Lima, 20 de mayo de 2025

Estimada
Jessica Córdova Lobatón
Presidenta de la Comisión de Mujer y Familia
Congreso de la República
Presente.—

Asunto: **Comentarios al Proyecto de Ley N° 10880/2024-CR, Ley de protección de niños y adolescentes en entornos digitales**

Hiperderecho es una asociación civil peruana sin fines de lucro, con más de 12 años de experiencia, dedicada a investigar y promover el respeto de los derechos humanos en entornos digitales, conformada por un equipo interdisciplinario de abogadas, comunicadoras y especialistas en tecnología. Como parte de nuestro trabajo, estudiamos todas las iniciativas de política pública que puedan impactar el ejercicio de derechos y libertades en entornos digitales.

Hemos revisado con detenimiento el Proyecto de Ley N° 10880/2024-CR que propone una Ley de protección de niñas, niños y adolescentes en entornos digitales (en adelante "NNA"). A fin de salvaguardar sus derechos a la salud mental, a la protección de sus datos personales, así como su seguridad en línea. A partir de ello, a continuación presentamos algunos comentarios relativos a las principales medidas que incluye la propuesta legislativa, como son (i) el control parental para el acceso de NNA a redes sociales (ii) la identificación biométrica de NNA, (iii) la detección y bloqueo de VPN como medio para asegurar el control parental y (iv) la creación de un registro de celulares de NNA.

Sin perjuicio de ello, recomendamos de forma general realizar un test de proporcionalidad en cada medida propuesta, así como establecer de forma clara y concisa cuáles son las obligaciones que tienen las plataformas, y cuáles son las que tienen los proveedores de acceso a Internet.

1. El control parental para el acceso de NNA a redes sociales

La propuesta de Ley establece límites de edad para el uso de dispositivos móviles y redes sociales, estos límites serían diferenciados entre tres grupos: menores de 12 años, de 12-16 años, y de 16-18 años. Si bien es ideal a través de la diferenciación de estos grupos reconocer el principio de desarrollo progresivo de los NNA en relación con el uso que le puedan dar al

internet, es importante tomar en cuenta también en este tipo de decisiones el principio de gobernanza de internet y múltiples partes interesadas.

Así, la propuesta legislativa pretende proponer soluciones técnicas operativas que deberían implementar los proveedores de dispositivos móviles y servicios de acceso a internet, así como las empresas de redes sociales. Estas son: (i) herramientas de control parental, (ii) pausas o bloqueos controlados por horas con funciones restringidas, como un "Modo de Aprendizaje", y (iii) desactivar funciones como reproducción automática, desplazamiento infinito y rachas.

Al respecto, cabe destacar que los dos primeros tipos de controles propuestos ya existen. Desde herramientas de control parental en Windows, sistema operativo más popular en el mercado, hasta aplicaciones para celulares como Google Family Link o funciones preestablecidas en el caso del sistema operativo móvil iOS.

Por un lado, para laptops y computadoras de escritorio, Windows cuenta con la función "Microsoft Family Safety", que se puede activar desde la configuración, en el apartado de "Cuentas". Esta función permite crear un usuario con restricciones de control parental relativas al tiempo en pantalla (control por horas), a los sitios web y contenido al que se pueden acceder en línea, a los juegos que se pueden comprar, y más. Inclusive es posible que la madre, padre o tutor que administra la cuenta reciba un informe de actividades y sitios web visitados semanalmente a su correo[1]. Las mismas funciones de control parental se permiten en el sistema operativo MacOS, en la opción "Ajustes del Sistema"[2].

Por otro lado, para celulares y tablets, en Android existe Google Family Link, la aplicación oficial de control parental para Android. Esta aplicación permite filtrar contenido, restringir el acceso, fijar límites de tiempo en pantalla, aprobar o bloquear la descarga de aplicaciones, proteger la privacidad y datos de NNA, entre otras herramientas. Inclusive, para la administración de aplicaciones, recomienda permisos basados en la edad del NNA, de acuerdo con el Pan European Game Information (PEGI), un sistema de autorregulación de la industria de los videojuegos, que clasifica y personaliza el modo de usuario, de acuerdo a su edad[3]. De igual forma, estas opciones se pueden ejecutar en la configuración de iOS, el sistema operativo móvil de Apple, para tablets y celulares[4].

Por tanto, sería ideal que la propuesta legislativa pueda identificar las herramientas ya existentes en el mercado. A fin de que la medida, que busca proteger los datos personales, privacidad y seguridad en línea de NNA, se oriente hacia un problema específico y actual, evitando así soluciones planteadas desde la falta de un estudio de las herramientas actuales. Más aún, en un espectro donde la autorregulación ya ha desarrollado estándares propios.

---

[1] Para más información, visitar: Microsoft Family Safety
[2] Para más información, visitar: https://support.apple.com/es-co/guide/mac-help/mchl8490d51e/mac
[3] Para más información, visitar: Family Link de Google - Seguridad para familias y herramientas de control parental
[4] Para más información, visitar: Utilizar el control parental del iPhone y el iPad - Soporte técnico de Apple (ES)

Finalmente, con respecto a la tercera solución técnica (desactivar funciones como reproducción automática, desplazamiento infinito y rachas) esta parece una medida dirigida hacia el contenido multimedia de plataformas de redes sociales y entretenimiento, y en el caso de las rachas, una medida específica dirigida hacia TikTok, Snapchat o BeReal, principales plataformas que incorporan esa característica. Sin embargo, esta oportunidad para discutir las características integradas de las plataformas de redes sociales y entretenimiento, y su impacto en la salud mental y la protección de datos personales, debe ser guiada por el principio de múltiples partes interesadas y gobernanza de internet, reconocidos en la Carta Peruana de Derechos Digitales (2022), el Decreto Supremo que aprueba el Sistema Nacional de Transformación Digital (2020) y su Reglamento (2021), en la Ley que promueve el uso de la IA en favor del desarrollo económico y social (2023), y la Alianza Nacional por una Internet Segura (2024).

Cabe señalar que existen algunas funciones como el *scroll* o desplazamiento infinito que no se pueden desactivar en algunas redes sociales, como Instagram, Facebook, Tiktok y Youtube (en el caso de Youtube Shorts); de igual forma la reproducción automática se puede desactivar en Facebook, pero no en Instagram ni Tiktok. De otro lado, el sistema de rachas sólo se encuentra en algunas plataformas como TikTok, Snapchat o BeReal, pero no en Facebook o Instagram, inclusive se encuentra en aplicaciones de aprendizaje como Duolingo.

Por tanto, al ser cada plataforma distinta, la formulación de políticas públicas o recomendaciones a las plataformas en materia de derechos humanos del niño, niña y adolescente, debe partir de un diálogo abierto, con invitación a representantes de cada plataforma. Un diálogo que cuente con participación de sociedad civil, academia, comunidad técnica, Estado y, por supuesto, plataformas.

Resulta importante además analizar el impacto que tendría poner en práctica esta propuesta legislativa en el derecho a la libertad de empresa, específicamente en su contenido de libertad de organización. Es decir, si se pretende eliminar por ley características del modelo de negocios de un sector de empresas, como son las características integradas de la interfaz para el usuario (desplazamiento infinito, reproducción automática y sistema de rachas), a fin de salvaguardar el derecho a la salud mental o la seguridad en línea de los NNA, primero se debe verificar que esta medida sea proporcional; es decir, debe superar el test tripartito de proporcionalidad.

2. La identificación biométrica de NNA

La propuesta de Ley señala en el artículo 3.5 (definiciones), como uno de los mecanismos tecnológicos que pueden implementar los proveedores para confirmar la edad: la verificación biométrica. Este sería un mecanismo de verificación de su edad, para de acuerdo a ello, según se indica en el Proyecto de Ley, controlar su acceso a redes sociales, plataformas de entretenimiento, aplicaciones o páginas web, y controlar su tiempo en línea.

Es positivo que se implementen mejores prácticas de verificación de identidad, en tanto resulta insuficiente la autodeclaración de la identidad. Sin embargo, existen otros mecanismos de

verificación de identidad menos invasivos de los datos sensibles de NNA, como son la verificación documental o a través de certificados digitales, que también son señalados en la norma.

Por ende, el mecanismo de verificación biométrica para NNA es desproporcionado al existir mecanismos menos lesivos de su derecho a la intimidad y a los datos personales, e igualmente satisfactorios para la finalidad de verificar su identidad y así garantizar su seguridad en línea.

De hecho, si bien la propuesta legislativa no lo menciona, resulta preocupante también determinar cuál sería la base de datos sobre la cual se verificaría la biometría. Por ejemplo, si se tratase de una base de datos biométricos de NNA, administrada por RENIEC, entonces ¿las plataformas tendrían acceso a RENIEC para verificar la identidad biométrica y con ello la edad? Esto debe ser cuidadosamente analizado pues el sistema centralizado de identidad digital de RENIEC actualmente no ofrece las garantías necesarias para garantizar la integridad de estos datos sensibles.

Eliminar el mecanismo de verificación biométrica para NNA es coherente además con el contenido de la Ley de Protección de Datos Personales y su Reglamento. Marco normativo a través del cual se promueve el uso mínimo de datos personales de NNA, y la protección especial y el tratamiento excepcional de los datos sensibles, así como las garantías de seguridad digital en el almacenamiento y tratamiento de estos datos.

Otro punto no menos importante a tener en cuenta cuando nos referimos a la identificación biométrica es también las barreras económicas de acceso a dispositivos móviles de gama alta. La verificación biométrica, sea el reconocimiento facial o por huella dactilar, demanda dispositivos móviles o tablets con determinadas características, que corresponden a una gama alta. Esto, en la práctica, podría generar un trato discriminatorio por razón económica para aquellos que no pueden acceder a este tipo de dispositivos. En ese sentido, recomendamos eliminar en el artículo 3.5. la “verificación biométrica” como uno de los mecanismos para confirmar la edad de las personas usuarias.

3. La detección y bloqueo de VPN como medio para asegurar el control parental

El Proyecto de Ley plantea también como una obligación de los proveedores de dispositivos móviles y servicios de internet: detectar y bloquear el uso de VPN, que, según el ámbito de aplicación del proyecto, sería aparentemente en instituciones educativas públicas y privadas[5]. Con el objetivo de fiscalizar las restricciones de edad y así garantizar las limitaciones de control parental y la seguridad en línea de los NNA. Al respecto, se debe notar que esta medida no es idónea por dos motivos.

[5] Aunque esto no queda claro en el artículo 4, sobre el ámbito de aplicación, pues menciona también a proveedores y dispositivos disponibles dentro del territorio peruano.

De un lado, la restricción de edad es una función del control parental que manejan las madres, padres o tutores de los NNA a través de sus dispositivos móviles, tablets, laptops o computadoras de escritorio. Por ello, sería una tarea que se encuentra en el ámbito de control de los apoderados de los NNA, y no de los proveedores de dispositivos móviles o proveedores del servicio de internet.

Por otro lado, el uso del VPN no asegura evadir los controles parentales. El sistema de control parental, como cualquier otro, no es infalible, y se puede usar el VPN para evitarlo, siempre y cuando el control parental usado está basado en la red (IP, DNS local, ubicación). Sin embargo otro tipo de controles parentales basados en *software* o cuentas, como los mencionados en el punto 2 de este informe, son más difíciles de evitar.

Finalmente, cabe acotar también que, independientemente de la idoneidad de los VPN para evadir los controles parentales, una obligación dirigida a los proveedores para detectar y bloquear el uso de la VPN en colegios tiene implicaciones en otros principios y derechos fundamentales, como el principio de neutralidad de la red (en su contenido de uso y acceso de dispositivos), la libertad de expresión, el acceso a la información, y el recientemente reconocido derecho de acceso a Internet, en su contenido de libertad y apertura en el acceso (derecho a conectarte a cualquier red, ya sea pública o privada por VPN).

Además, el bloqueo del VPN puede afectar la conectividad de otros dispositivos legítimamente empleados por el profesorado en clases, con fines educativos, o de los propios estudiantes en las salas de cómputo y bibliotecas del colegio. Cabe recalcar asimismo que el VPN puede ser usado también por el estudiantado para fines legítimos como acceder a contenidos educativos no disponibles en Perú. Por tanto, no es recomendable implementar una obligación de este tipo, pues no necesariamente el uso de VPN puede servir para evitar los controles parentales, y además el bloqueo del VPN afecta otros derechos fundamentales y principios que forman parte del ordenamiento jurídico, así como la conectividad en las escuelas.

4. La creación de un registro de celulares de NNA

En el Proyecto de Ley se señala que son deberes de los padres o tutores “declarar y registrar los dispositivos móviles en posesión de menores, así como sustentar la verificación de edad de los mismos”[6]. De igual forma, como seguimiento a este sistema de registro de celulares de NNA se propone como obligación para los proveedores de dispositivos móviles y servicios de internet:

> Gestionar de manera automatizada los límites de acceso a redes sociales para menores, en base a un registro, anonimizado y actualizado en tiempo real, de los códigos IMEI de dispositivos móviles en posesión de menores. Dicho registro se elaborará en base a la verificación de edad declarada y sustentada por los adquirentes de dichos equipos y/o contratantes de servicios de acceso a internet, incluyendo clientes corporativos[7].

[6] Artículo 10, inciso a.
[7] Artículo 9.1., inciso c.

Crear un registro de celulares IMEI de menores es una medida que no asegura que se cumpla con la finalidad de garantizar el control parental, y con ello la seguridad en línea de NNA. Por el contrario, crear ese registro implica un monitoreo constante de los flujos de datos que tiene un dispositivo respecto a un aplicativo o sitio web, lo que vulnera la privacidad de las infancias y adolescencias y expone sus datos personales, que hasta podrían ser objeto de filtraciones por vulneraciones de ciberseguridad. Es decir, tendría inclusive un efecto adverso a los derechos que se pretenden proteger en el Proyecto de Ley.

El crear un registro, por ley, implica crear una base de datos cuya recopilación es una limitación al principio de consentimiento, de acuerdo con el artículo 14, inciso 13 de la Ley de Protección de Datos Personales. En este sentido, toda creación de base de datos por mandato legal debe superar el test de proporcionalidad al limitar el consentimiento y, además, debe cumplir los principios de finalidad y proporcionalidad, igualmente reconocidos en la Ley.

Por otro lado, un registro como este afecta también los derechos a la libertad de comercio y a la propiedad, al enlazar la identidad de una persona con la del celular. Como consecuencia, se limitaría la compra-venta y hasta donación o simple traspaso entre familiares o amigos de dispositivos electrónicos que usan IMEI (tablets, celulares, smartwatches).

Asimismo, en el Proyecto de Ley no se señala cuál sería la sanción por no registrar los celulares de los NNA, ¿sería acaso el bloqueo del IMEI? En tal supuesto se afectaría con mayor intensidad los derechos al libre comercio y a la propiedad. En cualquier caso, el bloqueo no sería suficiente para garantizar el control parental, pues los NNA pueden utilizar sus celulares para conectarse a WiFi y así continuar accediendo a Internet y a las plataformas que se pretenden restringir, pues el bloqueo del IMEI no limita el acceso a Internet por WiFi.

Así, la medida no parece superar un test de proporcional, por cuanto inclusive si fuera idónea para alcanzar la finalidad de proteger la seguridad en línea de los NNA (control parental), y con ello su derecho a la integridad personal, no supera el subtest de necesidad, pues existen medidas menos lesivas para los derechos a la protección de datos personales, privacidad, libre comercio y propiedad, e igualmente satisfactorias para la integridad y seguridad en línea de los NNA. Por ejemplo, aquellas que viene ejecutando la Secretaría de Gobierno y Transformación Digital (SGTD), como campañas para fortalecer las competencias digitales, la seguridad en línea y el talento digital de NNA, como el “Programa Niñas Digitales”[8] o la “Alianza Nacional por una Internet Segura”[9], en concordancia con la Política Nacional de Transformación Digital al 2030, publicada en 2023.

Extendemos así la importancia de ser críticos con la creación de nuevas iniciativas y, en su lugar, reforzar las existentes. Por ejemplo, agregando un enfoque de salud mental para el uso de plataformas de redes sociales y de entretenimiento en las iniciativas que viene ejecutando la SGTD.

[8] Para más información, visitar: https://www.gob.pe/ninasdigitales
[9] Para más información, visitar: https://www.gob.pe/internetsegura

5. Comentarios finales

Saludamos la propuesta que busca aumentar los estándares de protección para reforzar la seguridad en línea de las niñas, niños y adolescentes, así como reforzar y hacer efectivo su derecho a la protección de datos personales y su salud mental. Desde Hiperderecho, velamos también por el mismo objetivo y por ello esperamos se tomen en cuenta los comentarios expuestos, a fin de que la propuesta sea coherente, y se base en problemas basados en la evidencia, y construya sobre la base tanto de los avances técnicos de control parental ya existentes, como de las políticas públicas que vienen siendo ejecutadas por el Ejecutivo (a través de la SGTD).

De igual forma, si bien en este oficio no se exponen detalladamente todas las medidas, es recomendable que estas sigan una evaluación cuidadosa desde garantías como el test de proporcionalidad o una evaluación de impacto en derechos humanos. Debido a que se contienen numerosas y diversas medidas, desde políticas públicas de rendición de cuentas (como la publicación de informes trimestrales de acceso público sobre la adopción y cumplimiento de las medidas propuestas); políticas de inclusión digital (como capacitaciones o iniciativas dirigidas a colegios de zonas rurales); y de salud mental financiadas por privados (como el 1% que deben pagar los proveedores para un Fondo de Salud Mental); hasta la creación de servicios (como la provisión de Wi-Fi gratuito en espacios públicos); e incluso sanciones administrativas (como multas a los proveedores). Por ello, esperamos también que esta Comisión del Congreso asegure la participación activa de múltiples y diversos actores en estas materias.

Esperamos que usted tenga a bien recibir los comentarios y sugerencias expuestas. Quedamos a su disposición para cualquier participación en mesas de diálogo, mesas temáticas o técnicas, para brindar mayores alcances sobre los comentarios alcanzados vinculados a este Proyecto, o a cualquier otra iniciativa que requieran en materia de derechos digitales. Sin más, le expresamos nuestros mejores deseos y mayor consideración.

Atentamente,

Rubiela Gaspar
Coordinadora Legal en Políticas Públicas
Correo: rubiela@hiperderecho.org

Dilmar Villena Fernández Baca
Director Ejecutivo
Correo: dilmar@hiperderecho.org

Asociación Civil Hiperderecho.