



Informe especial

¿QUIÉN ES RESPONSABLE DEL CONTENIDO QUE SE CONSUME EN INTERNET?

Informe especial

¿Quién es responsable del contenido que se consume en internet?



POR:
RAFAELA OJEDA
**COORDINADORA DEL
ÁREA LEGAL - AFIN**

Los riesgos del internet

En el entorno digital, los usuarios enfrentan una exposición constante a contenidos nocivos. La proliferación masiva de desinformación, noticias falsas y contenido sintético hiperrealista (deepfakes) diseñado para manipular la opinión pública coexiste con la facilidad con que los menores acceden a pornografía, discursos de odio, violencia explícita o plataformas que promueven la ludopatía, con consecuencias directas sobre su bienestar emocional, seguridad personal e integridad moral. Estos no son riesgos abstractos ni futuros: son realidades que afectan hoy a millones de niños y adolescentes peruanos, y que merecen una respuesta regulatoria seria, estructurada y coherente.





Cómo hemos regulado el Internet en el Perú

El Perú ha adoptado un marco normativo que aborda estos riesgos sin sacrificar la libertad de expresión ni el desarrollo tecnológico. La Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes (Ley N° 30254) y su reglamento (Decreto Supremo N° 093-2019-PCM), establecen el régimen superficial de protección frente

a contenidos potencialmente dañinos accesibles a través de internet, con énfasis en la protección de menores. Bajo este régimen, las empresas operadoras de telecomunicaciones tienen una obligación de informar a los usuarios sobre la posibilidad de contratar o autorizar filtros que restrinjan el acceso a determinados contenidos en sus dispositivos.

Derecho y políticas comparadas

1. Unión Europea

Reglamento de Servicios Digitales (RSD)

2. Organización para la Cooperación y el Desarrollo Económicos (OCDE)

Recomendaciones sobre niños en el entorno digital (2025)

3. Unión Internacional de Telecomunicaciones (UIT)

Directrices para la industria sobre protección infantil en línea



1. Unión Europea:

El Reglamento de Servicios Digitales de la Unión Europea (en adelante “RSD”), parte de una distinción técnica y jurídica fundamental, ya que clasifica los servicios intermediarios en tres categorías según su función técnica: mera transmisión, memoria caché y alojamiento de datos. Las empresas operadoras que proveen acceso a internet se ubican en la categoría de mera transmisión.

Bajo este régimen, el prestador del servicio no incurre en responsabilidad por la información transmitida siempre que no haya iniciado la transmisión, no haya seleccionado al destinatario y no haya seleccionado ni modificado el contenido. El RSD exige, adicionalmente, que el prestador no desempeñe un papel activo que le confiera conocimiento o control sobre la información. El operador que provee acceso a la red actúa, por tanto, como un conducto neutral, y esa neutralidad es precisamente la condición de su exención de responsabilidad.

Los prestadores de servicios intermediarios están sujetos a la obligación de atender requerimientos de autoridades competentes, como órdenes de restricción de acceso o de suministro de información sobre usuarios determinados. Lo que el RSD prohíbe expresamente es la imposición de una obligación general de monitorización del contenido, prohibición que constituye uno de los pilares del sistema europeo ya que el operador no puede ser convertido en guardián universal del contenido que sus usuarios generan o consumen en Internet, porque ello desnaturaliza su función técnica, vulnera la neutralidad de la red y genera desincentivos estructurales a la inversión en conectividad.

Así, el RSD asigna la obligación regulatoria a quien tiene poder efectivo sobre el riesgo. En el caso del contenido nocivo que circula en Internet, ese poder reside en las plataformas que lo crean, organizan, distribuyen y monetizan con su consumo, no en la empresa operadora, cuya función es proveer la infraestructura que permite el acceso a la red.



2. Organización para la Cooperación y el Desarrollo Económicos (OCDE):

Por su parte, la OCDE ha elaborado un conjunto de recomendaciones frente a los riesgos que el consumo de internet genera en los usuarios más jóvenes y vulnerables. En ellas, la OCDE (2025) estructura en cuatro pilares una política integral sobre esta problemática: establecer marcos regulatorios que promuevan tecnologías y servicios con seguridad prioritaria para los menores; fortalecer la alfabetización digital, las competencias de los niños y el rol de las escuelas y los docentes; proporcionar orientación a padres y cuidadores; e incorporar las perspectivas de los propios menores en el diseño de políticas.

El primer pilar tiene implicancias directas sobre quién debe soportar las obligaciones regulatorias en el ecosistema digital. La OCDE (2025) señala que los prestadores de servicios digitales tienen un rol crítico en la seguridad en línea, con obligaciones de respetar la privacidad, combatir la difusión de contenido inapropiado y ofrecer mecanismos de denuncia accesibles para los menores. Los gobiernos, por su parte, son responsables de establecer regulaciones y estándares orientados a la “seguridad por diseño”, esto es, la integración de medidas de seguridad desde el diseño mismo de los productos y servicios digitales. Ese principio implica que la obligación de protección recae en quien diseña y opera el entorno digital al que accede el menor, no en el operador que provee la infraestructura de acceso (OCDE, 2025).

En materia de alfabetización digital, la Recomendación sobre Niños en el Entorno Digital de la OCDE (2025) la reconoce como una herramienta fundamental para fortalecer la resiliencia de los menores frente a los riesgos en línea. La lógica subyacente es que un usuario con capacidades digitales puede identificar, resistir y reportar los riesgos a los que se expone, lo que reduce la dependencia de mecanismos externos restrictivos o prohibitivos. La OCDE (2025) recomienda fortalecer la regulación, mejorar las competencias digitales de los menores, orientar a padres y cuidadores, ampliar la base de evidencia sobre las actividades digitales de los menores y sus impactos, e incorporar las perspectivas de los niños en el diseño de políticas.



3. Unión Internacional de Telecomunicaciones (UIT)

Por su parte, la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación (TIC), ha elaborado directrices para la industria sobre protección infantil.

La primera contribución de esas directrices al debate es su sistema de clasificación de los actores del ecosistema digital según su rol técnico: proveedores de conectividad, almacenamiento de datos y servicios de hosting (Feature A), proveedores de contenido editorial curado (Feature B), plataformas que alojan contenido generado por usuarios (Feature C), y sistemas impulsados por inteligencia artificial (Feature D). Cada categoría recibe un conjunto diferenciado de obligaciones. Esa diferenciación expresa el principio rector del documento: la responsabilidad debe distribuirse en función del control efectivo que cada actor ejerce sobre el contenido al que los menores acceden.

En ese esquema, el proveedor de conectividad -la empresa operadora- queda sujeto a un conjunto acotado y específico de obligaciones, como establecer relaciones de colaboración con las autoridades de aplicación de la ley y con los organismos de denuncia para gestionar los reportes de material de abuso sexual infantil de los que tome conocimiento. Las directrices de la UIT no contemplan obligaciones generales de monitoreo para las empresas operadoras, ni les atribuye obligaciones de detección proactiva de contenido ilícito, ni les asigna responsabilidad editorial sobre los contenidos que son transmitidos. Esas obligaciones corresponden a las plataformas del Feature C, que son quienes crean los entornos donde el contenido se genera, organiza, distribuye y monetiza.

En consecuencia, el marco de la UIT, al igual que el RSD y las recomendaciones de la OCDE, ubica la obligación de protección donde reside el poder real sobre el riesgo, no en el operador que no genera, ni selecciona, ni organiza ni se beneficia económicamente del contenido consumido en internet.



Entonces, ¿quién es responsable del **contenido digital que se consume?**

Las empresas operadoras de telecomunicaciones no producen ni controlan el contenido que los usuarios consumen a través de internet, ni determinan cómo estos interactúan con las plataformas digitales a las que acceden. Su función consiste en proveer acceso a la red: son el canal, no la fuente del contenido.

Esta distinción tiene respaldo normativo expreso. La Ley N° 30254 circunscribe la obligación de las operadoras al plano informativo: deben informar a los usuarios sobre la disponibilidad de filtros y garantizar que el contrato contemple

la opción de activarlos, pero la decisión de hacerlo corresponde al usuario o, en el caso de menores, a sus padres o tutores. Confundir el medio (infraestructura) con el contenido que se transmite generaría graves desincentivos para la inversión en infraestructura de conectividad, precisamente cuando el país necesita ampliar su cobertura digital.

No obstante, a pesar de que la Ley N° 30254 ubica correctamente la responsabilidad de las empresas operadoras, no se pronuncia sobre el problema de fondo y solo opera en los bordes del ecosistema digital.

La principal debilidad es la de la política educativa

La protección real de los menores frente a los riesgos del entorno digital no se logra con filtros, sino, capacitando a los ciudadanos digitales desde la infancia. Esa es una responsabilidad indelegable del Estado, y se ejerce a través de la currícula escolar. La Ley N° 30254 no incorpora esto ni establece competencias digitales obligatorias dentro de la educación básica.

La segunda debilidad es que la Ley N° 30254:

No establece un régimen específico para plataformas digitales, redes sociales o motores de búsqueda, quienes determinan qué contenido llega a los usuarios, con qué frecuencia, en qué contexto y bajo qué lógica algorítmica. Son los titulares naturales de las obligaciones de protección por diseño. La Ley N° 30254 no los incluye en su ámbito de aplicación ni les impone ninguna obligación. El segmento del ecosistema digital que mayor poder ejerce sobre el riesgo queda fuera del alcance de ley que pretende abordarlo.

La tercera debilidad, quizás la más reveladora de todas, es institucional

La ley distribuye funciones entre el Ministerio de Transportes y Comunicaciones, el Ministerio de Educación, el Ministerio de la Mujer y Poblaciones Vulnerables, el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) y una Comisión Especial creada para este fin, sin que ninguno de esos actores tenga atribuida una responsabilidad de resultado clara, medible y exigible. En consecuencia, la responsabilidad se diluye la responsabilidad entre múltiples entidades.





Las políticas que **necesita el Perú**

La preocupación que motiva este artículo no es solo técnica. Los riesgos digitales que enfrentan los niños y adolescentes peruanos son reales y crecientes, y merecen una respuesta estatal que esté a la altura de su magnitud. Lo que el Perú necesita no es una regulación que descargue en el sector privado las obligaciones que el Estado no ha deseado asumir, sino una política pública coherente que asigne responsabilidades donde corresponde y establezca mecanismos claros de evaluación de resultados.

El debate regulatorio no debe plantearse como una elección entre prohibir y desregular, pues ambos extremos son igualmente ineficaces. La prohibición indiscriminada no elimina los riesgos; los desplaza hacia canales menos controlados, restringe el desarrollo tecnológico y penaliza a quienes actúan dentro del marco legal. La ausencia de regulación, por su parte, deja sin protección a quienes más la necesitan.

El enfoque más adecuado es el que ya subyace en la Ley N° 30254: asignar las obligaciones a quien tiene capacidad real de cumplirlas y atribuir la responsabilidad a quien tiene poder efectivo sobre el riesgo. En internet, eso significa empoderar al usuario para que tome decisiones informadas sobre el contenido que consume y a los padres y tutores para que ejerzan ese rol respecto de los menores a su cargo. No obstante, las políticas que el país necesita son las que fortalecen la educación digital, dotan al usuario de herramientas de control efectivo y establecen obligaciones claras y proporcionales sobre quienes tienen poder real sobre el contenido y los sistemas. No las que trasladan al operador de red una responsabilidad que no le corresponde, ni las que convierten en prohibición lo que debería ser regulación inteligente.



Bibliografía

- Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2025) How's Life for Children in the Digital Age? Publications. https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en.html
- Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2025) Recommendation of the Council on Children in the Digital Environment, OECD/LEGAL/0389
- Unión Internacional de Telecomunicaciones (UIT) (2020). Guidelines for Industry on Child Online Protection. Ginebra. ISBN 978-92-61-30411-9. <https://www.unicef.org/media/90796/file/ITU-COP-guidelines%20for%20industry-2020.pdf>