(f), 78(1)(g) y 79(1)(g), OSA).

El incumplimiento de estas órdenes se sanciona con 500 unidades de multa (sección 80, OSA) y el de la instrucción correctiva, también con 500 (sección 83(3), OSA). Además, el Comisionado puede emitir amonestaciones formales (secciones 76, 81 y 84, OSA) y avisos de infracción (sección 163(1)(f)-(h), OSA).

g. Mecanismos de revisión o impugnación

Si el Comisionado decide no emitir la orden, debe comunicarlo por escrito a quien presentó la queja o el aviso de oposición (secciones 77(3), 78(3) y 79(3), OSA).

Las decisiones pueden impugnarse ante el Tribunal de Revisión Administrativa:

- La orden dirigida al proveedor del servicio puede ser impugnarla por el proveedor del servicio y por el usuario que publicó la imagen (sección 220(2)-(3), OSA).
- La orden dirigida al proveedor de alojamiento puede ser impugnada por dicho proveedor y por el usuario que publicó la imagen (sección 220(6)-(7), OSA).
- La orden al usuario final también es impugnable (sección 220(10A), OSA), al igual que la instrucción correctiva (sección 220(12), OSA).
- La negativa a emitir una orden pueden ser impugnada por el denunciante o por la persona afectada, o por un tercero con su consentimiento (sección 220(4)-(5) y (8)-(9), OSA).

Todas estas decisiones admiten también la revisión interna de la sección 220A de la OSA.

h. Preservación de la evidencia digital

La Parte 6 tampoco establece un deber expreso de resguardar el contenido cuya retirada se ordena. Ahora bien, la ley considera exenta la difusión de una imagen íntima cuando es necesaria para hacer cumplir la ley, investigar una infracción o sustanciar un procedimiento judicial (sección 86(1)(d)-(e), OSA). Así, el uso de la imagen como prueba queda fuera de la prohibición, aunque la ley no impone su conservación.

Para la investigación rigen las facultades de obtener datos de identidad del usuario final (sección 194, OSA), citar a declarar (sección 199, OSA) y exigir la exhibición de documentos (sección 203, OSA).

3. México

En México, la respuesta jurídica frente a los efectos nocivos de la violencia digital se articula principalmente a través de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencias (LGAMVLV), que reconoce expresamente esta forma de violencia y establece mecanismos específicos para intervenir sobre los contenidos digitales que la generan. El artículo 20 Quáter define 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.
>
> 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.

El artículo 20 Sexies establece medidas de protección dirigidas específicamente a interrumpir, bloquear, destruir o eliminar determinados contenidos digitales y contempla expresamente su resguardo y conservación.

a. Tipo de medida

La LGAMVLV contempla expresamente medidas de interrupción, bloqueo, destrucción o eliminación de imágenes, audios o videos relacionados con la investigación. Estas medidas pueden ser ordenadas respecto de contenidos alojados en plataformas digitales, medios de comunicación, redes sociales o

páginas electrónicas. La norma exige, además, identificar al proveedor de servicios en línea responsable de la administración del sistema, sitio o plataforma y precisar la localización del contenido mediante el correspondiente Localizador Uniforme de Recursos (URL) (art. 20 Sexies, LGAMVLV).

b. Autoridad facultada

Conforme a la LGAMVLV, las medidas de protección pueden ser ordenadas por el Ministerio Público, la jueza o el juez, según corresponda. La norma dispone que estas autoridades ordenarán de manera inmediata las medidas de protección necesarias para garantizar la integridad de la víctima (art. 20 Sexies, LGAMVLV).

El régimen debe entenderse, en relación con el artículo 137 del Código Nacional de Procedimientos Penales (CNPP), que faculta al Ministerio Público para ordenar, fundada y motivadamente, medidas de protección idóneas cuando estime que el imputado representa un riesgo inminente para la seguridad de la víctima u ofendido. El mismo artículo establece que, tratándose de delitos relacionados con las violencias de género contra las mujeres, se aplicará supletoriamente la LGAMVLV.

c. Etapa o momento en que puede disponerse

La Ley establece que las medidas deben ordenarse de manera inmediata, tratándose de situaciones de violencia digital o mediática y con el objeto de garantizar la integridad de la víctima. Para ello, deben haberse satisfecho previamente los requisitos legales y el contenido debe encontrarse relacionado con la investigación. La orden debe identificar al proveedor del servicio en línea y la localización precisa del contenido en Internet (artículo 20 Sexies, LGAMVLV).

Por su parte, cuando las medidas se adopten en el marco de las facultades generales de protección del Ministerio Público, el artículo 137 del CNPP exige que este estime que el imputado representa un riesgo inminente para la seguridad de la víctima u ofendido y que la medida sea fundada y motivada (artículo 137, CNPP).

d. Presupuesto o estándar requerido

La legislación mexicana vincula la adopción de estas medidas con la necesidad de garantizar la integridad de la víctima y exige la previa satisfacción de los requisitos legales. Su ámbito material se determina a partir de la definición de violencia digital contenida en el artículo 20 Quáter de la LGAMVLV.

Esta última disposición comprende, entre otros supuestos, la exposición, distribución, difusión, exhibición, transmisión, comercialización, oferta, intercambio o compartición, sin consentimiento, aprobación o autorización, de imágenes, audios o videos reales o simulados de contenido íntimo sexual que causen daño psicológico o emocional. También comprende otros actos dolosos realizados mediante TIC que causen daño a la intimidad, privacidad o dignidad de las mujeres (arts. 20 Quáter y 20 Sexies, LGAMVLV).

En materia penal, el Código Penal Federal contempla además el delito de violación a la intimidad sexual, que sanciona, entre otras conductas, la divulgación, distribución o publicación de imágenes, videos o audios de contenido íntimo sexual de una persona adulta sin su consentimiento, aprobación o autorización (art. 199 Octies, Código Penal Federal).

e. Destinatario de la orden

La LGAMVLV permite dirigir la orden a empresas de plataformas digitales, medios de comunicación, redes sociales o páginas electrónicas, así como a personas físicas o morales. De esta manera, la medida puede dirigirse tanto a quienes administran los servicios o espacios digitales donde se encuentra alojado el contenido como a otros sujetos expresamente comprendidos por la disposición (art. 20 Sexies, LGAMVLV).

La misma disposición establece que las plataformas digitales, medios de comunicación, redes sociales o páginas electrónicas deben dar aviso inmediato al usuario que compartió el contenido, informándole que será inhabilitado en cumplimiento de una orden judicial (art. 20 Sexies, LGAMVLV).

f. Plazo de cumplimiento

La Ley establece que las medidas deben ser ordenadas de manera inmediata por la autoridad competente. Sin embargo, la disposición no establece un plazo específico —por ejemplo, de 24 o 48 horas— para que el destinatario material de la orden ejecute la interrupción, el bloqueo, la destrucción o la eliminación del contenido.

Por tanto, debe distinguirse entre la inmediatez exigida para la adopción de la medida por la autoridad y la ausencia de un plazo de cumplimiento expresamente fijado en esta disposición para las plataformas u otros destinatarios.

g. Mecanismos de revisión o impugnación

La LGAMVLV no establece un mecanismo específico de revisión o impugnación de las órdenes de interrupción, bloqueo, destrucción o eliminación dirigidas a los proveedores de servicios, plataformas digitales, redes sociales, páginas electrónicas o demás destinatarios (art. 20 Sexies, LGAMVLV)..

El CNPP, por su parte, contempla mecanismos de control judicial respecto de determinadas medidas de protección. En particular, el artículo 137 establece que, dentro de los cinco días siguientes a la imposición de las medidas previstas en sus fracciones I, II y III, debe celebrarse una audiencia en la que el juez podrá cancelarlas, ratificarlas o modificarlas mediante la imposición de las medidas cautelares correspondientes. Esta regla no se refiere específicamente a las medidas de contenido digital previstas en el artículo 20 Sexies de la LGAMVLV, por lo que no corresponde extenderla directamente a estas últimas (art. 137, CNPP).

h. Preservación de la evidencia digital

Una de las características del régimen mexicano es que el propio artículo 20 Sexies de la LGAMVLV establece expresamente una obligación vinculada con la preservación de la evidencia digital. La autoridad que ordene las medidas de protección deberá solicitar el resguardo y conservación lícita e idónea del contenido denunciado, de acuerdo con sus características.

Esta previsión permite distinguir conceptualmente entre la medida dirigida a impedir que el contenido continúe produciendo efectos nocivos para la víctima, mediante su interrupción, bloqueo, destrucción o eliminación, y la necesidad de conservar dicho contenido para los fines propios de la investigación.

4. Reino Unido

En el Reino Unido, el régimen aplicable a la difusión no consentida de imágenes íntimas se estructura principalmente a partir de la Ley sobre Seguridad en línea (*Online Safety Act* - OSA) de 2023,

complementado por las modificaciones introducidas por el *Crime and Policing Act* 2026. El OSA incorpora como conducta delictiva la divulgación o amenaza de divulgación de fotografías o videos íntimos sin consentimiento mediante el nuevo artículo 66B de la *Sexual Offences Act 2003*. Paralelamente, el OSA impone a los proveedores de servicios regulados obligaciones específicas destinadas a prevenir y retirar este tipo de contenido. (s. 66B, *Sexual Offences Act 2003*, introducido por s. 188, *Online Safety Act 2023*; ss. 10 y 27, *Online Safety Act 2023*).

a. Tipo de medida

El régimen contempla distintas medidas frente a la difusión no consentida de imágenes íntimas.

En primer lugar, respecto de los servicios usuario a usuario (*user-to-user services*), la sección 10(3A) del *Online Safety Act 2023*, incorporada por la sección 100 del *Crime and Policing Act 2026*, establece el deber de operar sistemas y procesos proporcionales destinados a retirar el contenido respecto del cual se haya presentado una denuncia de contenido de imagen íntima (*intimate image content report*), así como cualquier otro contenido que el proveedor identifique como igual o sustancialmente igual al contenido denunciado. La retirada debe realizarse tan pronto como sea razonablemente posible y, en todo caso, dentro de un plazo máximo de 48 horas, salvo las excepciones previstas por la norma. (s. 10(3A), OSA).

En segundo lugar, respecto de los servicios de búsqueda regulados (*regulated search services*), la sección 27(3A) establece una obligación equivalente destinada a garantizar que las personas dejen de poder encontrar el contenido íntimo denunciado como resultado de una búsqueda, así como cualquier contenido identificado como igual o sustancialmente igual. Se trata, por tanto, de una medida de exclusión o desindexación de resultados de búsqueda, además de la retirada en servicios usuario a usuario. (s. 27(3A), OSA).

Finalmente, el marco regulatorio incorpora medidas de prevención de la recirculación mediante la utilización de tecnología de *hash matching*. Ofcom ha establecido medidas específicas en sus *Illegal Content Codes of Practice* para que determinados servicios utilicen esta tecnología para detectar imágenes íntimas no consentidas y reducir su propagación. Estas medidas entran en vigor el 30 de septiembre de 2026 (Ofcom, 2026: 21 y siguientes).

b. Autoridad facultada

El modelo británico se diferencia de aquellos sistemas en que una autoridad administrativa o judicial ordena directamente a una plataforma retirar un contenido determinado. En el régimen del OSA, la obligación primaria recae directamente sobre los proveedores de servicios regulados, quienes deben implementar los sistemas y procesos exigidos por la ley.

Los proveedores deben recibir y tramitar los informes de contenido de imágenes íntimas (*intimate image content reports*) y aplicar las medidas de retirada o de exclusión correspondientes (secciones 20A y 31A, OSA).

La supervisión y fiscalización del cumplimiento corresponde a la Oficina de Comunicaciones del gobierno del Reino Unido (Ofcom), autoridad reguladora del régimen de seguridad en línea. Ofcom puede investigar el cumplimiento de las obligaciones y adoptar medidas de ejecución frente a proveedores que incumplan sus deberes. El OSA contempla además mecanismos específicos mediante los cuales Ofcom puede imponer determinados requisitos y sanciones (Partes 7 y 8, OSA).

c. Etapa o momento en que puede disponerse

La medida específica de retirada puede activarse cuando el proveedor recibe un informe de contenido de imágenes íntimas (*intimate image content report*) efectuado por la persona que aparece en el contenido o por alguien que actúa en su nombre. La sección 20A establece los requisitos de la denuncia: debe declarar que el contenido constituye imágenes íntimas (*intimate image content*), que quien lo presenta es la persona afectada o actúa en su nombre y que la denuncia se formula de buena fe y es verdadero según el conocimiento y convicción de quien lo presenta (sección 20A(2), OSA).

La misma lógica se aplica a los servicios de búsqueda mediante el mecanismo previsto en la sección 31A (sección 31A, OSA).

Por tanto, la intervención no depende necesariamente de que exista previamente una denuncia penal, una investigación judicial o una orden judicial. El mecanismo puede activarse directamente mediante el procedimiento de la denuncia previsto por la legislación de seguridad en línea.

d. Presupuesto o estándar requerido

El régimen exige que el contenido denunciado corresponda a la categoría legal de "contenido de imágenes íntimas" (*intimate image content*). La sección 59(10A) del OSA define esta categoría mediante remisión a las conductas constitutivas del delito previsto en la sección 66B(1), (2) o (3) de la Ley de Delitos Sexuales (*Sexual Offences Act*) de 2003.

La sección 66B, a su vez, contempla distintas hipótesis de responsabilidad por compartir intencionalmente una fotografía o película que muestre o parezca mostrar a otra persona en un estado íntimo, cuando esta no consiente y quien comparte no tiene una creencia razonable en su consentimiento. También contempla determinados supuestos en que la conducta se realiza con la intención de causar alarma, angustia o humillación, así como cuando existe una finalidad de obtener gratificación sexual (sección 66B(1)–(3), *Sexual Offences Act 2003*).

Para activar el procedimiento específico de la denuncia, este debe ser efectuada por la persona que aparece en el contenido o por alguien que actúa en su nombre, y debe cumplir los requisitos formales establecidos en los seccións 20A y 31A. (ss. 20A(2) y 31A(2), OSA).

e. Destinatario de la orden o medida

La obligación se dirige principalmente a los proveedores de servicios regulados.

En los servicios usuario a usuario, el destinatario es el proveedor del servicio, que debe retirar el contenido denunciado y cualquier otro contenido que identifique como igual o sustancialmente igual (s. 10(3A), OSA).

En los servicios de búsqueda, el destinatario es el proveedor del servicio de búsqueda, que debe adoptar medidas para impedir que las personas continúen encontrando el contenido denunciado como resultado de búsqueda, incluyendo contenidos iguales o sustancialmente iguales (s. 27(3A), OSA).

El régimen también permite la intervención de Ofcom respecto de los proveedores cuando existe incumplimiento de las obligaciones legales, mediante sus facultades de supervisión y ejecución.

f. Plazo de cumplimiento

La sección 10(3A) del OSA establece expresamente que la retirada del contenido debe realizarse tan pronto como sea razonablemente posible y, en ningún caso, después de 48 horas desde la recepción del *intimate image content report*, salvo que el proveedor considere que el contenido no constituye *intimate image content* o que quien presenta la denuncia no es la persona afectada ni actúa en su nombre.

El mismo plazo máximo de 48 horas se aplica a los servicios de búsqueda conforme al sección 27(3A), respecto de la imposibilidad de encontrar el contenido como resultado de búsqueda (ss. 10(3A) y 27(3A), OSA).

Por tanto, a diferencia de otros ordenamientos analizados, el régimen británico establece actualmente un plazo legal expreso de 48 horas para estas medidas específicas.

g. Mecanismos de revisión o impugnación

El OSA contempla mecanismos de reclamación y revisión frente a las actuaciones de los proveedores. En particular, la sección 21 establece obligaciones relativas a los procedimientos de reclamación de los servicios usuario a usuario, y las modificaciones efectuadas en 2026 incorporaron un procedimiento acelerado de reclamaciones para aquellas relacionadas con un *intimate image content report* (s. 21(2A), OSA).

A nivel regulatorio, las decisiones adoptadas por Ofcom en ejercicio de sus facultades de supervisión y ejecución pueden ser objeto de apelación ante el Upper Tribunal en los supuestos contemplados en la sección 168 del OSA. La apelación puede ser presentada por cualquier persona que tenga un interés suficiente en la decisión, con las reglas específicas establecidas por la norma (s. 168, OSA).

La sección 168 contempla, entre otras, las apelaciones contra determinadas decisiones de Ofcom, incluidas las *confirmation decisions* y *penalty notices*. El Tribunal aplica los mismos principios que aplicaría el High Court en una revisión judicial y puede desestimar la apelación o dejar sin efecto la decisión y devolverla a Ofcom para su reconsideración (s. 168(3)–(5), OSA).

h. Preservación de la evidencia digital

El *Online Safety Act 2023* establece obligaciones generales de registro y conservación de información relacionada con el cumplimiento de las obligaciones de seguridad en línea, pero no establece, para los *intimate image content reports*, una obligación específica equivalente a la prevista en México, consistente en conservar el contenido denunciado como evidencia para una eventual investigación penal.

En particular, la sección 23 del OSA exige a los proveedores de servicios usuario a usuario mantener registros escritos de las evaluaciones de riesgo y de las medidas adoptadas para cumplir las obligaciones pertinentes. La sección 34 establece obligaciones equivalentes de registro para los servicios de búsqueda (ss. 23 y 34, OSA).

III. Consideraciones finales

Los casos analizados- Ley Modelo Interamericana del MESECVI, como estándar regional de referencia, y la legislación de Australia, México y Reino Unido - coinciden en que la respuesta frente a los

contenidos digitales nocivos no puede limitarse a sancionar al autor, sino que debe incluir medidas que actúen directamente sobre la circulación del material.

Todos los modelos contemplan el retiro o la eliminación del contenido. Se diferencian, sin embargo, en quién adopta la decisión. México sigue un modelo de protección de carácter procesal, en el que el Ministerio Público o el juez ordenan la medida en el marco de una investigación. Australia opta por un modelo administrativo, en el que el *eSafety Commissioner* emite órdenes vinculantes sin autorización judicial previa. El Reino Unido impone la obligación directamente a las plataformas y reserva a Ofcom un papel de supervisión y sanción. La Ley Modelo adopta una fórmula mixta: admite la intervención administrativa y judicial, pero exige control judicial para las medidas que restrinjan derechos fundamentales.

El ámbito de aplicación y el modo de activar las medidas también difieren. México y la Ley Modelo se centran en la violencia digital contra las mujeres basada en género, mientras que el Reino Unido regula específicamente las imágenes íntimas difundidas sin consentimiento. Australia, por su parte, distingue procedimientos según el tipo de contenido y la edad de la víctima, con estándares graduados. En el ciberacoso dirigido a NNA el estándar exige que el contenido tenga un efecto grave de amenaza, intimidación, acoso o humillación. En el ciberabuso dirigido a personas adultas, se exige además una probable intención de causar un daño grave. En el caso de las imágenes íntimas, el elemento central es la falta de consentimiento.

En cuanto a la activación, México vincula la medida a una investigación en curso, mientras que la Ley Modelo permite adoptar medidas precautelares antes de iniciado el proceso. En Australia el procedimiento se inicia mediante una queja ante el Comisionado, Como regla general, previamente debe haberse reclamado ante la plataforma y haber transcurrido 48 horas sin que el contenido haya sido retirado; este requisito no se exige en los casos de difusión no consentida de imágenes íntimas. En el Reino Unido, en cambio, el mecanismo se activa directamente mediante una denuncia ante el proveedor, sin necesidad de una denuncia penal previa.

Existen diferencias relevantes en la variedad de medidas y en los plazos. La Ley Modelo es la que ofrece el catálogo más amplio: suspensión y restricción de contenidos, desactivación de la monetización y cierre de cuentas. México contempla la interrupción, el bloqueo, la destrucción y la eliminación. Australia añade órdenes dirigidas al propio autor, que puede ser obligado a retirar el material, abstenerse de publicar nuevo contenido o pedir disculpas en el caso de menores. Solo el Reino Unido incorpora la exclusión de resultados de búsqueda y la detección de contenidos “iguales o sustancialmente iguales” mediante *hash matching*[1], las dos herramientas que la literatura identifica como más eficaces para prevenir la recirculación. En materia de plazos, Australia exige cumplir en 24 horas y el Reino Unido en un máximo de 48, mientras que México y la Ley Modelo exigen una actuación inmediata sin fijar un plazo concreto de cumplimiento para el destinatario.

Por último, los regímenes presentan diferencias tanto en los mecanismos de revisión de las medidas como en la preservación de la evidencia digital. Australia contempla la notificación de la negativa a emitir una orden, mecanismos de revisión interna y la posibilidad de recurrir ante el Tribunal de Revisión Administrativa. El Reino Unido prevé un procedimiento acelerado de reclamación ante la plataforma y la apelación ante el Upper Tribunal respecto de determinadas decisiones de Ofcom. La Ley Modelo

[1] Medidas que entrarán en vigor el 30 de septiembre de 2026.

establece control judicial inmediato de las medidas, mientras que México no contempla un mecanismo específico de revisión para las órdenes analizadas. En materia de preservación de la evidencia, México y la Ley Modelo establecen expresamente la conservación del contenido para fines probatorios. En particular, la Ley Modelo aborda de forma explícita la relación entre retiro y preservación de la evidencia, al permitir una remoción temporal y controlada que impide el acceso público al contenido y, al mismo tiempo asegura su conservación como prueba. En Australia y el Reino Unido, los regímenes examinados no establecen una obligación específica equivalente.

Referencias

Harlan, G., Jo, A., & Crockett, C. (2026). Mapping the burden: Toward survivor-centered reporting systems and policies for non-consensual intimate images. Berkman Klein Center for Internet & Society,

Harvard University. Disponible en: https://asml.cyber.harvard.edu/wp-content/uploads/sites/18/2026/06/NCII-Whitepaper-Final.pdf

Howard, J. W., & Kira, B. (2026). Remove or reduce: Demotion, content moderation, and human rights. Law and Philosophy, 45, 483–513. Disponible en: https://doi.org/10.1007/s10982-026-09557-8

Huber, A. R., & Ward, Z. (2025). Non-consensual intimate image distribution: Nature, removal, and implications for the Online Safety Act. European Journal of Criminology, 22(1), 30–50. Disponible en: https://doi.org/10.1177/14773708241255821

Ofcom (2026). Illegal content Codes of Practice for search services. Disponible en: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/detecting-intimate-image-abuse/illegal-content-codes-of-practice-for-search-services-9sep2026.pdf?v=425250 (septiembre, 2026).

UNESCO. (2023). Directrices para la gobernanza de las plataformas digitales: Salvaguardar la libertad de expresión y el acceso a la información con un enfoque de múltiples partes interesadas. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000387360

Women and Equalities Committee. (2025). Tackling non-consensual intimate image abuse (Fourth Report of Session 2024–25, HC 336). House of Commons. Disponible en: https://committees.parliament.uk/publications/46899/documents/241995/default/

Referencias normativas

Ley Modelo Interamericana

- Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI) (2025). Ley Modelo Interamericana para Prevenir, Sancionar y Erradicar la Violencia Digital contra las Mujeres basada en Género. Disponible en: https://www.oas.org/es/mesecvi/docs/LeyModeloFemicidio-ES.pdf (septiembre, 2026).

Australia

- Online Safety Act (2021). Disponible en: https://www.legislation.gov.au/C2021A00076/latest/text (diciembre, 2025).
- Criminal Code Act (1995). Disponible en: https://www.legislation.gov.au/C2004A04868/2022-11-10/text/2 (diciembre, 2025).

México

- Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (2007). Disponible en: https://legislacion.scjn.gob.mx/Buscador/Paginas/wfOrdenamientoDetalle.aspx?q=WVhKjmhCYz0ufl+8glULlOKRtBAaWggk3wJWIia8xCd3zP+J+u+m8GxYOketZi6x (septiembre, 2026).
- Código Nacional de Procedimientos Penales (2014). Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf (septiembre, 2026).
- Código Penal Federal (1931). Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf (septiembre, 2026).
-

Reino Unido

- Online Safety Act (2023). Disponible en: https://www.legislation.gov.uk/ukpga/2023/50 (septiembre, 2026).
- Sexual Offences Act (2003). Disponible en: https://www.legislation.gov.uk/ukpga/2003/42 (septiembre, 2026).
- Crime and Policing Act (2026). Disponible en: https://www.legislation.gov.uk/ukpga/2026/20/contents (septiembre, 2026).

Nota aclaratoria

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.

Creative Commons Atribución 3.0
(CC BY 3.0 CL)