

TRABAJO PRÁCTICO

Evolución del Sistema de Derechos en la Sociedad de la Información: Protección de Menores en Redes Sociales

Alumno:	[Lucas Eduardo Ramirez Bonch]
Carrera:	Técnico Superior en Análisis de Sistemas
Curso:	3er año - CICLO LECTIVO: 2025
Docente:	Valeria Alejandra Sosa
Fecha de Presentación:	12/12/2025

Repositorio: <https://github.com/Lubonch/TP-Legislacion>

Índice

INTRODUCCIÓN	3
1. EL SISTEMA DE DERECHOS	4
2. RIESGOS DIGITALES Y DELITOS INFORMÁTICOS CONTRA MENORES	4
2.1. Delitos y contenidos ilícitos	5
3. Regulación internacional	5
4. El impacto de la regulación de redes en el sistema de derechos	6
4.1. Verificación de edad y sus riesgos: El caso de Discord	7
5. ¿Cómo aborda la justicia Argentina la regulación de redes sociales?	7
5.1. Responsabilidad de los proveedores de servicios	7
5.2. Responsabilidad parental y el sharenting	8
CONCLUSIÓN	10
BIBLIOGRAFÍA	11

INTRODUCCIÓN

El surgimiento de las TICs(Tecnologías de la Información y la Comunicación) provocó una transformación en el ámbito empresarial y social, creando lo que se denomina la sociedad de la información y el conocimiento. Aunque estas tecnologías tienen como objetivo mejorar la calidad de vida humana, la transición digital presenta desafíos en la seguridad informática. El inicio de la web 2.0 consolidó este panorama tecnológico mediante la facilitación de espacios interactivos donde los usuarios pueden interactuar creando contenido, estableciendo comunidades virtuales.

En este marco digital, se manifiesta una tensión entre el ejercicio de los derechos fundamentales como la libertad de expresión y la intimidad, por un lado, y la necesidad de establecer marcos regulatorios que protejan bienes jurídicos esenciales, sobre todo cuando involucran menores de edad, que son los más vulnerables frente a los riesgos del entorno digital.

El objetivo de este trabajo es analizar la evolución del sistema de derechos en su adaptación a los problemas emergentes del ciberespacio, concentrándose en las exigencias regulatorias que se le exigen a las plataformas digitales para asegurar la protección de los menores.

1. EL SISTEMA DE DERECHOS

El ordenamiento jurídico argentino establece una jerarquía normativa, colocando en lo más alto a la constitución nacional junto con los tratados internacionales incorporados mediante el Art. 72 inc. 22

Esta estructura constitucional reconoce la evolución histórica de los derechos fundamentales, los cuales se pueden categorizar en distintas generaciones según su desarrollo temporal y características.

1. **Derechos de Primera Generación** : Surge durante las grandes revoluciones liberales (como la Revolución Francesa), con el propósito de establecer un límite entre el poder del estado y la autonomía individual. Incluye la libertad de expresión y el derecho a la intimidad.
2. **Derechos de Segunda Generación** : Corresponden a los Derechos Económicos Sociales y Culturales que surgieron a principios del siglo XX en respuesta a las desigualdades y explotación laboral derivadas de la revolución industrial
3. **Derechos de Tercera Generación** : Corresponden a los derechos colectivos, responden a la necesidad de proteger intereses compartidos, como el derecho a un medio ambiente sano, los derechos de los pueblos originarios. Sin estos derechos se pondría en riesgo el ejercicio de las generaciones anteriores.
4. **Derechos de Cuarta Generación** : Corresponden a los derechos que nacen del mundo informático, busca adaptar las garantías fundamentales al entorno digital. Incluyen el derecho al libre acceso a la información, la reducción de la brecha digital y la protección de datos personales.

2. RIESGOS DIGITALES Y DELITOS INFORMÁTICOS CONTRA MENORES

La exposición de los menores de edad a los riesgos del entorno digital requieren la intervención del derecho penal y civil. En Argentina, el Código civil y comercial de la nación establece el régimen de capacidad progresiva, que afecta cómo el menor ejerce sus derechos.

Capacidad progresiva : Una persona menor de 13 años no es capaz de ejercer derechos por sí misma y requiere la representación de sus padres o tutores legales. Los adolescentes entre 13 y 16 años tienen una capacidad limitada y son escuchados en procesos que los involucran. A partir de los 16 años ya es considerado un adulto para las decisiones relacionadas con el cuidado de su cuerpo.

2.1. Delitos y contenidos ilícitos

1. **Pornografía Infantil** : La Ley 26.388 tipifica la pornografía infantil(art 128 Código Penal) como la representación de un menor de dieciocho años dedicado a actividades sexuales explícitas.
2. **Grooming** : La Ley 26.904 tipifica el grooming como el acto de un adulto que contacta a un menor de edad mediante medios digitales con el propósito de cometer un delito contra su integridad sexual.
3. **Acceso ilegal a datos personales** : El acceso ilegal(Art. 153 bis y 157 bis del Código Penal) es tipificado por la Ley 26.388. Incluye la violación de correos electrónicos, redes sociales y otros servicios digitales.

3. Regulación internacional

País/Ley	Edad Mínima	Características principales
Estados Unidos KOSMA/PKSMA (S.278)	13 años (cuentas) 17 años (algoritmos)	Prohíbe los sistemas de recomendación personalizados (profiling) para menores de 17 años. Pendiente de promulgación (Entraría en vigor 1 año después de su aprobación).
Australia Online Safety Act	16 años	Prohíbe el acceso a redes sociales a menores de 16 años. Requiere verificación de edad a los titulares de cuentas en las plataformas restringidas. Vigente: 10 de Diciembre 2025.
Unión Europea Digital Services Act	13 años (Aprobación PE) Debate: 15/16 años	Exige a las grandes plataformas online (VLOPs) que eliminen mecanismos adictivos. Busca implementar la Carta Digital.europea para control de edad más efectivo. Vigente: 16 de Noviembre 2022.

Cuadro 1: Comparación de regulaciones internacionales sobre protección de menores en redes sociales

1. **PKSMA/KOSMA** : El proyecto S. 278 busca prohibir que los menores de 13 años accedan a redes sociales y limitar los sistemas de recomendación personalizados(profiling) para menores de 17 años.
2. **OSA** : La OSA(online safety act) prohíbe el acceso a redes sociales a menores de 16 años, exige que las plataformas implementen medidas para el cumplimiento e impone multas millonarias por la violación. Exige la verificación de edad para todos los titulares de cuentas en plataformas que estén restringidas por edad.
3. **DSA** : La DSA(Digital Service Act) obliga a las grandes plataformas a tener la responsabilidad de proteger a los menores. Prohíbe la eliminación de mecanismos

adictivos (como las rachas, o "streaks") y exige verificación de edad para acceder a servicios en línea. El Parlamento Europeo aprobó fijar la edad mínima de acceso a redes sociales en 13 años, pero los estados miembros debaten elevarla a los 15 o 16 años. La comisión europea está trabajando en el desarrollo de la "European digital wallet" para facilitar la verificación de la identidad digital y facilitar la implementación de controles de edad.

4. El impacto de la regulación de redes en el sistema de derechos

La regulación de las redes sociales impone deberes de control que generan un impacto directo en las distintas generaciones de derechos.

1. **Libertad de expresión y la primera Generación :** Los filtros y controles de contenido pueden crear efectos de censura que limitan la libertad de expresión. Existe el riesgo de que algoritmos de detección eliminen contenido legítimo o que la autocensura se incremente por temores a las restricciones. Esto plantea un dilema entre proteger a los menores sin vulnerar los principios que caracterizan a los derechos de primera generación.
2. **Refuerzo de la tercera y cuarta generación:** La regulación internacional se justifica ya que los usuarios no tienen el mismo nivel de conocimiento técnico que tienen las plataformas digitales. Por lo que la regulación busca proteger los derechos colectivos.
 - **Libertad de expresión:** El control algorítmico y el profiling se basan en almacenar los datos de forma indiscriminada, lo que genera un oligopolio de la información y pone en riesgo la autodeterminación informativa de los usuarios. Al exigir que las grandes plataformas eliminen los mecanismos adictivos y prohibir el profiling para menores, se refuerza el control del individuo sobre sus datos personales.
 - **Protección de datos y verificación de edad:** Implementar sistemas de verificación de edad por parte de las plataformas conlleva grandes riesgos de privacidad. La recolección de datos sensibles necesarios para esta verificación genera una gran incertidumbre sobre cómo se van a proteger estos datos. Esto aplica tanto a menores como a los adultos, ya que ambos pueden verse afectados por la mala gestión de estos datos.

4.1. Verificación de edad y sus riesgos: El caso de Discord

Discord es una aplicación de mensajería que permite a los usuarios crear servidores y canales para comunicarse a través de texto, voz y video.

Durante abril del 2025 Discord comenzó a implementar un sistema de verificación de edad solicitando una foto de un documento de identidad para adelantarse a las futuras regulaciones, prometiendo que las fotos solo se iban a usar para la verificación y que no iban a ser almacenadas.

Sin embargo, en octubre del 2025 un incidente de seguridad que sufrió un proveedor externo de servicios (5SA) puso en compromiso los datos personales de unos 70.000 usuarios, incluyendo las fotos de los documentos de identidad que se usaron para verificación de edad.

Este caso pone en evidencia que más allá de proteger a los menores de edad, la verificación de edad trae nuevos riesgos que se deben considerar al momento de implementar estos sistemas y se debe tener un marco de seguridad legal que imponga:

- La obligación de garantizar que las plataformas adopten medidas de seguridad y confidencialidad para proteger los datos personales sensibles.
- La supresión de datos sensibles una vez que se haya completado la funcional para la que fueron recolectados.
- Delegar los procesos de verificación a proveedores externos no debe sacar la responsabilidad de proteger los datos personales a las plataformas digitales.

5. ¿Cómo aborda la justicia Argentina la regulación de redes sociales?

La justicia argentina aborda los conflictos del entorno digital aplicando los principios generales del derecho adaptándolos a un contexto tecnológico.

5.1. Responsabilidad de los proveedores de servicios

Los proveedores de servicios de internet son definidos como intermediarios tecnológicos que permiten acceder a redes datos, así como también transmitir y almacenar los datos.

La ley 27.078(Ley argentina Digital) declara de interés público el desarrollo de las TICs y establece principios para los prestadores de servicios:

1. **Neutralidad de Red** : Garantiza la completa neutralidad de las redes y prohíbe que los prestadores de servicios bloqueen, interfieran o restrinjan el acceso a

cualquier contenido o aplicación, salvo por una orden judicial o una expresa solicitud del usuario.

2. **Inviolabilidad de las comunicaciones :** Garantiza la inviolabilidad de la correspondencia y comunicaciones electrónicas, incluyendo los datos de tráfico. Su interceptación solo puede realizarse mediante una orden judicial.

Los proveedores de servicio también tienen el deber de prevenir el daño que tiene cualquier otra persona (Art 1710 CCyC), lo que les exige tener que adoptar medidas necesarias para evitar que se produzca un daño o en el peor de los casos disminuir su magnitud. Esto se ve reforzado por las obligaciones legales específicas:

1. **La obligación de ofrecer software de protección que impida el acceso a sitios específicos,** al momento de ofrecer los servicios de internet (ley 25.690).
2. **La obligación de informar y recomendar el uso de programas de bloqueo de sitios,** en las facturas que emiten. Esta inscripción debe recomendar a los padres a ejercer un razonable control por los contenidos que consumen sus hijos aconsejar que consulten con el proveedor para que les brinde asesoramiento sobre programas de bloqueo de sitios.

5.2. Responsabilidad parental y el sharenting

La Responsabilidad parental es el conjunto de deberes y derechos que tienen los padres sobre la persona y bienes del hijo para su protección, desarrollo y formación integral(y dentro del contexto digital también incluye la protección de su identidad digital y privacidad). El estado actúa como garante para exigir el cumplimiento de estos deberes.

La ley 26.061 establece que los menores tienen el derecho a ser respetados en su dignidad, reputación y propia imagen.

El sharenting es la práctica de los padres donde comparten contenido relacionado con sus hijos en las redes sociales y ha generado jurisprudencia debido a la ausencia de legislación donde los tribunales intervinieron para proteger los derechos personalísimos de los hijos.

1. **V. F. C/ S. B. S/ MEDIDAS PRECAUTORIAS (ART. 232 DEL CPCC) :** en el fallo el Padre(V. F. C.) solicita que se intime a la madre(S. B.) a abstenerse de subir fotos y videos de sus hijas en redes sociales con fines comerciales. El tribunal aplicó el interés superior del niño, dándole prioridad a los derechos personalísimos de las niñas sobre el derecho a la libertad de expresión de la madre.

El Fallo reafirma que la responsabilidad parental no incluye el derecho a exponer a los hijos en las redes sociales y no puede realizarse de forma unilateral y siempre debe ceder ante el interés y la voluntad del niño.

CONCLUSIÓN

El avance constante de la tecnología transformó la forma en la que interactuamos y nos comunicamos entre nosotros. Estos cambios trajeron consigo nuevos desafíos y riesgos, sobre todo cuando se trata de proteger a los menores de edad. Esto genera la necesidad de establecer marcos regulatorios que los protejan pero que a su vez no limiten su libertad de expresión y acceso a la información.

La regulación internacional muestra que no existe una solución única, mientras en la Unión Europea se optó por un enfoque que mezcla la regulación de datos y la transparencia de los algoritmos, en Australia se tomó una medida más drástica prohibiendo el acceso a las redes sociales para los menores de 16 años. Un gran desafío que tienen estas regulaciones es encontrar el equilibrio en la protección de los derechos de primera generación y la cuarta generación, ya que la protección de los datos busca prevenir que la dignidad humana se vea afectada por el manejo indiscriminado de datos personales.

El caso de Discord muestra cómo la implementación de un sistema de verificación de edad puede generar riesgos críticos en la seguridad de los datos y que si bien la verificación de edad es importante para proteger a los menores, el no garantizar que los datos sensibles sean eliminados adecuadamente puede exponer a todos los usuarios a problemas más graves.

En Argentina, el marco jurídico actual nos da una base sólida que requiere actualización para poder abordar estos problemas. La Ley de Protección de Datos Personales (25.326) ya establece el principio de calidad de los datos y obliga a que la recolección sea adecuada y no excesiva, y que estos datos sean destruidos una vez que se cumpliera la finalidad para la que fue recolectado. Sin embargo, esta ley debería incluir una disposición específica sobre los algoritmos y la verificación de edad para controlar las decisiones automatizadas que pueden poner en peligro la dignidad de la persona.

BIBLIOGRAFÍA

- *Digital Services Act (DSA)*. The Digital Services Act package, UE.
- *General Data Protection Regulation (GDPR)*. Data protection under GDPR, UE.
- Investigación sobre el DSA: TikTok y Meta (El Confidencial, Julio 2025).
- Debate sobre la edad mínima en redes sociales: 15 o 16 años (Infobae, Junio 2025).
- Enmienda de Seguridad en Línea (Ley de Australia, The Guardian, Noviembre 2024).
- Enmienda de Seguridad en Línea (Enlace oficial, Ley de Australia).
- *Protecting Kids on Social Media Act (KOSMA)*. Proyecto de ley S. 278, EE. UU.
- *Protecting Kids on Social Media Act (Argumentos de apoyo, Social Media Victims)*.
- *Código Civil y Comercial de la Nación (Argentina)*.
- *Ley N° 25.326 (Protección de los Datos Personales)*.
- *Ley N° 25.506 (Firma Digital)*.
- *Ley N° 26.388 (Delitos Informáticos)*.
- *Ley N° 27.078 (Argentina Digital)*.
- *Responsabilidad por daños derivados de Internet*. Claudio F. Leiva, SAIJ.
- *V. F. C/ S. B. S/ MEDIDAS PRECAUTORIAS*. Suprema Corte de Justicia de la Provincia de Buenos Aires, Causa N° 3672.
- *Nuevas Tecnologías: Plataformas digitales y competencia*. Corte Suprema de Justicia de la Nación.
- *Update on a Security Incident Involving Third-Party Customer Service*. Discord Press Release.
- *ID photos of 70,000 users may have been leaked, Discord says*. BBC News.