# NOTA TÉCNICA

## INTERNET SEGURO POR DEFECTO PARA LA INFANCIA Y EL PAPEL DE LA DE VERIFICACIÓN DE EDAD

Octubre 2024

# ÍNDICE

# I. RESUMEN EJECUTIVO

En la presente nota técnica de la AEPD se demuestra que **es posible realizar una protección efectiva de niños, niñas y adolescentes (NNA) en Internet sin que ello suponga una vigilancia sistemática o invasión de la privacidad de todos los usuarios**, y sin exponer a los NNA a ser localizados y expuestos a nuevos riesgos. Para ello, es necesario **cambiar el paradigma** utilizado hasta ahora para proteger a la infancia: en lugar de emplear las actuales estrategias reactivas, se propone conseguir una protección real y efectiva de los NNA aplicando los principios de **protección de datos por defecto**. Este cambio de aproximación a la hora de diseñar los tratamientos de datos personales que se llevan a cabo en Internet permite configurar un espacio seguro por defecto para la infancia que garantiza que los NNA puedan **disfrutar de sus derechos y libertades en el entorno digital.**

En la presente nota se analizan **cuatro casos de uso diferentes** y se recomiendan buenas prácticas para proteger a los NNA, y por extensión a todos los colectivos vulnerables, en su acceso a Internet ante riesgos relacionados con el acceso a contenidos, el contacto con personas que puedan ponerlos en peligro, la contratación de productos y servicios, la monetización de sus datos personales, la inducción a comportamientos adictivos que afecten a su integridad física o mental y con otros aspectos de corte transversal. **Todos estos riesgos tienen como causa o efecto el tratamiento de datos personales de menores**.

Las **estrategias reactivas** empleadas hasta el momento se basan en permitir que los NNA sean expuestos a dichos riesgos y, en el mejor de los casos, reaccionar cuando se detecte que ya se está produciendo un daño o impacto. En ocasiones también se ha propuesto una protección basada en que **los proveedores de servicios** de Internet conozcan **qué usuario es un NNA**, por ejemplo, para posibilitar la creación de espacios o cuentas específicos para los NNA. Estas estrategias precisan de una **intervención intrusiva en forma de vigilancia o perfilado** que vulnera de manera sistemática la privacidad de todos los usuarios: permiten **tener al menor localizado y fácilmente accesible** para cualquier actor malicioso, pueden pretender **legitimar nuevos tratamientos de datos personales de NNA**, adaptan los mensajes para que tomen decisiones que, en muchos casos, no les corresponden o pueden **esconder propósitos de perfilado** en relación con patrones engañosos o adictivos, fidelización, contratación, consumo o monetización de datos personales.

Todos estos riesgos se pueden evitar haciendo efectivo el derecho de NNA, y de otros colectivos vulnerables, a un **Internet seguro por defecto**. Seguro más allá de la ciberseguridad, en el sentido de impedir cualquier daño al interés superior del menor y a sus derechos fundamentales debido al tratamiento de sus datos personales, de manera que los NNA, familias y resto usuarios tengan el control de sus propios datos.

**La verificación de edad** es una de las herramientas que permite el diseño de este Internet seguro por defecto y la propuesta de la AEPD es que esta verificación de edad sea un **habilitador** para acceder a cualquier elemento que implique un riesgo, asumible para las personas con madurez e información suficiente, o para tomar decisiones cuando asumen la patria potestad o tutela de un NNA. Además, manteniendo **la carga de la prueba en el usuario con la edad adecuada para ello, y nunca en el NNA,** evitando la creación de esquemas de identidad para menores controlados por distintos proveedores de servicios.

**La verificación de edad, *per se*, no es suficiente** para garantizar un Internet seguro por defecto, es necesario que se diseñe e implemente de manera que se cumplan todos los principios y requisitos recogidos en el RGPD, además de la adaptación de los servicios de Internet y la integración con otras soluciones para que sea efectiva, no genere nuevos riesgos, no permita localizar NNA y que su uso no suponga ninguna pérdida de derechos o libertades.

## II. INTRODUCCIÓN

Internet ofrece **oportunidades** educativas, sociales o creativas para las niñas, niños y adolescentes (NNA). Sin embargo, y en el marco del tratamiento de sus datos personales, en Internet se materializan **nuevos riesgos** asociados al contenido inapropiado, al ciberacoso, la explotación, las adicciones o el consentimiento para ciertas actividades u operaciones. Otros riesgos que afectan a los NNA son los que implican considerarlos sujetos pasivos que pueden ser **dirigidos, manipulados o convertidos en clientes** cautivos a largo plazo, o tratados como **productos monetizables** a través de su "datificación". La protección del **interés superior del menor** debe ser una **prioridad** en el entorno digital al igual que lo es en el mundo físico.

La **normativa de protección datos** establece principios, derechos y obligaciones con relación al tratamiento de los datos personales en general, y **con mayores garantías cuando se trata de los datos personales de NNA**. Estas implican obligaciones de cumplimiento específicas que legitimen los tratamientos y que gestionen los riesgos para los derechos y libertades de los NNA y de todos los usuarios de Internet.

La estrategia seguida **hasta el momento** para proteger a la infancia en Internet por parte de la mayoría de los proveedores de productos digitales ha sido de tipo **reactivo**. Es decir, mantener un diseño de los servicios que permiten que **los NNA sean expuestos a dichos riesgos** a través de tratamientos de sus datos personales y, en el mejor de los casos, reaccionar cuando se detecte que ya se está produciendo un daño o impacto. Esto implica exponer al menor a que, por ejemplo, cualquier usuario pueda contactarlo; someter a todos los usuarios a técnicas de vigilancia y perfilado; acumular evidencias de acoso, *grooming*, pedofilia u otros; aplicar criterios establecidos por el proveedor y finalmente actuar. Este tipo de estrategia necesita que exista evidencia de un daño al NNA para que se activen medidas de protección. Otras estrategias están basadas en **posibilitar a los proveedores de servicios** de Internet el conocimiento de **quién es un NNA**, o incluso qué edad concreta tiene. Por ejemplo, cuando se ofrecen espacios o cuentas específicos para menores. De esta forma, el proveedor pretende configurar y monitorizar la actividad del NNA durante el uso de su servicio o adaptar los mensajes para que tome decisiones (que, en muchos casos, no le corresponden).

La aplicación de estas estrategias precisa de una **intervención intrusiva de los servicios de Internet en forma de vigilancia o perfilado** que vulnera de manera sistemática la privacidad de todos los usuarios. Además, implican **tener al menor localizado y fácilmente accesible** para servicios de terceros o, directamente, actores maliciosos. Esta estrategia **puede pretender legitimar un tratamiento masivo datos personales de NNA y de todos los usuarios.** Además, pueden **esconder propósitos de perfilado** en relación con patrones engañosos o adictivos, fidelización, contratación, consumo o monetización de datos personales. En muchos casos además pretenden crear **nuevos esquemas de identidad digital**, planteada la identidad como un servicio en lugar de como un derecho. Y es que estos esquemas, aplicados inicialmente a los NNA, serían los que se extenderían en el futuro, dado que los usuarios que ahora son NNA se convertirán en usuarios adultos más adelante.

Estos riesgos se pueden evitar haciendo efectivo el derecho de los NNA, y de otros colectivos vulnerables, a un **Internet seguro por defecto**. Hay que aclarar que seguridad significa mucho más que ciberseguridad. Seguridad implica impedir que se produzca un daño al interés superior del menor y a sus derechos fundamentales debido al **tratamiento de sus datos personales**. No solo hay que proteger sus datos personales de un tratamiento no autorizado, su pérdida, destrucción o daño, se deben **proteger a los NNA también de los riesgos que producen tratamientos de datos personales "autorizados"** y que son causa o efecto de, por ejemplo, para su integridad tanto física como mental. También

significa devolver al NNA, y a aquellos que ostentan la patria potestad o tutela, **el poder de las decisiones sobre sus propios datos**, lo que se traduce en poder decidir hasta qué punto se expone al menor a contactos, contratos, conductas y contenidos potencialmente dañinos.

Un Internet seguro por defecto debe construirse **desde el diseño**, y siguiendo el principio de minimización, ya que el tratamiento de los datos personales del NNA, su localización y su accesibilidad, son algunas de las principales causas de riesgo. Para ello, no es suficiente incluir una capa de seguridad adicional sobre los servicios de Internet tal como están implementados actualmente, sino que **los proveedores de servicios en Internet tienen la obligación** de evolucionar para **implementar los principios de protección de datos desde el diseño y por defecto**.

**La verificación de edad** es una de las herramientas que permite el diseño de un Internet seguro por defecto, aunque no es la única ni puede dar solución a todos los retos que este diseño implica por sí sola. Se debe entender la verificación de edad como un **habilitador** para acceder a cualquier elemento que implique un riesgo, asumible para las personas con madurez e información suficiente, o para tomar decisiones cuando asumen la patria potestad o tutela de un menor. De esta forma, **el NNA no debe probar que lo es**, ni exponer su naturaleza para que se bloqueen contenidos, contactos, contratos o funcionalidades, ni recibir una información para poder tomar decisiones que no le corresponden. Al contrario, esta aproximación **proactiva** devuelve a los familiares y tutores la capacidad de ejercer su deber de cuidado, y **trasladan "la carga de la prueba" de superación de un umbral de edad para exponerse a riesgos**, y de la voluntad de hacerlo, al adulto, como establece el Artículo 8 del RGPD y el Artículo 7 de la LOPDGDD. Para que sea efectiva, además, debe hacerse **por defecto**.

Con un Internet seguro por defecto, la condición de menor de un NNA o su edad no se exponen ni tratan. El tratamiento los datos personales de los NNA, incluida su condición de menor, no es necesario, proporcional y, en muchos casos, no es leal. **La carga de la prueba de superar el umbral de edad necesario para realizar una actividad determinada en Internet recae en el usuario con la edad adecuada. Y será un usuario adulto el que seleccione aquellos elementos (con los riesgos asociados) que se adecúan al nivel de madurez del NNA bajo su tutela**. El tipo de contenido al que puede acceder un NNA, sus contactos, los contratos que puede realizar o las funcionalidades de los servicios a las que puede acceder son decisiones que la normativa asigna a aquellos que ostentan la patria potestad o tutela, que son los que han de acreditar su capacidad de obrar y a los que ha de estar dirigida la información que les permita tomar una elección fundamentada, no al NNA.

La tecnología se debe diseñar e implementar para dar soluciones sin crear nuevas amenazas ni recortar los derechos y libertades de todos los usuarios. En particular, la verificación de edad **no debe crear nuevos riesgos, ni para los sujetos individuales, ni en forma de riesgos sistémicos** para la sociedad en su conjunto.

El ecosistema de Internet **no puede tratarse como un conjunto de islas independientes**. Para implementar un cambio de paradigma en la protección de los NNA se requiere, no solo una **cooperación** entre los intervinientes (proveedores, fabricantes, intermediarios, etc.) a la hora de diseñar sus soluciones, sino también una **comunicación efectiva** entre ellos y con el resto de la sociedad ante la identificación de nuevas amenazas a través de un **marco de gobernanza.**

Por ello, este documento está dirigido a los **proveedores, fabricantes, intermediarios y resto de operadores de Internet**, así como a las **autoridades de protección de datos, de consumo y a las competentes en la regulación del mercado**, especialmente de productos y servicios que se ofrecen en Internet y a las **organizaciones gubernamentales y no gubernamentales** que tienen como propósito la educación y la protección del menor, tanto

españolas como europeas. Por supuesto, también está dirigido a los **responsables de tratamientos de datos personales** que consuman o utilicen dichos productos y servicios que se ofrecen en Internet y a **aquellos que ostentan la patria potestad o tutela** de los NNA.

# III. ANTECEDENTES Y CONTEXTO

## A. OBLIGACIONES EN EL ECOSISTEMA DE INTERNET

**Diferentes agentes** como los padres, los educadores, los gobiernos, los reguladores, las autoridades judiciales o las autoridades de control **deben asumir sus correspondientes obligaciones** para garantizar que los NNA pueden aprovechar las oportunidades que ofrece el espacio digital mientras son **protegidos adecuadamente de los riesgos** que supone. En particular los miembros de la industria tecnológica deben asumir sus obligaciones en la protección de la infancia de manera que cumplan con la regulación vigente, en particular de **cumplimiento de la normativa de protección de datos** ya sea como responsables o encargados de tratamiento, y sean más ambiciosos mediante la incorporación de herramientas proactivas y la adaptación de procesos que permitan a los agentes ya mencionados ejercer sus diferentes responsabilidades. Además, hay que tener en cuenta que **el artículo 28 del Reglamento de Servicios Digitales** establece que las plataformas en línea que puedan utilizar los menores deben asegurarse de que sus servicios ofrecen un alto nivel de privacidad, seguridad y protección a los usuarios más jóvenes.

Los proveedores de servicios de Internet, y en la medida que les compete los distintos intervinientes en el ecosistema de Internet (fabricantes, otros proveedores, intermediarios, etc.), deben proporcionar **un entorno que sea seguro por defecto para la infancia**, sin arrogarse funciones que corresponden a los padres, los educadores, los gobiernos, los reguladores, las autoridades judiciales o las autoridades de control. La protección del menor estará en riesgo si se pretende impedir que ejerzan sus obligaciones en la vigilancia, cuidado y educación de los NNA. **Sus diferentes responsabilidades no son delegables**, ni deben basarse en “actos de fe”, sobre todo, en actores de Internet cuyos intereses, dado su modelo de negocio actual, pueden colisionar directamente con la **protección de los derechos fundamentales** de todos los usuarios.

Cuando esto ocurre, se suele desplegar una **hipervigilancia** que implica tratamientos masivos de datos personales de todos los ciudadanos, perfilado, detección de NNA en, por y a través de los servicios digitales, pérdida de control de los datos personales (considerando 7 del RGPD) y, en el peor de los casos, una manipulación (a través de patrones engañosos y adictivos) con propósitos de monetización.

## B. SEGURIDAD POR DEFECTO Y DESDE EL DISEÑO

Hasta ahora, la **prevención** de los riesgos para NNA en Internet se ha dejado, principalmente, en las manos de los propios NNA y en las de sus **padres y educadores**. Los **proveedores** y el resto de los intervinientes en el ecosistema digital se han centrado en desarrollar **estrategias reactivas** en las que, una vez expuestos los NNA a los riesgos e incluso una vez producidos los daños o impactos, se actúa en consecuencia. Un claro ejemplo es la posibilidad (incluso el fomento) de que cualquiera pueda iniciar un contacto con un NNA a través de un servicio o plataforma sin que, por defecto, la decisión de quién puede realizar este contacto esté en manos de aquellos que ostentan la patria potestad o tutela. Sólo ante la evidencia de algún tipo de acoso, siguiendo los criterios del propio proveedor del servicio, se ponen en marcha los mecanismos de alerta.

Esta aproximación supone **un riesgo para el interés superior del menor y para sus derechos fundamentales**. Pero también para los **derechos fundamentales del resto de los usuarios de Internet**, ya que se centra en **la vigilancia y el perfilado** realizados por los

proveedores de servicios para detectar las situaciones de riesgo y sus potenciales impactos con criterios establecidos por ellos mismos. Implica un tratamiento de datos personales que no es necesario y que **no cumple el principio de minimización**. Este enfoque hace que la reacción, si es que se produce, tenga lugar cuando ya se han producido daños que pueden ser irreversibles, por lo que no se supera un análisis de necesidad. El tratamiento no es idóneo al no cumplir su objetivo con eficacia.

Las medidas reactivas se han justificado en el pasado porque se han diseñado los productos digitales para que se dificulte, o directamente se impida a los padres, los educadores, los gobiernos, los reguladores, las autoridades judiciales o las autoridades de control, ejercer sus obligaciones en relación con la protección de los NNA. Todos estos productos digitales **facilitan desde el diseño, o incluso fomentan, que los NNA sean usuarios**. Una vez que lo son, queda en manos de los proveedores de dichos productos realizar los tratamientos necesarios para desplegar este tipo de medidas reactivas. Esto podría suponer **un quebrantamiento del principio de lealtad**. La lealtad es un principio general que exige que los datos personales no se traten de manera injustificadamente perjudicial, ilícitamente discriminatoria, inesperada o engañosa para el interesado[1].

Tomando como ejemplo el mundo físico, para garantizar el derecho de los NNA a circular libremente por las calles, éstas deben ser seguras por defecto y siempre deben hacerlo bajo supervisión de un adulto. Padres, educadores, gobiernos, reguladores y otras autoridades deben disponer de los recursos necesarios para ejercer sus diferentes obligaciones y establecer, en cada caso, las medidas *a priori* que eviten los principales elementos de riesgo.

Pero no se puede pretender un nivel de protección superior en el entorno digital que en el físico o con un nivel de participación o de involucración menor de los agentes antes mencionados (padres, educadores, gobiernos, reguladores, autoridades judiciales, autoridades de control) para conseguirla. Esto exige una **visión holística** del interés superior del menor y de la protección de sus derechos fundamentales, es decir, un Internet seguro por defecto no puede limitarse a unos aspectos concretos (acceso a contenido inadecuado, captación, adicción, etc.), ni considerarlos de forma inconexa, sino que tienen que contemplarse **todos los derechos de forma unificada, sin establecer ninguna jerarquía o prioridad entre ellos**.

Hay que tener en cuenta además que la seguridad de los NNA en Internet está directamente relacionada con el concepto de ***safety* o protección**, es decir, se debe garantizar que, con la excusa de un seguridad sesgada o mal entendida, no se produce un daño al interés superior del menor y que no se vulneran sus derechos fundamentales. Y no tanto con el concepto de *security* o seguridad (ciberseguridad), es decir, la garantía de que la información vinculada a la actividad del NNA esté sometida a unas medidas adecuadas que reduzcan el riesgo de pérdida, destrucción o daño accidental. Aunque **la seguridad es un factor importante** para alcanzar la protección, **no se puede reducir** la segunda a la primera, esto es una simplificación que lleva a cometer errores como pensar que una única medida o estrategia puede resolver el problema. De hecho, se puede alcanzar un alto grado de ciberseguridad sin proteger al NNA, es más, incluso con graves impactos en sus derechos y libertades.

[1] EDPB, Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, Versión 2.0, Adoptadas el 20 de octubre de 2020: https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf

## C. VERIFICACIÓN DE EDAD

Si bien la protección de la infancia es crucial, debe ser siempre compatible con los **derechos y libertades de toda la ciudadanía**. Esta protección se puede conseguir con una **combinación adecuada** de diferentes métodos, herramientas y procesos, entre los que juega un papel crucial la **verificación de edad de forma estrictamente respetuosa con todos los derechos fundamentales de todos los usuarios**.

Las soluciones de verificación de edad son aquellas que permiten **determinar si un usuario supera la edad mínima requerida para pasar un control de edad (*age gate*) en línea**. Por ejemplo, si un usuario supera los 18 años requeridos para jugar a un videojuego calificado como violento o para configurar una *app* de mensajería de manera que se puedan recibir mensajes de cualquier otro usuario sin limitaciones. Como se desarrolla en la presente nota técnica, este tipo de solución permite asegurar que el usuario que accede a contenidos, contactos, contratos o funcionalidades con restricciones de edad tiene la edad requerida para hacerlo.

El RGPD exige el cumplimiento del principio de exactitud en los datos con respecto a los fines para los que se tratan (artículo 5, apartado 1, letra d del RGPD). La verificación de edad, en cuanto puede limitar derechos fundamentales, ha de ser exacta en cuanto a la idoneidad para cumplir con su propósito: capacitar para el acceso a ciertos elementos de Internet que implican un riesgo para los NNA. Esto no significa que siempre sea necesario el tratamiento de la fecha de nacimiento de los usuarios de Internet por parte de los proveedores de productos digitales. **Recoger la fecha de nacimiento o la edad precisa** de los usuarios de Internet, cuando no es necesario, es contario al principio de minimización. En la mayor parte de casos de uso será suficiente con saber si el usuario **supera un umbral de edad** o, en caso de recurrir a terceros de confianza mediante arquitecturas *tokenizadas*[2], simplemente si está capacitado para acceder al elemento que solicita con un "supera el umbral de edad requerido", "SÍ", "OK", etc.

El enfoque de aplicación de la verificación de edad debería ser siempre el de **habilitación**, es decir, orientado a demostrar que se supera el umbral de edad y que, por lo tanto, se puede realizar la operación que se está solicitando. De esta manera se limita el riesgo para los menores, se aplica la minimización de datos, y el tratamiento es proporcional, ya que se evita el tratamiento de datos personales de NNA para disponer de acreditaciones o certificados específicos, instalar aplicaciones, etc. Los productos digitales deben proteger **por defecto y desde el diseño** a los NNA, impidiendo que corran riesgos, no esperando a que ya estén expuestos a ellos para reaccionar e intentar mitigarlos. En este sentido, la verificación de edad puede ser una herramienta muy útil.

Por este motivo la presente nota técnica explora el uso de las soluciones de verificación de edad para la protección de la infancia en Internet, ya que se trata de una las herramientas con más potencial en lo que se refiere a dicha protección. Pero, al mismo tiempo, con más **implicaciones para la privacidad y protección de datos**. De hecho, como es probable que, por su naturaleza, alcance, contexto u fines, la verificación de edad entrañe un alto riesgo para los derechos y libertades de los individuos, el responsable del tratamiento de datos personales asociado a esta verificación deberá realizar, antes del tratamiento, **una evaluación del impacto que dicho tratamiento tiene en la protección de datos personales**.

[2] En este tipo de arquitecturas tecnológicas un proveedor tercero de confianza especializado en realizar verificación de edad es quién realiza las comprobaciones de oportunas con el usuario, de manera que al proveedor de la aplicación o servicio sólo le llegue un token o credencial que acredita que el usuario supera el umbral de edad requerido, ninguna otra información.

## D. RIESGOS SISTÉMICOS

En relación con estas implicaciones para los derechos y libertades y con el concepto de riesgo, se debe evitar además que las soluciones de verificación de edad puedan tener un **impacto realmente significativo en la sociedad**, la economía o la seguridad a causa de su amplia influencia o de su capacidad para afectar a un gran número de usuarios[3]. Estos riesgos, podrían ocurrir si se otorga al proveedor de una solución de verificación el poder de un monopolio, o la capacidad de perfilar a un número significativo de usuarios de Internet o si un fallo en su seguridad podría afectar a datos sensibles de ese número significativo de usuarios.

Hay que tener en cuenta que no sólo deben evitarse los riesgos para el interés superior del menor y para los derechos y libertades de todos los ciudadanos, sino también **los riesgos sistémicos** que un diseño o implementación determinado de las soluciones de verificación de edad pueden implicar dada su potencial escala. Un riesgo **es sistémico cuando puede provocar daños a personas a gran escala o a sistemas esenciales para la gobernanza y buen funcionamiento de la sociedad**.

Según el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) existen **cuatro categorías de riesgos sistémicos** (considerando 80). Dos de ellas tienen una relación muy estrecha con los tratamientos de datos personales que se realizan en las soluciones de verificación de edad.

La segunda categoría que se identifica en el Reglamento (considerando 81) se refiere a los **efectos reales o previsibles del servicio para el ejercicio de los derechos fundamentales**, tal como los protege la Carta. Si las soluciones de verificación de edad no se diseñan e implementan de manera adecuada, muchos de estos derechos pueden verse vulnerados, incluidos la libertad de expresión y de información, el derecho a la vida privada, el derecho a la protección de datos o el derecho a la no discriminación.

En concreto, y en relación con el derecho a la protección de datos, la protección del menor se emplea en ocasiones como una **justificación para la recogida masiva de datos de NNA y del resto de los usuarios en Internet**: perfilado masivo, categorización de contenidos y de usuarios, evaluaciones o decisiones automatizadas, etc. Las soluciones de verificación de edad en algunos casos se plantean como soluciones para la **gestión de la identidad digital** de los usuarios de Internet. Dicha identidad, proporcionada y gestionada como un servicio en lugar de como un derecho, **no está bajo el control de los propios usuarios**, sino que depende de los criterios e intereses de un proveedor que puede, discrecionalmente, eliminar dicha identidad o limitar la capacidad de obrar de las personas.

**La creación de un Internet seguro por defecto para la infancia no puede, en ningún caso, ser la coartada para estos tratamientos masivos de datos personales** que no cumplen con los principios de lealtad, transparencia o minimización de datos y vulnerarían diferentes derechos y libertades. Este riesgo sería sistémico dada su potencial escala y alcance.

Además, hay que tener en cuenta que una solución de verificación de edad que acaparase gran parte del mercado podría conducir a **una falta de disponibilidad puntual del acceso a contenidos, servicios, contratos**, etc. que afectara a diferentes derechos y libertades, pero también a la resiliencia de la infraestructura digital y a la economía.

[3] Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

La tercera categoría de riesgos sistémicos (considerando 82) se refiere a los **efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, así como sobre la seguridad pública**. Hay que tener en cuenta que, por su escala y nivel de intermediación en los flujos de información, ciertos servicios y aplicaciones se han convertido en espacios públicos con un papel central que facilita el debate público, el acceso a información o las transacciones económicas, por mencionar algunos ejemplos. El daño potencial, para los usuarios individuales, pero también para la sociedad, que implican soluciones de verificación de edad mal diseñadas e implementadas desde el punto de vista de su idoneidad es enorme (errores, sesgos, exclusión, etc.). De nuevo, la creación de un Internet seguro por defecto para la infancia **no puede, en ningún caso, ser la coartada para la limitación de acceso** a estos servicios y aplicaciones incumpliendo los principios de licitud, lealtad o exactitud y que vulnerarían diferentes derechos y libertades. Este riesgo sería además sistémico dada su potencial escala y alcance.

Si bien estas dos categorías de riesgos sistémicos son las que pueden provocar las soluciones de verificación de edad si no se diseñan o implementan adecuadamente, cabe otra reflexión: **no realizar verificación de edad en absoluto o hacerlo de manera que no sea idónea, también puede implicar riesgos sistémicos**. De hecho, la cuarta categoría de riesgos que identifica la DSA se deriva del **diseño, el funcionamiento o la utilización, mediante la manipulación, de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño, con un efecto negativo real o previsible en la protección de la salud pública, los menores y graves consecuencias negativas para el bienestar físico y mental de una persona, o en la violencia de género**. Como se establece en esta nota técnica la verificación de edad no evita por completo estos riesgos para el bienestar físico y mental de los menores, pero sí que es una herramienta fundamental para su protección. Por lo que, en ciertos casos, no realizar verificación de edad en absoluto o realizarla de manera que no cumpla su función, también puede suponer un riesgo sistémico, en particular cuando dicho sistema permite identificar y detectar NNA en Internet.

## E. CATEGORIZACIÓN DE LOS RIESGOS PARA LA INFANCIA EN INTERNET

Para comprender cómo la verificación de edad puede ayudar a proteger a los menores en línea primero es necesario comprender de qué hay que protegerlos exactamente. En esta nota se emplea la clasificación de la OCDE[4], de manera que se tienen en cuenta cinco categorías de riesgos, las denominadas cinco Cs:

1. **Contenido:** El contenido de odio (por raza, género, religión, orientación sexual, etc.), el dañino (pornografía, violencia extrema, consumo de sustancias, extremismo, desórdenes alimenticios, etc.), el ilegal (abuso sexual, terrorismo, etc.) y la desinformación pueden provocar impactos en la salud mental y en desarrollo afectivo de los menores.
2. **Conducta:** De nuevo, se observan los cuatro tipos de riesgos ya mencionados, pero en este caso se refieren al comportamiento del propio menor cuando utiliza Internet, que puede colocarle en una posición vulnerable por participar en conductas de odio (ciberacoso, etc.), dañinas (*sexting*, etc.), ilegales o participar en la distribución de desinformación.
3. **Contacto:** Se producen riesgos en categorías similares, pero en este caso los NNA son contactados por alguien que interactúa con ellos gracias a Internet y les hace

[4] "CHILDREN IN THE DIGITAL ENVIRONMENT: REVISED TYPOLOGY OF RISKS", OECD Digital Economy Papers, January 2021 No. 302. https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en

objeto de mensajes de odio, dañinos, ilegales o problemáticos por otros motivos. Algunos ejemplos claros son la sextorsión, el *grooming,* o las situaciones en las que los NNA proporcionan datos suficientes para pasar del contacto en el entorno real al contacto en el entorno físico, con riesgo para su derecho a la integridad. La diferencia con los riesgos de conducta es que en este caso el NNA es objeto o víctima directa en lugar de actor o parte activa.

4. **Consumo (contrato o consentimiento):** Se producen cuando el NNA es un cliente o consumidor, principalmente porque recibe publicidad de productos que no son adecuados (como tabaco, alcohol o servicios de citas), porque recibe publicidad que no puede identificar como tal (por ejemplo, por *product placement* o a través de un *influencer*), porque se aprovecha su credulidad, inexperiencia o falta de madurez para que consienta con acuerdos o contratos que no son beneficiosos para él o ella (por ejemplo, empleando patrones engañosos) o porque, directamente, no le corresponde al NNA tomar las decisiones sobre consumo, contrato o consentimiento[5].
5. **Corte transversal:** En esta categoría entran riesgos bastante heterogéneos que no se pueden clasificar en las categorías anteriores, principalmente:
    a. Riesgos para la **privacidad:** Como la sobreexposición provocada por ellos mismos, el *sharenting*, los tratamientos asociados a las tecnologías y plataformas educativas, etc.
    b. Riesgos asociados a las **nuevas tecnologías:** Como los asociados al uso de inteligencia artificial (por ejemplo, herramientas que producen fotografías falsas de desnudos que se ofrecen en chats de videojuegos), Internet de las cosas (por ejemplo, relojes inteligentes infantiles que permiten la geolocalización), al tratamiento de neurodatos (por ejemplo, para jugar a videojuegos o monitorizar la atención en clase) o la autenticación biométrica (por ejemplo, para pagar en los comedores de los colegios o para acceder a un evento deportivo).
    c. Riesgos asociados a la **salud mental y física:** Como los asociados a los patrones adictivos empleados por algunos servicios y aplicaciones o al tiempo excesivo de pantalla.

Una vez comprendidos los riesgos principales que sufre la infancia en Internet, se pueden realizar las siguientes afirmaciones, que se fundamentarán a lo largo de este documento:

- Las soluciones de verificación de edad, con el modelo adecuado, pueden ser de **gran ayuda** para evitar o mitigar gran parte de estos riesgos **desde el diseño y por defecto**.
- La selección del modelo adecuado para la verificación de edad, así como su diseño e implementación, deberían partir de una **evaluación de impacto para los derechos de la infancia** (Child Rights Impact Assessment o CRIA[6]). La gestión de los riesgos para la infancia en Internet no debe realizarse a ciegas ni de una manera rígida o estándar, sino tras una **evaluación sistemática y específica las cinco categorías de riesgos** ya mencionadas en el caso de una aplicación o servicio concreta, tanto por su **funcionalidad** como por su **público objetivo**, **contexto de uso**, etc.
- La verificación de edad puede emplear, para gestionar todos estos riesgos, el **enfoque habilitador** que comprueba que el usuario supera el umbral de edad

[5] Artículo 7 del RGPD y de la LOPDGDD.
[6] "CHILD RIGHTS IMPACT ASSESSMENTS IN RELATION TO THE DIGITAL ENVIRONMENT: DEVELOPING GLOBAL GUIDANCE", UNESCO, April 2024. https://www.unicef.org/reports/CRIA-responsibletech

requerido para realizar cambios en la configuración, permitir acceso a la comunicación con terceros, instalar aplicaciones para adultos, etc.

- Esto permite gestionar los riesgos de manera **proactiva**, y devolver a familiares y tutores la capacidad de ejercer su deber de cuidado y el resto de sus obligaciones.
- La verificación de edad n**o necesita verificar una edad concreta ni una fecha de nacimiento**, sólo la superación de dicho umbral. Umbral que puede ser distinto en función del tipo de actividad o elemento al que se desea acceder en Internet.
- La verificación de edad resulta inútil si **todo el ecosistema** (aplicaciones, herramientas, interfaces, etc.) no se adapta para la **protección del menor por defecto** y para comprobar que los usuarios que realizan ciertas solicitudes tienen la edad requerida para ello de forma que se garantice el anonimato, la no trazabilidad y que no se detecta a NNA.

El resto de la presente nota técnica analiza los cuatro casos de uso más extendidos en la actualidad tal y como se describen en la tabla 1, para concluir con una discusión sobre los principios que deben aplicar en relación con la privacidad y la protección de datos para que garanticen, no sólo la defensa del interés superior del menor, sino también los derechos y libertades de todos los ciudadanos y que no se generen nuevos riesgos sistémicos.

| **Caso de uso analizado** | **Riesgos que incluye y que pueden evitarse o mitigarse mediante la verificación de edad** |
|---|---|
| 1.Protección ante contenidos inadecuados | Contenido |
| 2.Entornos seguros para menores | Contenido+Conducta+Contacto+Corte transversal |
| 3.Consentimiento en línea para el tratamiento de datos personales | Consumo (contrato o consentimiento) |
| 4.Diseño adecuado para la edad | Conducta+Consumo (contrato o consentimiento)+ Corte transversal |

*Tabla 1. Casos de uso analizados en la presente nota técnica*

Como se analizará en las siguientes secciones de esta nota, la verificación de edad es una herramienta esencial para evitar o mitigar gran parte de estos riesgos, pero no es la única en ningún caso, deberá integrarse y complementarse con otro tipo de herramientas, soluciones y procesos (figura 1) en un sistema de protección del menor.


*Figura 1. Relación de la verificación de edad con otras soluciones en los diferentes casos de uso*

## IV. MODELOS PARA LA VERIFICACIÓN DE EDAD

Para que la verificación de edad se lleve a cabo de manera correcta una de las decisiones fundamentales que deben tomarse es la relativa a su **temporización**. Y es que la verificación de edad puede realizarse **en diferentes momentos** de la interacción de un usuario con los servicios y aplicaciones, de manera además que pueden realizarla diferentes actores. Los actores que realicen la verificación de edad pueden hacerlo con sus propias soluciones o confiando en soluciones ofrecidas por terceros de confianza, en este documento no se discuten las diferentes arquitecturas ni métodos posibles para hacerlo.

Hay un principio de diseño que debe cumplirse, en cualquier caso: se debe realizar la verificación de edad en el marco del acceso a un servicio o aplicación **antes de realizar cualquier otro tratamiento de datos personales**. Es decir, no se deben recoger datos personales de un usuario para, a continuación, denegarle el acceso porque no cumple con los requisitos de edad.

Por lo demás, se pueden distinguir dos modelos diferentes.

### A. SERVICIOS Y APLICACIONES PARA ADULTOS


*Figura 2. Verificación de edad en servicios y aplicaciones para adultos*

Todos los usuarios son adultos, en ningún caso NNA, que no deben poder acceder dada su naturaleza y los riesgos que esta implica para ellos.

**¿Quién debe aplicar la verificación de edad?** Si se trata de una *app*, el *store* correspondiente, que debería verificar que el usuario que desea descargarse e instalarse la app supera el umbral de edad requerido (normalmente +18). Ya que existen otros medios para descargar e instalar aplicaciones, también podría ser el proveedor del servicio al que se accede a través de la *app* el que realizara las comprobaciones oportunas, por ejemplo, la

primera vez que se realiza un acceso. Si se trata de un servicio que puede ser accedido a través de un navegador web, es el proveedor del servicio quien debería comprobar si el usuario supera el umbral de edad requerido antes de crear una cuenta o de realizar un acceso aislado. El navegador debería proporcionar todo el soporte necesario para realizar esta comprobación de manera adecuada.

**¿Cuándo se realiza la verificación de edad?** La verificación de edad es, en este modelo, el habilitador de entrada para el uso del servicio o de la aplicación: para poder comenzar a usarlo, se debe demostrar que se supera la edad requerida. Este proceso debería realizarse como mínimo una vez, en el *store* o ante el proveedor, para poder descargar la *app* o crear la cuenta.

**¿Se debe realizar refresco en algún momento?** La respuesta a esta pregunta depende del balance correcto entre distintos factores: el riesgo de inferencia de la condición de menor de los usuarios, el riesgo que el acceso a contenido inadecuado supone para NNA, el riesgo de manipulación de los procedimientos de verificación de edad o la usabilidad.

Como ya se ha mencionado, la verificación de edad debería realizarse siempre al menos una vez, para descargar la *app* o para abrir la cuenta. Después podría repetirse cuando se produzcan determinados eventos, por ejemplo, eventos del dispositivo como reinicios o cambios de la SIM, cambios en funcionalidades o términos de servicio que puedan afectar a los requisitos de edad, modificaciones en la información de la cuenta de usuario como el email, por ejemplo (para evitar el traspaso de cuentas entre usuarios), etc. Si el servicio permite realizar accesos como invitado, sin necesidad de crear una cuenta, se debería realizar verificación de edad en cada sesión.

**Ejemplo de buena práctica 1**

Una aplicación para móvil de citas y contactos es adecuada sólo para adultos, hay que tener 18 años o más para poder instalarla.

Las *store* oficiales de *apps* se encargan de realizar la verificación de edad antes de permitir al usuario descargar e instalar esta *app*.

Realizan la verificación de nuevo en cada actualización de la *app*.

**Ejemplo de buena práctica 2**

Una página web de contenidos pornográficos es sólo para adultos, hay que tener 18 años o más para poder crearse una cuenta y poder acceder a los contenidos que ofrece.

El proveedor de la página se encarga de realizar la verificación de edad antes de permitir al usuario crearse su cuenta.

Realiza la verificación de nuevo en cada actualización de la información asociada a esta cuenta de usuario: nombre de usuario o dirección de email.

**Ejemplo de mala práctica 1**

Una página web de apuestas es sólo para adultos, hay que tener 18 años o más para poder realizar apuestas. No se ofrece en ella ningún otro tipo de contenido o servicio.

El proveedor de la página permite a todos los usuarios crearse una cuenta, por lo que realiza el tratamiento de datos personales asociado a esta creación para todos ellos, sin realizar ninguna comprobación acerca de su edad. No realiza la verificación de edad hasta el momento en el que el usuario intenta realizar una apuesta.

Los datos personales de los usuarios por debajo de 18 años se tratan en el momento de creación de la cuenta de manera completamente innecesaria, ya que luego no se les permite acceder al servicio para el que se habían creado dicha cuenta. El error está en la mala decisión de diseño en cuanto al momento en el que se debe realizar la verificación de edad.

**Ejemplo de mala práctica 2**

Una página web de contenidos generalistas es para todos los públicos. No se ofrece en ella ningún otro tipo de contenido o servicio que se pueda catalogar “para adultos” y no se solicitan consentimientos para el tratamiento de datos personales.

Sin embargo, el proveedor decide realizar verificación de edad a todos sus usuarios para recoger nuevos datos (como mínimo, la edad) y poder personalizar contenidos, publicidad, etc. en función del rango de edad al que pertenecen. De nuevo se trata de un tratamiento de datos personales que no es necesario, tampoco es proporcional. El error está en la mala decisión de diseño en cuanto a la realización de verificación de edad en un sitio para todos los públicos que no implica riesgos significativos específicos para los NNA.

### B. SERVICIOS Y APLICACIONES PARA TODOS LOS PÚBLICOS O MIXTAS

En este caso, los usuarios pueden ser tanto NNA como adultos. Algunos contenidos, funcionalidades o configuraciones se consideran aptos para todos los usuarios mientras que otros se consideran inapropiados para la infancia por los riesgos que pueden suponer y deben estar protegidos por verificaciones de edad.

En este caso existen dos alternativas de diseño.

### 1. El proveedor ofrece dos versiones del servicio o aplicación (separación por edad)

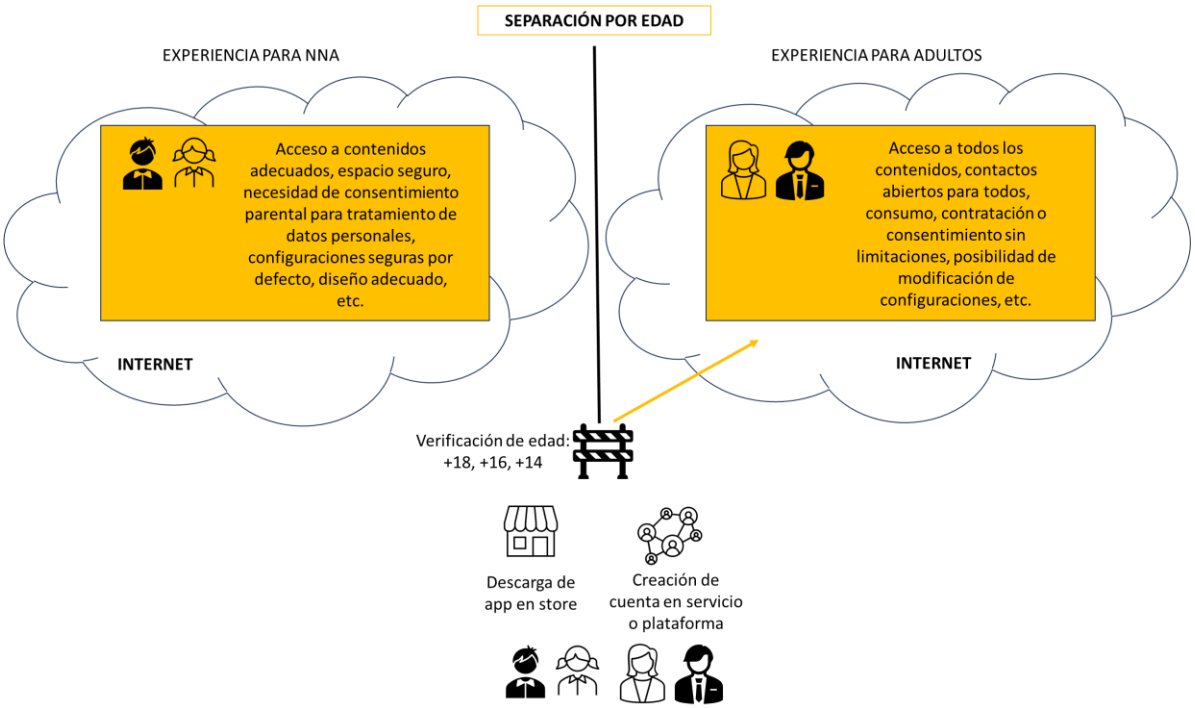


*Figura 3. Verificación de edad en servicios y aplicaciones para todos los públicos con separación por edad*

El proveedor ofrece dos experiencias diferentes en su servicio o aplicación. Una de las versiones implica protección por defecto para todos los usuarios de manera que sólo permite acceder a contenidos, funcionalidades, configuraciones y elementos seguros o para todos los públicos, sin restricciones de edad. La otra no implica este tipo de protección por defecto y el usuario la utiliza a pesar de los riesgos que puede implicar. Para ello, debe superar un umbral de edad y demostrarlo.

**¿Quién debe aplicar la verificación de edad?** Si se trata de una *app*, el *store* correspondiente debería verificar que el usuario que desea descargarse e instalarse la versión sin protección por defecto de la *app* supera el umbral de edad requerido (normalmente +18). Si el *store* no está preparado para realizar este tipo de verificación de edad, el proveedor de la *app* podría ofrecer una única versión para que se descarguen todos los usuarios, la que ofrece protección por defecto. Una vez descargada, incorpora una opción de configuración para la que es necesario verificar edad ante el proveedor de la *app*, que deshabilita todas las protecciones de manera global. Esto convierte a la *app* en la versión que no ofrece protección por defecto tras un único proceso de verificación de edad.

Si se trata de un servicio que puede ser accedido a través de un navegador web, el proveedor del servicio debería comprobar antes de crear una cuenta sin protección por defecto que el usuario supera el umbral de edad requerido, con el soporte proporcionado por el navegador.

En cualquier caso, si el usuario no puede demostrar que supera la edad requerida, o bien ante el *store* o bien ante el proveedor, podrá acceder a la *app* o a la cuenta, pero siempre con protección por defecto.

**¿Cuándo se realiza la verificación de edad?** Como ocurría en el modelo 1, la verificación de edad es el habilitador de entrada al uso del servicio o aplicación, en este caso

en su versión sin protección por defecto. Lo habitual es que este proceso se realice, como mínimo una vez, en el store o ante el proveedor.

**¿Se debe realizar refresco en algún momento?** Igual que en el Modelo 1.

**Ejemplo de buena práctica 3**

Una red social decide ofrecer dos versiones diferentes de su aplicación. La primera implica protección por defecto para todos los usuarios, por lo que puede ser utilizada por NNA sin que suponga un riesgo para ellos: no permite el acceso a contenidos con requisitos de edad, limita las opciones de contacto con otros usuarios (por ejemplo, mediante listas blancas), no realiza tratamiento de datos personales, lleva configuradas por defecto todas las opciones seguras, etc. La otra versión de la aplicación no incorpora estas protecciones por defecto, por lo que implica un riesgo que sólo puede ser asumido por adultos.

La versión con protección por defecto se la pueden instalar todos los usuarios sin necesidad de ninguna verificación de edad. Las *store* oficiales de *apps* se encargan de realizar la verificación de edad antes de permitir al usuario descargar e instalar la versión que no realiza protección por defecto.

Realizan la verificación de nuevo en cada actualización de la aplicación a una nueva versión.

**Ejemplo de buena práctica 4**

Un servicio de transmisión de vídeo en directo decide ofrecer cuentas con protección por defecto y cuentas sólo para adultos. Las cuentas con protección por defecto no permiten el acceso a transmisiones de otros usuarios con restricciones de edad, limitan las opciones de contacto con otros usuarios (por ejemplo, mediante listas blancas de contactos o interlocutores), no realizan tratamiento de datos personales, no permiten monetizar los contenidos compartidos, llevan configuradas por defecto todas las opciones seguras, etc. Todas estas protecciones no se ofrecen por defecto en las cuentas sólo para adultos.

La creación de cuentas con protección por defecto no necesita ninguna verificación de edad. El proveedor del servicio se encarga de realizar la verificación de edad antes de permitir al usuario crearse su cuenta sólo para adultos.

Realiza la verificación de nuevo una vez al mes, de manera periódica.

**Ejemplo de mala práctica 3**

Una red social decide ofrecer cuentas infantiles y cuentas de adultos. Las cuentas infantiles implican perfiles privados por defecto, no permiten el acceso a contenidos inapropiados para la infancia, limitan las opciones de contacto con otros usuarios (por ejemplo, mediante listas blancas de contactos o interlocutores), no realizan tratamiento

de datos personales, no permiten monetizar los contenidos compartidos, llevan configuradas por defecto todas las opciones seguras, etc. Todas estas protecciones no se ofrecen de manera predeterminada en las cuentas para adultos.

La creación de cuentas para adultos no necesita ninguna verificación de edad, pero la de cuentas infantiles sí. El proveedor de la red social se encarga de realizar la verificación de edad antes de permitir al usuario crearse su cuenta infantil.

Esto implica un riesgo de detección y localización de NNA (por parte de un proveedor malicioso, de empleados deshonestos, de terceros que acceden a los datos de manera no autorizada tras una brecha de datos, etc.) y hace que el tratamiento no sea proporcional.

El error está en obligar a los NNA a verificar su edad, la cuenta por defecto debe ser, siempre, la que es segura por defecto para todos los usuarios. La verificación de edad debe ir orientada a comprobar que el usuario dispuesto a correr un riesgo determinado tiene la edad requerida para hacerlo, es un proceso habilitador para ello.

**2. El proveedor ofrece un único servicio o aplicación con protección por defecto para todos los usuarios**

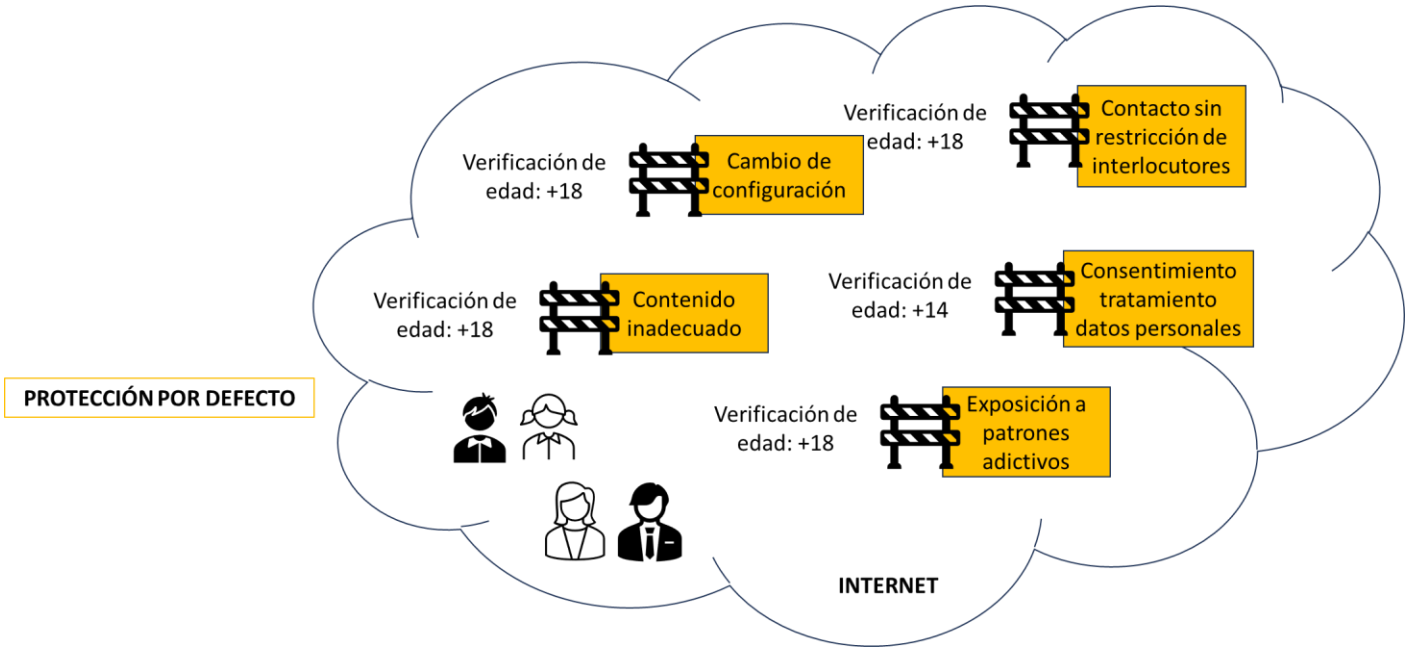


*Figura 4. Verificación de edad en servicios y aplicaciones para todos los públicos con protección por defecto*

En ocasiones la interacción del usuario con el servicio es puntual, anónima, no implica realizar ningún tipo de descarga o crear una cuenta, etc. En este caso, la versión 1 de este modelo de verificación de edad no es posible y no se pueden separar las experiencias de los usuarios por edades. Entonces se deberán realizar verificaciones de edad específicas en momentos concretos de dicha interacción.

**¿Quién debe aplicar la verificación de edad?** La única versión que se ofrece el servicio o aplicación debería garantizar protección por defecto para todos los usuarios. Cuando un usuario decida que quiere tener acceso a los contenidos, funcionalidades o configuraciones con restricciones de edad por los riesgos que supone, el proveedor debería comprobar, de manera específica para esa petición, que el usuario supera el umbral de edad requerido. Y debería hacerlo con cada petición de contenido, funcionalidad o configuración que, por el riesgo que supone, exige superar un umbral de edad.

**¿Cuándo se realiza la verificación de edad?** En este caso es probable que la verificación de edad se realice con una frecuencia mayor, cada vez que el usuario desee acceder a un contenido, funcionalidad o configuración para adultos. Y quien realiza la verificación es siempre el proveedor del servicio o de la aplicación, ya que en las *store* se descarga siempre la misma versión de la *app* (la única disponible, con protección por defecto para todos) sea cual sea la edad del usuario.

**¿Se debe realizar refresco en algún momento?** En principio se debería realizar una verificación de edad cada vez que un usuario solicitara un contenido, funcionalidad o configuración con restricciones por edad. Si se quiere evitar esto, se podrían implementar verificaciones "reutilizables", asociando de alguna forma la verificación de edad al dispositivo en el caso de *apps* o integrándola con la gestión de sesión del usuario en el caso de servicios. De esta forma, si el usuario ha verificado ser mayor de 18 para acceder a un contenido para adultos, se puede evitar que tenga que volver a realizar esta verificación para ver otro contenido para adultos justo a continuación, en el mismo dispositivo o durante la misma sesión. Pero se trata de decisiones de diseño muy específicas de cada proveedor.

**Ejemplo de buena práctica 5**

Una *app* de comunicación y mensajería ofrece en las *store* una única versión para todos los usuarios. Todos los usuarios se pueden descargar e instalar esta *app* sin necesidad de realizar una verificación de edad.

La *app* incorpora configuraciones seguras por defecto (no se muestra información de usuario, no se comparte ubicación, no se tratan datos personales, se limita la accesibilidad a la lista de contactos y no se muestran mensajes de otros usuarios que no han sido aprobados previamente de manera explícita, etc.). Si un usuario desea modificar cualquiera de estas configuraciones tiene que demostrar, cada vez, mediante un proceso de verificación de edad realizado por el proveedor de la *app,* que tiene la edad necesaria para hacerlo. Por ejemplo, tendrá que hacerlo para poder recibir mensajes de cualquier usuario o para comenzar a compartir la ubicación.

**Ejemplo de buena práctica 6**

Una plataforma de comercio electrónico no realiza, en principio, distinción entre usuarios en función de su edad. Todos los usuarios pueden navegar por su web y realizar compras sin necesidad tener cuenta, como invitados.

Pero realiza un proceso de verificación de edad antes de mostrar información sobre productos que no son adecuados para NNA, como el tabaco o el alcohol.

Si un usuario demuestra tener la edad adecuada para acceder a la información de este tipo de productos, se asocia esta información a su *cookie* de sesión, de manera que durante toda la sesión no es necesario volver a realizar una verificación de edad. Cada plataforma podría configurar la duración de las sesiones según sus necesidades específicas.

**Ejemplo de mala práctica 4**

Una plataforma de vídeo juegos ofrece una única versión de cuenta para todos los usuarios, sin necesidad de realizar una verificación de edad.

Se pueden bloquear configuraciones seguras por defecto (no se muestra información de usuario, no se comparte ubicación, no se tratan datos personales, se limitan los contactos y no se muestran mensajes de otros usuarios que no han sido aprobados previamente de manera explícita, se limita el acceso a vídeo juegos con contenidos no apropiados, etc.) para una cuenta concreta si se verifica que es para un NNA. Lo pueden hacer los propios NNA o sus padres o tutores, en el ejercicio de su deber de cuidado.

Esto implica un riesgo de detección y localización para los NNA y hace que el tratamiento de datos personales involucrado en la verificación de edad no sea proporcional. El error está en obligar a los NNA a verificar su edad para estar protegidos, cuando la opción segura debería ser siempre la opción por defecto: siempre se debe verificar que el usuario supera el umbral de edad requerido para realizar una actividad que implica un riesgo para los NNA (la verificación de edad es un habilitador), y no al contrario.

# V. CASO DE USO 1: PROTECCIÓN ANTE CONTENIDOS INADECUADOS

## A. MARCO PRELIMINAR

El acceso incontrolado a contenidos inadecuados por parte de NNA es una de las **principales preocupaciones** de padres y educadores en la actualidad. Por este motivo diferentes agentes están trabajando en proteger a los menores de estos contenidos sin arriesgar su integridad física o seguridad y sin someterlos a vigilancia o seguimiento. Ni tampoco al resto de usuarios de Internet, ya que **todos los contenidos han de ser libremente accesibles para aquellas personas que pueden demostrar que superan el umbral de edad** establecido respetando sus derechos fundamentales y libertades.

La Agencia Española de Protección de Datos publicó en diciembre del 2023 diferentes materiales en relación con su proyecto relativo a este caso de uso. En concreto, una Infografía con las amenazas y los riesgos para los derechos y libertades asociados a los sistemas de verificación de edad en este caso de uso y un Decálogo de Principios que deben cumplir los sistemas de verificación de edad cuando se emplean en la protección de personas menores de edad ante contenidos inadecuados. Otras autoridades de control europeas de protección de datos (CNIL[7], Garante per la protezioni dei dati personali[8]) así como los reguladores del mercado audiovisual (Arcom[9], Agcom[10]) han publicado también sus propuestas y conclusiones recientemente. Además, la Comisión Europea está trabajando en ofrecer una **solución armonizada** en los estados miembro con diferentes iniciativas[11],[12],[13].

## B. FUNDAMENTOS JURÍDICOS

En la siguiente regulación europea y nacional se recoge la necesidad de proteger a la infancia ante contenidos inadecuados, señalando en algunos casos como los más nocivos aquellos que muestran violencia gratuita o pornografía.

| | |
|---|---|
| **RGPD**<br><br>**considerando 38** | Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. |

[7] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
[8] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9965235
[9] https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne
[10] https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5lVOIXoE_assetEntryId=33778802&_101_INSTANCE_FnOw5lVOIXoE_type=document
[11] Better Internet for Kids: https://www.betterinternetforkids.eu/
[12] Digital Services Act: Task Force on Age Verification: https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0
[13] European Board for Digital Services: https://digital-strategy.ec.europa.eu/en/policies/dsa-board

| | |
|---|---|
| **RGPD**<br><br>**considerando 75** | Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo;…; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados. |
| **Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual**<br><br>**artículo 88** | Los prestadores del servicio de intercambio de vídeos a través de plataforma adoptarán medidas para proteger:<br><br>a) A los menores de los programas, de los vídeos generados por usuarios y de las comunicaciones comerciales audiovisuales que puedan perjudicar su desarrollo físico, mental o moral. |
| **Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual**<br><br>**artículo 89** | 1. Los prestadores del servicio de intercambio de vídeos a través de plataforma, para proteger a los menores y al público en general de los contenidos audiovisuales indicados en el artículo anterior, tomarán las siguientes medidas:<br><br>a) Incluir y poner en práctica en las cláusulas de condiciones del servicio de las plataformas de intercambio de vídeos las obligaciones establecidas en el artículo 88 sobre determinados contenidos audiovisuales.<br><br>b) Establecer y operar mecanismos transparentes y de fácil uso que permitan a los usuarios notificar o indicar al correspondiente prestador los contenidos que vulneren las obligaciones establecidas en el artículo 88.<br><br>c) Establecer y operar sistemas a través de los cuales los prestadores del servicio expliquen a los usuarios el curso que se ha dado a las notificaciones o indicaciones a que se refiere la letra anterior.<br><br>d) Establecer y aplicar sistemas de fácil uso que permitan a los usuarios del servicio calificar los contenidos que puedan vulnerar las obligaciones establecidas en el artículo 88.<br><br>e) Establecer y operar sistemas de verificación de edad para los usuarios con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores que, en todo caso, impidan el acceso de estos a los contenidos audiovisuales más nocivos, como la violencia gratuita o la pornografía.<br><br>f) Facilitar sistemas de control parental controlados por el usuario final con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de los menores.<br><br>g) Establecer y aplicar procedimientos transparentes, eficaces y de fácil uso para el tratamiento y la resolución de las reclamaciones de los |

| | |
|---|---|
| | usuarios a los prestadores del servicio, en relación con la aplicación de las medidas a que se refieren las letras anteriores.<br><br>h) Facilitar medidas y herramientas eficaces de alfabetización mediática y poner en conocimiento de los usuarios la existencia de esas medidas y herramientas.<br><br>i) Facilitar que los usuarios, ante una reclamación presentada por ellos y no resuelta satisfactoriamente, puedan someter el conflicto a un procedimiento de resolución alternativa de litigios de consumo, de acuerdo con lo previsto en la Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo. Todo ello sin perjuicio de que los usuarios puedan acudir a la vía judicial que corresponda. |

## C. UNA PRIMERA APROXIMACIÓN

El enfoque que permite resolver este caso de uso protegiendo el interés superior del menor y los derechos y libertades de todos los usuarios es el que se basa en **verificar, siempre que se realice un acceso a un contenido con restricción de edad, que el usuario supera la edad requerida para realizar dicho acceso**. Cuando un usuario no pueda probar que supera la edad requerida, el contenido deberá filtrarse o el acceso a él bloquearse con el método escogido, fuera del alcance de esta nota técnica.

En el caso de **servicios o aplicaciones para adultos** que obligan a verificar que el usuario es mayor de 18 años, ya se sabe que dicho usuario tiene la edad adecuada para acceder a cualquier contenido que se le pueda ofrecer. Es decir, se trata del modelo A de la sección IV de este documento.

En el caso de **servicios o aplicaciones para todos los públicos o audiencias** porque ofrecen contenidos híbridos o mixtos (algunos con restricciones de edad, otros no), se pueden dar dos escenarios, los explicados en los modelos B.1 y B.2 de la misma sección IV.

Conviene recordar que **las soluciones de verificación de edad resuelven una parte del problema** de la protección de la infancia, pero que será necesario complementarlas con otras como las de **bloqueo o filtrado de contenidos** (mientras no se verifique la edad del usuario) o las de **etiquetado de servicios, aplicaciones, sitios o contenidos** (para clasificar en función del umbral edad desde el punto de vista tecnológico) para que el propósito de proteger al menor se cumpla por completo. En este sentido, la **modificación o adaptación** de las *stores* de aplicaciones, de las *apps* de acceso a contenidos o de los navegadores actuales puede ser de gran ayuda para la integración de todos los elementos necesarios.

## D. EQUÍVOCOS

Es habitual encontrarse con proveedores que gestionan la verificación de edad como si su fin último fuera el conocimiento de la edad específica de todos los usuarios o el

conocimiento de qué usuarios en concreto son NNA. Pero esto no es así, en este caso de uso **el objetivo es proteger al menor** ante contenidos inadecuados. Y este objetivo se puede cumplir **sin conocer la edad exacta de los usuarios y sin someter a los NNA a procesos de verificación**. Con el **enfoque habilitador** de la verificación de edad, son los adultos los que prueban que "superan el umbral de edad requerido" para acceder a los servicios, versiones adultas de las *apps* o contenidos específicos. Los NNA están así **protegidos por defecto**, sin necesidad de instalar aplicaciones o herramientas adicionales, de que el NNA tenga que entender una información proporcionada por el proveedor ni de someterse a nuevos tratamientos de datos. Y, en resumen, **de manera proactiva y sin necesidad de correr nuevos riesgos**. Para ello es fundamental, no solo un proceso de verificación de edad como se ha señalado anteriormente, sino que los propios servicios y aplicaciones implementen dicha protección por defecto.

También es frecuente cometer el error de pensar que para cualquier solución que se proponga para proteger a los menores van a surgir **métodos de elusión o burla** y que, por este motivo, no se debería desplegar ningún tipo de sistema de protección. Por ejemplo, es habitual escuchar el argumento según el cual no merece la pena el esfuerzo porque los NNA aprenderán a usar VPNs (*Virtual Private Networks*) para acceder a los contenidos inadecuados o terminarán por usar la prueba de edad o credencial de un mayor, o incluso falsificada.

En primer lugar, esto es un error porque la tecnología actual permite diseñar y desarrollar soluciones que hagan muy complicado sortearlas[14] (aunque no imposible, como ocurre con otro tipo de protecciones en otros dominios de aplicación). En segundo lugar, porque ese mismo argumento aplicaría a multitud de protecciones para la infancia en otros contextos y, sin embargo, la sociedad entiende que **los esfuerzos** realizados para proteger a la mayor parte de NNA en la mayor parte de los casos **implementan una protección que alcanza a un alto porcentaje de NNA y es obligatorio** realizarlos.

[14] Por ejemplo, si el filtrado de contenidos se realiza de manera local por parte de los navegadores o de las aplicaciones de acceso a contenidos instaladas en el propio dispositivo, sortear los mecanismos de protección es mucho más complicado, sobre todo cuando la edad de los NNA es baja.

# VI. CASO DE USO 2: ENTORNOS SEGUROS PARA LA INFANCIA

## A. MARCO PRELIMINAR

Diferentes participantes en el ecosistema de Internet están trabajando para crear entornos seguros para la infancia. **No existe una definición universal, concreta y ampliamente aceptada** de lo que implica un entorno o espacio seguro para la infancia en Internet, ni de los requisitos que debe cumplir o de sus propiedades deseables. Desafortunadamente esto lleva a equívocos importantes que pueden aprovecharse por diferentes actores de manera interesada.

En la actualidad hay un enfoque bastante extendido que suele asociarse con este concepto del entorno seguro: los entornos son los mismos para todos los usuarios, **los menores serán identificados y, por defecto, también los mayores**, ambos serán **vigilados** en sus acciones para que, cuando se evidencie la **exposición a un riesgo** por parte de un menor, por ejemplo, las 5Cs mencionadas en la sección de Introducción de este documento, se tomen **acciones correctivas**. Todo ello bajo **el criterio, la supervisión y la vigilancia** de todas las acciones de los sujetos por parte de unos **actores de Internet** cuyos intereses legítimos, dado su modelo de negocio actual, pueden colisionar directamente con la protección de los derechos fundamentales de toda la ciudadanía. Además, mediante el uso de herramientas diseñadas para que las familias, los educadores, los reguladores o las autoridades **no puedan ejercer de forma efectiva sus diferentes obligaciones**.

Por norma general este **planteamiento equivocado del entorno seguro** se basa en saber quién es NNA y en muchos casos, en conocer su edad concreta. No sólo en la recogida de dicha edad concreta de los usuarios (o de su rango de edad), sino en su **perfilado**, menores incluidos. En este último caso, para “mejorar la experiencia del usuario” y que los servicios o aplicaciones resulten más atractivos o usables para usuarios en distintos rangos de edades.

La comercialización de un servicio o aplicación etiquetados así como “entorno seguro” puede, en el peor de los casos, permitir a **actores maliciosos** atraer, detectar o localizar NNA. Es decir, este tipo de entornos pueden producir el efecto “pescar en una pecera”. La detección y la localización no implican solamente conocer que una cuenta determinada pertenece a un NNA, sino poder asociarle una identidad en el mundo real, una dirección física (geolocalización) o digital y tener acceso a él o ella para personalizar mensajes, ofertas, etc. Incluso con la mejor voluntad del proveedor del servicio o de la aplicación, siempre existe la posibilidad de que un miembro de la entidad la **utilice de manera ilegítima** o que exista una **brecha de datos personales** que exponga al NNA ante terceros.

Sin embargo, la creación de un entorno seguro debería **perseguir, desde el diseño, la mitigación de las amenazas concretas** que pueden generarse sobre los derechos fundamentales del menor y de todos los usuarios de Internet. Para crear un espacio seguro **no basta con acumular protecciones genéricas**, sino que éstas deben ser adecuadas para las amenazas concretas identificadas. Las medidas o herramientas para crear entornos seguros deben solucionar problemas concretos y **no generar nuevas vulnerabilidades** incluso más graves. Para ello se debe tener una visión global de las medidas adoptadas, que protejan *a priori* a los NNA, y de cómo interaccionan entre ellas.

Los entornos seguros lo deben ser desde el diseño. Para ello, **no es suficiente incluir una capa de seguridad adicional** sobre la infraestructura ya existente, sino que todos los actores tienen que evolucionar para incorporar desde el diseño las propiedades que convierten a los entornos en seguros. Como ya se ha mencionado en el caso de uso anterior, por ejemplo, las *stores* de aplicaciones, las propias *apps* o los navegadores. El ecosistema de Internet **no puede tratarse como un conjunto de islas independientes**. Para ello es

necesario, no solo una **cooperación** entre los intervinientes a la hora de diseñar sus soluciones, sino también una **comunicación efectiva** entre ellos ante la identificación de nuevas amenazas para la seguridad del menor a través de un **marco de gobernanza adecuado.**

Las medidas que protejan al menor han de permitir a quien tiene el deber de su cuidado ejercer sus obligaciones. Y es que **las diferentes obligaciones asociadas a la creación de** entornos seguros para menores en Internet **no son delegables ni debes basarse en actos de fe**, sobre todo, en actores de Internet cuyos intereses son la monetización de usuarios y la fidelización, si no adicción, a sus servicios y aplicaciones. Además, han de poder ejercerlas **por defecto**, es decir, que el desconocimiento por parte de los que tienen el deber de cuidar a los NNA de cómo funcionan ciertas medidas o herramientas no suponga un obstáculo importante para la protección de dichos NNA.

La protección de los derechos fundamentales no sólo se aplica al menor, sino que implica **la protección de los derechos de todos los usuarios de Internet**, en particular, el derecho a obrar física y virtualmente, a la no discriminación, a la libertad de educación, información, pensamiento, creencias, a la privacidad y la intimidad, etc., pero, sobre todo, hay que tener en cuenta la protección de la integridad física. Hay que recordar que **los NNA no son el único colectivo en situación de vulnerabilidad** por determinadas prácticas de los proveedores de servicios y aplicaciones digitales.

## B. FUNDAMENTOS JURÍDICOS

Como ya se ha comentado con anterioridad, no existe una definición de lo que es run entorno seguro para menores en Internet. Pero diferentes marcos regulatorios recogen, desde diferentes puntos de vista, la protección que los menores deben recibir en diferentes contextos. De hecho, son los mismos analizados en el caso de uso 1, ya que este número 2 se puede considerar una extensión del 1 que tiene en cuenta otros riesgos adicionales a los producidos exclusivamente por el acceso a contenidos. Adicionalmente se pueden tener en cuenta los siguientes.

| | |
|---|---|
| **DSA**<br><br>**considerando 71** | ... Puede considerarse que una plataforma en línea es accesible para los menores cuando sus condiciones generales permiten a los menores utilizar el servicio, cuando su servicio está dirigido a menores o es utilizado predominantemente por ellos, o cuando el prestador es consciente de que algunos de los destinatarios de su servicio son menores, por ejemplo, porque ya trata para otros fines datos personales de los destinatarios de su servicio que revelan su edad.<br><br>Los prestadores de plataformas en línea utilizadas por menores deben adoptar medidas adecuadas y proporcionadas para proteger a los menores, por ejemplo, diseñando sus interfaces en línea o partes de estas con el máximo nivel de privacidad, seguridad y protección de los menores por defecto, cuando proceda, o adoptando normas para la protección de los menores, o participando en códigos de conducta para la protección de los menores.<br><br>…<br><br>Los prestadores de plataformas en línea no deben presentar anuncios basados en la elaboración de perfiles mediante la utilización de datos |

| | |
|---|---|
| | personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor.<br><br>De conformidad con el Reglamento (UE) 2016/679, en particular el principio de minimización de datos previsto en su artículo 5, apartado 1, letra c), esta prohibición no debe llevar al prestador de la plataforma en línea a mantener, obtener o tratar más datos personales de los que ya dispone para evaluar si el destinatario del servicio es un menor. Por lo tanto, esta obligación no debe incentivar a los prestadores de plataformas en línea a capturar la edad del destinatario del servicio antes de su uso. Esto debe aplicarse sin perjuicio del Derecho de la Unión en materia de protección de datos personales. |
| **DSA**<br><br>**artículo 35** | Reducción de riesgos<br>1. Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño aplicarán medidas de reducción de riesgos razonables, proporcionadas y efectivas, adaptadas a los riesgos sistémicos específicos detectados de conformidad con el artículo 34, teniendo especialmente en cuenta las consecuencias de dichas medidas sobre los derechos fundamentales. Dichas medidas podrán incluir, cuando proceda:<br>a) la adaptación del diseño, las características o el funcionamiento de sus servicios, incluidas sus interfaces en línea;<br>b) la adaptación de sus condiciones generales y su ejecución;<br>c) la adaptación de los procesos de moderación de contenidos, incluida la velocidad y la calidad del tratamiento de las notificaciones relacionadas con tipos específicos de contenidos ilícitos y, en su caso, la rápida retirada de los contenidos notificados, o el bloqueo del acceso a ellos, en particular en el caso de la incitación ilegal al odio o la ciberviolencia, así como la adaptación de los procesos de toma de decisiones pertinentes y los recursos específicos para la moderación de contenidos;<br>d) la realización de pruebas y la adaptación de sus sistemas algorítmicos, incluidos sus sistemas de recomendación;<br>e) la adaptación de sus sistemas publicitarios y la adopción de medidas específicas dirigidas a limitar o ajustar la presentación de anuncios publicitarios en asociación con el servicio que prestan;<br>f) el refuerzo de los procesos internos, los recursos, la realización de pruebas, la documentación o la supervisión de cualquiera de sus actividades, en particular en lo que respecta a la detección de riesgos sistémicos;<br>g) la puesta en marcha o el ajuste de la cooperación con los alertadores fiables de conformidad con el artículo 22 y la ejecución de las decisiones de los órganos de resolución extrajudicial de litigios en virtud del artículo 21;<br>h) la puesta en marcha o el ajuste de la cooperación con otros prestadores de plataformas en línea o motores de búsqueda en línea mediante los códigos de conducta y los protocolos de crisis a que se refieren, respectivamente, los artículos 45 y 48;<br>i) la adopción de medidas de concienciación y la adaptación de su interfaz en línea con el fin de proporcionar más información a los destinatarios del servicio; |

| | |
|---|---|
| | j) la adopción de medidas específicas para proteger los derechos de los menores, incluidas herramientas de comprobación de la edad y de control parental, herramientas destinadas a ayudar a los menores a señalar abusos u obtener ayuda, según corresponda;<br>k) garantizar que un elemento de información, ya se trate de imagen, audio o vídeo generado o manipulado que se asemeja notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puede inducir erróneamente a una persona a pensar que son auténticos o verídicos, se distinga mediante indicaciones destacadas cuando se presente en sus interfaces en línea y, además, proporcionar una funcionalidad fácil de utilizar que permita a los destinatarios del servicio señalar dicha información. |

## C. UNA PRIMERA APROXIMACIÓN

Crear entornos seguros para los NNA sin exigir la verificación de la edad a los propios NNA es un **reto complejo**, pero el **enfoque habilitador, proactivo y por defecto** ya mencionado puede ayudar enormemente a conseguirlo. El objetivo es **equilibrar la accesibilidad y la protección de los derechos y libertades fundamentales** (incluido el interés superior del menor y la privacidad) para garantizar que Internet sea un espacio de oportunidades para todas las edades.

En este caso de uso se debe **proteger a los NNA ante contenido** de odio, dañino o ilegal pero también ante **herramientas o funcionalidades** que los coloquen en una posición vulnerable por participar en conductas de odio, dañinas o ilegales, así como **de interacciones** con otros usuarios que les hagan objeto de mensajes de odio, dañinos, ilegales o problemáticos por otros motivos. También hay que protegerlos de riesgos de corte transversal que impliquen una **sobreexposición**, ciertos tratamientos de datos personales asociados a las **nuevas tecnologías** (inteligencia artificial, Internet de las cosas, neurodatos, autenticación biométrica). Y por supuesto de los patrones adictivos.

En el caso de **servicios o aplicaciones para adultos** (modelo A en la sección IV), **no es necesario** diseñar este tipo de entornos seguros para la infancia, ya que los NNA no son usuarios y no necesitan ser protegidos. Lo están, por defecto, por la verificación de edad necesaria para acceder a estas servicios y aplicaciones, que garantiza que se si se ha conseguido el acceso, se está por encima de 18 años.

En el caso de servicios o aplicaciones **para todos los públicos o audiencias**, hay dos formas de ofrecer entornos seguros para la infancia, los modelos B.1 y B.2 ya mencionados. El modelo B.1 es el que siguen, por ejemplo, muchas plataformas de *streaming*, que permiten la creación de cuentas con protección por defecto, que permite convertirlas en espacios seguros. Si un servicio o aplicación predice que puede tener usuarios de diferentes edades, puede ofrecer **experiencias diferentes** según la edad, incorporando la protección desde el diseño para los usuarios que no verifiquen edad. Esto puede conseguirse con cuentas sólo para adultos, *apps* diferentes para los adultos en las *stores* de los teléfonos, etc. La verificación de edad deben realizarla siempre los adultos, para demostrar que lo son cuando quieren abrirse una cuenta de adulto (se verifican ante el proveedor del servicio) o instalarse la versión de la *app* para adultos (se verifican en el store en el que descargan la *app*). De esta manera los NNA están protegidos por defecto, ya que sólo podrán acceder a las cuentas con protección por defecto.

En el resto de los casos, se aplica el modelo B.2 y se trata a todos los usuarios de la misma manera, sin que existan experiencias diferenciadas. El espacio seguro debe serlo por

defecto y desde el diseño para todos los potenciales usuarios, que pueden tener diferentes edades. **Los contenidos, funcionalidades y aspectos específicos con restricciones de edad solo deben ser accesibles cuando el usuario "supera el umbral de edad requerido**" porque un proceso de verificación de edad comprueba que su edad está por encima del umbral de edad requerido en cada caso. Ya se han proporcionado un par de ejemplos de buenas prácticas (el 5 y el 6) en la sección IV de esta nota. Las funcionalidades y configuraciones disponibles por defecto deben ser siempre las seguras, sin que se puedan modificar si no se realiza antes un proceso de verificación de edad.

En los dos escenarios anteriores, en los que sí se debe crear un entorno seguro para NNA, la verificación de edad podría ser complementada por algunas herramientas y procesos como son:

- **Restricción de interlocutores:** Se trata de métodos y herramientas específicos que permiten limitar la capacidad de interacción o comunicación de los NNA con otros usuarios, de manera que ésta se limite a los que aparecen en listas blancas o de contactos permitidos.
- **Participación de los padres y control parental:** En este caso a través de otras herramientas que les permitan supervisar y controlar la actividad de la cuenta de sus hijos sin revelar los datos personales del NNA, configurar búsquedas seguras o establecer filtros de contenido o lenguaje.
- **Educación a los NNA acerca de los riesgos en línea y del uso responsable de Internet**: Esto incluye reconocer comportamientos sospechosos y saber cómo denunciarlos en servicios y aplicaciones específicos.

Además, los gobiernos, las ONG, las asociaciones de padres y la industria deben colaborar, en un contexto de corregulación, para crear un entorno digital más seguro para los niños mediante **la identificación de riesgos (y la definición de metodologías para hacerlo), la compartición de las mejores prácticas para gestionarlos, la elaboración de códigos de conducta**, etc.

## D. Equívocos

Muchas propuestas actuales se basan en la restricción de interlocutores y el control parental ya mencionados, así como en otro tipo de herramientas que suelen incluir:

- **Moderación realizada por la comunidad:** Moderadores adultos de confianza (verificados a través de comprobaciones exhaustivas de antecedentes) pueden supervisar las interacciones para garantizar que sigan siendo apropiadas y amigables para los niños.
- **Moderación automatizada:** Se pueden establecer sistemas automatizados para detectar (antes de compartir) y eliminar (después de compartir) contenido inapropiado o comportamiento inadecuado para niños.
- **Métodos de denuncia entre pares:** Herramientas que permitan a los NNA denunciar comportamientos sospechosos que los moderadores adultos puedan revisar.
- **Análisis conductual:** Herramientas de análisis basadas en aprendizaje automático o inteligencia artificial que monitoricen los patrones de juego, el uso del lenguaje o los estilos de interacción para identificar y marcar el comportamiento (no a los usuarios) que es inconsistente con el de un NNA típico.

Pero estas herramientas, **por sí mismas, son insuficientes** para establecer un entorno seguro, ya que se basan en enfoques reactivos (el NNA ya ha sido expuesto al riesgo) y que

no protegen por defecto. Además, habría que analizar caso por caso si cumplen con la **regulación de protección de datos**, porque algunas de estas propuestas se basan en el tratamiento masivo de datos personales, el perfilado de los usuarios. En ocasiones, en decisiones automatizadas que pueden generar serios efectos jurídicos, y que además son propensas a sesgos. En resumen, que pueden vulnerar derechos y libertades de todos los usuarios.

En este caso de uso, además, hay un equívoco muy extendido según el cual **un entorno seguro lo es por el mero hecho de permitir solamente el acceso a usuarios que sean NNA**. En este caso, el umbral de edad se interpreta a la inversa, ya que solo se "supera" cuando los usuarios están por debajo de dicho umbral. Ya se han explicado con anterioridad en esta nota los riesgos que implica basar la protección en conocer qué usuarios en concreto son NNA (cuentas infantiles o para adolescentes, por ejemplo).

Pero es que, además, suponer que un entorno es seguro por el hecho de que sólo se permite el acceso a NNA **es un error** ya que:

- Al igual que sucede en el mundo físico, **un sitio no es seguro solo porque solo se permite que accedan NNA**. Más bien al contrario, porque es muy probable que no cuenten con la madurez o experiencia suficientes para poder afrontar las situaciones de riesgo que surjan en ese contexto de tipo "corralito" o que ellos mismos generen.
- Este escenario **aumenta el riesgo de localizar a NNA (ya se ha mencionado el efecto de "pesca en pecera")** y de hacerles objetivo de fines comerciales o malintencionados (redes de pedofilia, etc.).
- El acceso a contenido inapropiado debería impedirse de forma predeterminada para los NNA, pero ¿qué impediría que fuera uno de ellos el que lo compartiera dentro de uno de estos espacios? Probablemente alguna de las herramientas de moderación o denuncia enumeradas antes, pero a posteriori, siguiendo un **enfoque reactivo que no evita la exposición al riesgo**.
- Las protecciones **no deben aplicarse después** de que el NNA ya haya estado expuesto al riesgo, de manera reactiva. Las protecciones deben aplicarse por adelantado, y de forma predeterminada, por defecto y desde el diseño. Sólo de esta manera se puede intentar evitar o minimizar el riesgo y su potencial impacto.
- La disponibilidad del NNA para que cualquier persona pueda acceder a él o ella a través de Internet debe ser **nula de forma predeterminada** para cualquier persona que no pertenezca a su entorno de confianza. No basta con confiar en que el resto de los usuarios son todos del mismo rango de edad.
    - Un NNA puede ser presionado o amenazado por un adulto, directa o indirectamente, para que se ponga en contacto con otros NNA.
    - La mezcla de NNA con edades muy diferentes podría implicar un riesgo. No deben ser tratados como un grupo homogéneo, ni se debe realizar una asociación directa entre edad y madurez o etapa de desarrollo.
- Las protecciones que podrían aplicarse son, en muchos casos, **proporcionadas por terceros ajenos al entorno de confianza del NNA**, por lo que esos mismos terceros son un riesgo.
    - Determinar el interés superior de un menor es una obligación de los padres y del resto de agentes ya mencionados en esta nota, no puede dejarse en manos de empresas tecnológicas con intereses comerciales legítimos.

Hay que tener en cuenta que **ningún marco normativo exige la creación de espacios seguros en los que todos los usuarios sean NNA**. Las recomendaciones para hacer de Internet un espacio seguro para la infancia, y que para ello sea sensible a la edad (*age-aware*), siempre pueden interpretarse en el otro sentido: solo los usuarios confirmados como

adultos pueden acceder a ciertos contenidos, pueden tener contacto con otros usuarios sin limitaciones, pueden estar expuestos a ciertas funcionalidades o tecnologías, o modificar ciertas configuraciones.

# VII. CASO DE USO 3: CONSENTIMIENTO EN LÍNEA PARA EL TRATAMIENTO DE DATOS PERSONALES

## A. MARCO PRELIMINAR

El actual marco regulatorio para la protección de datos **permite recabar y tratar datos personales de menores si se cumplen ciertas condiciones**. El consentimiento puede ser una de las bases legales que legitime estos tratamientos de datos personales (artículos 6.1 y 8 del RGPD, y 7 de la LOPDGDD) o una de las condiciones que pueden permitir levantar la prohibición de tratar categorías especiales de datos (artículo 9.2 del RGPD). En este contexto, el consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen, y en el caso de los menores de 14 años (en otros países europeos el límite de edad para el consentimiento puede ser otro, pero siempre **entre los 13 y los 16 años**), ese consentimiento tendrá que ser otorgado por aquellos que ostentan su patria potestad o tutela. Por lo tanto, la información para obtener dicho consentimiento no deberá estar adaptada al NNA, sino al adulto al que compete tomar las decisiones.

En España, los menores de entre 14 y 18 años podrán otorgar el consentimiento para la utilización de sus datos personales por sí mismos, salvo que una norma específica exija la asistencia de los padres o tutores (artículo 7.1 de la LOPDGDD[15]). Para ello, **el responsable del tratamiento debe hacer esfuerzos razonables para verificar** que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

**La regulación no especifica qué métodos o mecanismos** debe utilizar el responsable de un tratamiento para saber si el usuario de un servicio en línea o aplicación supera este límite de edad, ni tampoco cómo se debe recabar el consentimiento parental cuando éste es necesario o demostrar que se ha recabado con la debida diligencia.

## B. FUNDAMENTOS JURÍDICOS

Se recogen a continuación algunos aspectos esenciales en relación con el consentimiento para el tratamiento de datos personales en el caso de los NNA:

| | |
|---|---|
| **RGPD**<br>**considerando 38** | Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños. |

[15] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

| | |
|---|---|
| **EDPB Guidelines 05/2020 on consent sección 7.1** | La expresión «en particular» indica que la protección específica no se limita a la mercadotecnia o a la elaboración de perfiles, sino que incluye el ámbito más amplio de «obtención de datos personales relativos a niños». |
| **RGPD**<br>**considerando 58** | El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender. |
| **EDPB Guidelines 05/2020 on consent sección 7.1** | Tal y como se menciona en la sección 3.1 sobre el consentimiento informado, la información deberá ser comprensible para la audiencia a la que el responsable del tratamiento se dirija, teniendo especialmente en cuenta el caso de los niños. Con el fin de obtener el «consentimiento informado» de un niño, el responsable debe explicar en un lenguaje que sea claro y sencillo para los niños, de qué manera pretende tratar los datos que recoja61. Si es el progenitor quien debe dar el consentimiento, es posible que se requiera un conjunto de datos que permitan a los adultos tomar una decisión informada. |
| **RGPD**<br>**considerando 75** | Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, …. en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados. |
| **RGPD**<br>**artículo 8, Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información** | 1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.<br>Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. |

| | |
|---|---|
| | 2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.<br><br>3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño. |
| **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales**<br><br>**artículo 7, Consentimiento de los menores de edad** | 1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.<br><br>Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.<br><br>2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela. |
| **EDPB Guidelines 05/2020 on consent**<br><br>**sección 7.1** | Está claro, por lo antes mencionado, que el artículo 8 se aplicará únicamente cuando se cumplan las siguientes condiciones:<br><br>que el tratamiento de esté relacionado con servicios de la sociedad de la información ofrecidos directamente a los niños,<br><br>que el tratamiento se basa en el consentimiento.<br><br>…<br><br>El TJUE ha mantenido que servicios de la sociedad de la información incluye los contratos y otros servicios que se celebran o transmiten en línea.<br><br>…<br><br>si un proveedor de servicios de la sociedad de la información deja claro a sus posibles usuarios que únicamente ofrece sus servicios a personas de 18 o más, y ello no queda menoscabado por cualquier otro indicio (como el contenido del sitio o los planes de mercadotecnia) entonces no se considerará que dicho servicio sea «ofrecido directamente a un niño» y el artículo 8 no será de aplicación<br><br>…<br><br>En particular, cabe señalar que un responsable del tratamiento que preste un servicio transfronterizo no puede siempre limitarse al cumplimiento de la legislación del Estado miembro en el que tiene su establecimiento principal, sino que puede verse en la obligación de cumplir las respectivas legislaciones nacionales de cada Estado miembro en el que ofrezca el servicio o los servicios de la sociedad de la información<br><br>…. |

| | |
|---|---|
| | Cuando presten servicios de la sociedad de la información a niños sobre la base del consentimiento, se espera que los responsables adopten todas las medidas razonables para verificar que el usuario supera la edad del consentimiento digital, y estas medidas deben ser proporcionales a la naturaleza y riesgos de las actividades de tratamiento<br><br>…<br><br>Si los usuarios declaran que superan la edad de consentimiento digital, el responsable podrá llevar a cabo las comprobaciones necesarias para verificar que dicha declaración es cierta<br><br>…<br><br>Si el usuario declara no haber alcanzado la edad necesaria para dar su consentimiento digital, entonces el responsable puede aceptar dicha declaración sin más comprobaciones, pero deberá entonces obtener la autorización de los padres y verificar que la persona que da el consentimiento es el titular de la patria potestad o tutela<br><br>….<br><br>La verificación de la edad no debe conducir a un tratamiento excesivo de datos. El mecanismo elegido para verificar la edad del interesado debe conllevar una evaluación del riesgo del tratamiento propuesto. En algunas situaciones de bajo riesgo, puede resultar adecuado solicitar a los nuevos subscriptores de un servicio que indiquen su año de nacimiento o rellenen un formulario en el que declaren que son (o no son) menores.<br><br>En caso de duda, el responsable deberá revisar sus mecanismos de verificación de la edad en un caso concreto y considerar si se requieren otras comprobaciones<br><br>…<br><br>Corresponde al responsable del tratamiento determinar qué medidas son las adecuadas en un caso específico. Como norma general, los responsables del tratamiento deben evitar las soluciones de verificación que conllevan una excesiva recogida de datos personales.<br><br>…<br><br>se espera que los responsables del tratamiento mantengan sus actividades de tratamiento y la tecnología disponible en constante revisión. |
| **RGPD**<br><br>**artículo 12, Transparencia de la información, comunicación y modalidades de ejercicio de los** | 1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por |

| | |
|---|---|
| **derechos del interesado** | escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios. |
| **EDPB Guidelines 05/2020 on consent sección 7.1** | Tras alcanzar la edad de consentimiento digital, el niño tendrá la posibilidad de retirar él mismo el consentimiento, de conformidad con el artículo 7, apartado 3. Con arreglo a los principios de lealtad y responsabilidad, el responsable del tratamiento debe informar al niño sobre esta posibilidad |
| **RGPD**<br>**artículo 40, Códigos de conducta** | 2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:<br>…<br>(g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño; |
| **EDPB Guidelines 05/2020 on consent sección 7.1** | En lo referente a la autorización de un titular de la patria potestad o tutela, el RGPD no establece disposiciones prácticas para obtener el consentimiento de los padres o establecer que alguien tiene derecho a realizar dicha acción67. Por lo tanto, el CEPD recomienda la adopción de un enfoque proporcionado, en consonancia con el artículo 8, apartado 2, y el artículo 5, apartado 1, letra c), del RGPD (minimización de datos). Un enfoque proporcionado puede ser centrarse en obtener una cantidad limitada de información, por ejemplo, los datos de contacto de un padre o tutor.<br>Lo que será razonable, en relación con la verificación de que un usuario tenga edad suficiente para dar su propio consentimiento o de que una persona que da su consentimiento en nombre de un niño sea el titular de la patria potestad o la tutela, podrá depender de los riesgos inherentes al tratamiento, así como de la tecnología disponible. En casos de bajo riesgo, la verificación de la patria potestad o la tutela por correo electrónico puede ser suficiente. Por el contrario, en casos en los que el riesgo es elevado, puede resultar adecuado pedir más pruebas, de manera que el responsable pueda verificar y conservar la información de conformidad con el artículo 7, apartado 1, del RGPD68. Los servicios de verificación de terceros de confianza pueden ofrecer soluciones que minimicen la cantidad de datos personales que el propio responsable deba tratar. |

## C. UNA PRIMERA APROXIMACIÓN

Si se tienen en cuenta los fundamentos recogidos en la sección anterior, **se debe verificar siempre que se realice un consentimiento** en línea en un servicio o aplicación para todos los públicos que el usuario que lo proporciona es “capaz de consentir” o está

"capacitado para consentir". Es decir, que supera la edad entre 13 y 16 años que establezca la ley en su país (se pasa de la comprobación del +18 de los casos de uso contemplados hasta el momento a un +14, por ejemplo, en España). Cuando un usuario no pueda verificar esta capacidad, el tratamiento de datos personales que necesite de un consentimiento sólo puede realizarse tras un consentimiento de aquellos que ostentan su patria potestad o tutela. Si dicho consentimiento no se presta la consecuencia podría ser la de **prestación de un servicio de forma limitada o diferente** para estos casos, no necesariamente a que el usuario no pueda usar el servicio.

En este caso de servicios o aplicaciones para todos los públicos o audiencias, puede ocurrir que ofrezca experiencias diferentes según la edad (modelo B.1 de la sección IV) como puedan ser cuentas sólo para adultos, *apps* de adultos en las *stores* de los teléfonos, etc. **Si se hace coincidir la restricción de edad NNA/adulto con la edad necesaria para el consentimiento** (14 años en el caso de España), se puede evitar el tratamiento de datos personales cuya base legal sea el consentimiento en las versiones sin verificación de edad (las que incorporan la protección por defecto) o solicitar siempre el consentimiento parental para dichos tratamientos, por defecto. Mientras que, en el caso de las versiones para mayores, se sabe seguro que los usuarios están capacitados para otorgar los consentimientos cuando sea necesario.

Si se implementa la protección por defecto (modelo B.2), se trata a todos los usuarios de la misma manera, sin que existan cuentas o *apps* de acceso diferenciadas. Por lo tanto, siempre que un tratamiento de datos personales se base en el consentimiento es necesario **comprobar primero si el usuario está "capacitado para consentir"** realizando para ello un proceso de verificación de edad.

**En el caso de servicios o aplicaciones para adultos que obligan a verificar que el usuario es mayor de 18 años** (modelo A), **ya se sabe que dicho usuario tiene la edad adecuada para consentir** a un tratamiento de datos personales y el artículo 8 del RGPD no se debe aplicar.

Es importante recordar que el responsable de un tratamiento, antes de obtener el consentimiento, debe **proporcionar información básica** al menos de la identidad de dicho responsable, los fines del tratamiento, los destinatarios de los datos, y del ejercicio de los derechos (artículo 13 del RGPD). Y que la solicitud de consentimiento se prestará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo (artículo 7.2).

Esto significa que **un servicio no necesita tener mensajes adaptados a menores de 14 años, porque ellos no deben otorgar el consentimiento**, lo otorgan los adultos que tienen ese deber de cuidado. A su vez, si puede tener usuarios mayores de 14 años, la información también tiene que estar adaptada para ellos. Hay que tener en cuenta que **no todos los usuarios mayores de 14 años están en las mismas circunstancias** por razones de educación, de cultura, de capacidades mentales, de circunstancias personales, de la urgencia por acceder al servicio, etc. De hecho, pretender dividir el tipo de mensajes entre mensajes para 14-18 y mayor de 18 es una gran simplificación.

Es decir, cuando un servicio es para todos los públicos y no se conoce con exactitud la edad del usuario, ni sus otras circunstancias, sólo que está "capacitado para consentir", se debe garantizar que se protegen adecuadamente los derechos de todos los potenciales usuarios, **por defecto y desde el diseño**.

Aunque esta nota se centra en el caso de uso relativo al consentimiento para el tratamiento de datos personales, un enfoque similar podría seguirse para los riesgos asociados a otros consentimientos o a la firma de contratos, aceptación de condiciones, etc. Sería necesario, eso sí, realizar los matices oportunos en función de las bases legales

correspondientes (con toda probabilidad no aplicaría exclusivamente el RGPD), los umbrales de edad, etc.

También cabe recordar que las soluciones de verificación de edad resuelven una parte del problema, pero que será necesario complementarlas con otras como las de **consentimiento parental o gestión de recibos de consentimiento** para garantizar el cumplimiento de todas las obligaciones recogidas en el RGPD en relación con el consentimiento, y en concreto, con el consentimiento de los NNA.

### D. Equívocos

En este caso de uso se observa en ocasiones una **interpretación expansiva** de las obligaciones que implica el cumplimiento del RGPD. No es necesario conocer la edad de los usuarios de un servicio para cumplir con el reglamento ni saber cuáles de estos usuarios en concreto son NNA. Sólo es necesario conocer que **superan la edad mínima para otorgar un consentimiento** en aquellos casos en los que el servicio se ofrece a NNA y en los que además sea necesario recabar ese consentimiento para poder realizar un tratamiento de datos personales.

**Tampoco es necesario verificar en ningún caso la edad de los NNA**, ya que el enfoque debe ser el contrario, el usuario que desea otorgar su consentimiento debe probar que está capacitado para hacerlo.

En ocasiones también se critica la opción de la protección por defecto porque parece implicar una infantilización de todos los usuarios. Pero **el lenguaje involucrado en la solicitud del consentimiento y en el resto de las comunicaciones debe ser claro y sencillo para usuarios que superen los 14 años** (en el caso español), que son lo que están capacitados para consentir. Lo que, en la actualidad, no implica una infantilización de los mensajes e incluso puede beneficiar indirectamente a todos los usuarios sea cual sea su edad y su circunstancia. Siempre existe la opción, además, de dejar que el usuario escoja, una vez verificada su edad por encima de los 14 años, entre diferentes opciones de mensajes, explicaciones, solicitudes, etc. según su grado de competencia digital, madurez, etc.

# VIII. CASO DE USO 4: DISEÑO ADECUADO PARA LA EDAD

## A. MARCO PRELIMINAR

El término "diseño adecuado para la edad" **no tiene tampoco una definición universal, concreta y ampliamente aceptada**. En general, cuando se utiliza este concepto se asocia al de diseño adecuado para la infancia y suele referirse a **servicios, aplicaciones, términos, condiciones, políticas, interfaces y experiencia de usuario que sean adecuados para los NNA en general teniendo en cuenta sus derechos y bienestar** (incluidos derechos muy específicos, como el derecho a jugar). Y en ocasiones, se aumenta la granularidad del término para categorizar a los NNA en función de su edad.

Hay que tener en cuenta que diferentes compañías y organizaciones interactúan con los NNA de manera intencionada o específica mientras que otras lo hacen en el curso de sus actividades generales, como lo hacen con usuarios de cualquier otra edad. Todas ellas deben tener en cuenta el caso de uso 3 y lo ya explicado en lo relativo al consentimiento para el tratamiento de datos personales.

En cualquier caso, existe cierta **obligación hacia la infancia de proporcionar servicios y aplicaciones adecuados, o al menos, no inadecuados**. Pero ¿qué implica esta obligación? ¿quién debe asumirla y hasta qué punto? Porque este caso de uso debe separarse claramente del 2, que se refiere exclusivamente a los entornos seguros y por lo tanto está relacionado con la protección frente a riesgos asociados a contenido, conducta, contacto o de corete transversal. En este caso de uso 4 **los riesgos están relacionados con la conducta, el consumo, consentimiento o contrato y con otros riesgos de corte transversal**. Es decir, con riesgos que pueden afectar igualmente al interés superior del menor o a sus derechos y libertades, pero de otra forma. En general, sin impactos importantes para su integridad física y mental.

Cabe destacar que la Comisión Europea ha formado recientemente un "Special group on the EU Code of conduct on age-appropriate design"[16] que está trabajando desde el verano del 2023 en el *EU Code of conduct on age-appropriate design* (BIK Code). Este código no se ha hecho público todavía, pero sí otros **códigos de diseño adecuado para la infancia** como el del ICO[17], el primero publicado, o el *California Age Appropriate Design Code*[18] (que está a la espera de una decisión en un tribunal para comenzar a aplicarse[19]). Diferentes países están trabajando en la actualidad en nuevos borradores de los que ya se han compartido algunos detalles.

También es interesante para este caso de uso el estándar *2089-2021: IEEE Standard for an Age Appropriate Digital Services Framework*[20] basado en los trabajos previos de la organización 5Rights, que se centra en los **procesos que las organizaciones deben llevar a cabo para que sus servicios y aplicaciones sean adecuados para la infancia**. Existe además un Workshop Agreement de septiembre del 2023 en relación con este estándar a nivel europeo, a través de CEN y CENELEC (CWA 18016[21]).

[16] https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design
[17] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/
[18] https://californiaaadc.com/
[19] https://natlawreview.com/article/california-age-appropriate-design-code-act-enjoined
[20] https://ieeexplore.ieee.org/document/9627644
[21] https://www.cencenelec.eu/news-and-events/news/2023/eninthespotlight/2023-09-14-cwa-18016-children-protection-online/

## B. FUNDAMENTOS JURÍDICOS

El concepto de diseño adecuado para la edad es transversal, ya que los derechos de los NNA, su bienestar y la protección de su interés superior aparece en muchas regulaciones y muy heterogéneas. Se pueden encontrar menciones al diseño adecuado en normas europeas de:

- Protección de datos (ya se ha discutido en los casos uso anteriores).
- Protección del consumidor.
- Seguridad y protección de integridad física, sexual y ante abusos.
- Servicios, productos y mercados digitales.
- Educación.
- Salud.
- Igualdad.

La diferencia fundamental con los tres casos de uso ya discutidos en este documento es que el diseño adecuado para la infancia o para la edad no suele ser una obligación legal sino una recomendación o un elemento deseable pero opcional.

## C. UNA PRIMERA APROXIMACIÓN

Si se sigue el mismo razonamiento que en los casos de uso anteriores, **los servicios o aplicaciones para adultos no tienen que preocuparse por ofrecer un diseño adecuado para la infancia**. Son los servicios o aplicaciones para todos los públicos o audiencias los que pueden plantearse hacerlo, y se distinguen dos escenarios.

Cuando se separa por edad (modelo B.1), la versión para la experiencia infantil es la que debería ajustarse, por defecto, a las diferentes recomendaciones recogidas en los códigos de diseño adecuado que sean de aplicación. Lo que no ocurre en el caso de la versión para mayores. En este caso, hasta el momento, **el límite de edad no está fijado en ninguna regulación europea** sino en los códigos ya mencionados y en las obligaciones o recomendaciones que recogen.

En el caso de la protección por defecto (modelo B.2), se trata a todos los usuarios de la misma manera porque no se conoce su edad, ni si superan una edad determinada. Se deben aplicar los estándares del código a todos los usuarios de manera que **los NNA estén expuestos siempre a un diseño adecuado para ellos**. Esto garantiza que se respetan sus necesidades y que se protege su interés superior. **Los adultos que verifiquen su edad podrán modificar este diseño o configuraciones predeterminadas si así lo desean**. Este enfoque puede ser beneficioso para usuarios con menos competencia digital, personas mayores o con ciertas discapacidades, por mencionar sólo algunos ejemplos.

En relación con esto último, una buena práctica, en general, es **no relacionar madurez o competencia digital con edad**. Todos los usuarios (no sólo los NNA) deberían tener la opción de acceder de manera voluntaria a versiones diferentes, en cuanto a diseño, de los interfaces de los servicios y aplicaciones que utilizan según sus necesidades y preferencias. Este **diseño adaptativo** no tiene por qué basarse necesariamente en procesos de verificación de edad, sino en dar opciones a los usuarios para que escojan libremente las que creen más adecuadas, útiles o beneficiosas para ellos. **Los navegadores o las aplicaciones de acceso a los diferentes servicios pueden dar un soporte importante en todo lo relativo a dicho diseño adaptativo**, de manera que el usuario no tenga que

realizar su selección caso por caso y en cada ocasión, sino que sus decisiones puedan recordarse o automatizarse en función de ciertas configuraciones o preferencias.

### D. Equívocos

En el caso de diseños adaptados para la infancia existen equívocos importantes en relación con **las servicios y aplicaciones clasificados por rango de edad**.

En resumen, el primero es el ya comentado a lo largo de toda esta nota de basar la solución en conocer qué usuarios en concreto son NNA y en la supuesta **necesidad de conocer su edad concreta. El segundo, confundir la edad o el rango de edad con el grado de madurez**, que varía entre géneros y situaciones educativas y culturales, por ejemplo. Como ya se ha explicado, con el enfoque habilitador, proactivo y por defecto de la verificación de edad, son los mayores los que, en algunos casos, tendrán que verificar su edad para acceder a un diseño adecuado o cómodo para ellos, y no al contrario. Y además sólo cuando deseen ese tipo de adaptación, ya que podría suceder que por su grado de madurez o por otras circunstancias prefirieran el interfaz que por defecto se considera adecuado para los NNA (esto sólo con el modelo B.2, con el A y el B.1 tendrán un interfaz por defecto diferente del adecuado para NNA).

El tercero es que un proveedor de Internet predetermine qué grado de madurez tiene un NNA en función de su edad o rango de edad, y **no sea la familia, o incluso el NNA**, el que pueda elegir qué diseño desea emplear teniendo en cuanta sus circunstancias personales. Los proveedores no deberían imponer la forma en la que un NNA utiliza Internet en función de sus criterios particulares.

Y el cuarto es la falta de concreción o estandarización del término “diseño adecuado para la infancia”. Hay que preguntarse **¿adecuado para qué?** Ya que una respuesta puede ser la de que sea más persuasivo o adictivo para NNA, convirtiendo este tipo de diseño en **un patrón engañoso que debería evitarse por los riesgos que implica**.

## IX. APLICACIÓN DEL DECÁLOGO PROPUESTO POR LA AEPD

Como ya se ha mencionado con anterioridad en esta nota la AEPD publicó en diciembre del 2023 su "Decálogo de principios: Verificación de edad y protección de personas menores de edad ante contenidos inadecuados". Este decálogo se planteó para facilitar el cumplimiento del RGPD y la defensa del **interés superior del menor** en escenarios en los que el propósito fuera la protección de la infancia ante **contenidos inadecuados**. Contenidos en el sentido más amplio de la palabra, ya que se puede tratar también de servicios, funcionalidades o productos. Es decir, se centraba, esencialmente, en el caso de uso 1 de esta nota técnica.

Pero, como se ha analizado en las secciones anteriores, las soluciones de verificación de edad pueden emplearse en **otros escenarios diferentes** de este, por lo que surge la pregunta de si el decálogo de principios propuesto puede ser aplicado directamente a estos casos de uso que no están relacionados exclusivamente con la protección ante contenidos inadecuados sino con la protección ante otros tipos de riesgos.

La respuesta es afirmativa, ya que el enfoque para utilizar la verificación de edad como herramienta fundamental en la protección de los NNA es el mismo en todos los casos de uso: debe emplearse **sólo cuando sea necesario, minimizando los datos tratados** (no es necesario conocer la fecha de nacimiento ni la edad exacta, sólo que se supera un umbral de edad), poniendo la **carga de la prueba en el usuario que supera el umbral del edad** (la verificación de edad es siempre un habilitador) y respetando los principios y requisitos que recoge el RGPD. Simplemente habría que **generalizar el lenguaje** con el que se expresan estos principios para que fueran aplicables a todos los casos de uso:

- **Principio 1:** La verificación de edad no debe posibilitar la identificación, el seguimiento o la localización de menores a través de Internet.
- **Principio 2:** La verificación de edad debe posibilitar que las personas con la edad adecuada acrediten su condición de persona que "supera el umbral de edad requerido", y no al contrario, acreditar su condición de "menor de edad" o "no supera el umbral de edad requerido".
- **Principio 3:** La acreditación de la superación del umbral de edad requerido debe ser anónima para los proveedores de servicios de Internet y terceras entidades.
- **Principio 4:** La obligación de acreditar la condición de persona que "supera el umbral de edad requerido" estará limitada únicamente a los tratamientos en los que dicha acreditación sea necesaria.
- **Principio 5:** La verificación de edad debe cumplir los requisitos de exactitud, idoneidad y minimización de datos. Para esto último debe categorizar si la persona "supera el umbral de edad requerido" o equivalente.
- **Principio 6:** La verificación de edad no debe posibilitar el perfilado de las personas en función de su navegación por Internet.
- **Principio 7:** La verificación de edad no debe posibilitar la vinculación de la actividad de una persona entre distintos servicios de Internet.
- **Principio 8:** Toda solución para la verificación de edad debe garantizar el ejercicio de la patria potestad por los progenitores cuando el caso de uso así lo exija.
- **Principio 9:** Toda solución para la verificación de edad debe garantizar los derechos fundamentales de todas las personas en su acceso a Internet.
- **Principio 10:** Toda solución para la verificación de edad debe tener definido un marco de gobernanza.

## X. CONCLUSIONES

Un Internet seguro por defecto supone **garantizar a niños, niñas y adolescentes (NNA) sus derechos y libertades en el entorno digital** minimizando los riesgos asociados a contenidos perjudiciales, al contacto con otras personas, a la inducción a comportamientos nocivos, a la contratación de productos y servicios o a la falta de control sobre sus propios datos personales, por mencionar sólo algunos ejemplos.

Las soluciones de verificación de edad son una **herramienta esencial** para conseguir este Internet seguro por defecto y pueden ayudar a gestionar los riesgos asociados a las 5Cs: Contenido, Contacto, Conducta, Consumo (consentimiento o contrato) y de Corte transversal. Así lo recogen diferentes **regulaciones nacionales y europeas que imponen obligaciones** a los actores de Internet. Sin embargo, hay que tener en cuenta que las soluciones de verificación de edad, por sí mismas, no bastan para proteger a la infancia en Internet. Los servicios de Internet y las herramientas que permiten acceder a ellos (como las aplicaciones que se ofrecen en las *stores* o los navegadores) deben **integrar adecuadamente** las comprobaciones de edad con otras soluciones y herramientas para proteger de forma efectiva a los NNA y los derechos de todos los ciudadanos.

La presente nota ha identificado **diferentes modelos** para incorporar la verificación de edad en servicios de Internet **desde el diseño y por defecto**. Y los ha analizado en cuatro casos de uso diferentes: protección ante contenidos inadecuados, entornos seguros para la infancia, consentimiento en línea para el tratamiento de datos personales y diseño adecuado para la edad. **Cada caso de uso analizado está sujeto al RGPD en cuanto a los tratamientos de datos personales y a otros marcos regulatorios diferentes que deben examinarse cuidadosamente** para garantizar que el tratamiento de datos personales que se realiza durante el proceso de verificación de edad es **lícito**.

Existen **equívocos, errores, ambigüedades y tergiversaciones** en relación con la protección de los NNA en Internet, en concreto con sus requisitos, propiedades deseables o implicaciones. Algunos de los equívocos más peligrosos son los **relacionados con los "entornos seguros", "cuentas para menores" o con el diseño "adecuado para la infancia"**. En muchos casos se propone saber **qué usuarios concretos son NNA** para configurar y monitorizar su actividad. Esto supone un riesgo, ya que el menor está localizado y fácilmente accesible para servicios de terceros (autorizados o no autorizados) o explícitamente maliciosos, creando el efecto de "pescar en una pecera".

Una excusa habitual para conocer qué usuarios concretos son NNA es que la información para la toma de decisiones ha de estar adaptada a un lenguaje que ellos puedan entender, por ejemplo, en el caso de los términos de servicio. Sin embargo, la toma de decisiones para consentir tratamientos de datos personales, contratar o consentir el contacto con otros usuarios es una obligación, el deber de cuidado, que legalmente recae sobre los que ostentan la patria potestad o tutela. **No es necesario adaptar el lenguaje para que NNA tomen decisiones que, según su edad, ni siquiera les corresponden**.

Otra excusa empleada para localizar a NNA es la adaptación de los entornos digitales o diseños a su edad. Sin embargo, esto supone, o bien que los menores han de estar en entornos de Internet que ofrecen las mismas características y funcionalidades a todos los usuarios de entre 5 y 14/16/18 años, o bien que se requiere una mayor granularidad en la determinación de la edad del NNA. En cualquier caso, se fuerza a estos usuarios a adaptarse a la "media" o a estándares definidos por un proveedor. De nuevo existe el riesgo de mantener a los NNA en espacios separados de tipo "corralito". Además, estas aproximaciones pueden pretender **legitimar el tratamiento de datos del menor,** y por ende de todos los usuarios, y esconder propósitos de perfilado más preciso con relación a patrones engañosos y adictivos, fidelización, contratación, consumo o monetización de datos personales. Además, en muchos casos implican la utilización de nuevos esquemas de

gestión de identidades en Internet, o bien específicos para menores o bien para todos los usuarios, que recogen datos personales fuera de las garantías a la propia identidad desarrolladas en la regulación nacional o europea, dependientes de servicios (en ocasiones localizados fuera de la UE), sin garantías de disponibilidad. Y, lo que podría ser más preocupante que convierten la identidad de las personas, un derecho, en un servicio.

Otro error muy extendido es el que pretende ofrecer un Internet seguro por defecto basado exclusivamente en estrategias de tipo **reactivo**: dejar que se realicen tratamientos de datos personales de NNA, que sean expuestos a riesgos y, en el mejor de los casos, reaccionar cuando se detecte que se está produciendo un daño. Esto implica exponer al menor a que, por ejemplo, cualquier usuario pueda contactarlo; someter a todos los usuarios a técnicas de vigilancia y perfilado; acumular evidencias de acoso o pedofilia; aplicar criterios establecidos por el proveedor servicio y finalmente actuar. Esta estrategia precisa que se produzca un daño al menor y, además, que se produzca una intervención intrusiva y sistemática a la privacidad de todos los usuarios, por lo que **los tratamientos de datos personales involucrados no son idóneos ni leales**.

Esta nota explica cómo conseguir un Internet seguro por defecto con **un cambio de paradigma** que rechace todos estos equívocos. La aproximación para la gestión de los riesgos para los NNA debe ser siempre **proactiva**, enfocada en la prevención y con la intención de evitar o minimizar los impactos y daños, no de reaccionar una vez se han producido. El enfoque debe ser **habilitador**, de manera que se verifique que los usuarios superan el umbral de edad requerido para pasar realizar una acción o acceder a un elemento en Internet. De esta forma se evita someter a la verificación de edad (con el consiguiente tratamiento de datos personales) a los NNA, que quedan **protegidos por defecto**. Por lo tanto, el menor no debe probar que es menor, ni exponer su naturaleza para que se "bloqueen" contenidos, contactos, comportamientos o contratos. Al contrario, este paradigma devuelve a los familiares y tutores la capacidad de ejercer su deber de cuidado, trasladando la carga de la prueba a los usuarios que pueden asumir riesgos y tienen la voluntad de hacerlo.

Un Internet seguro por defecto se puede conseguir aplicando el **decálogo** de principios propuesto por la AEPD para la verificación de edad en todos los casos de uso analizados y en otros que puedan surgir en el futuro relacionados con la protección de la infancia ante los riesgos asociados las 5 Cs. La verificación de edad o conocer la edad de los usuarios **no es la finalidad** o el objetivo en sí mismo, la finalidad de cualquier tratamiento de datos en el marco de los cuatro casos de uso descritos es el de la protección de los NNA.

Las decisiones de diseño de estas soluciones deben basarse siempre en procesos rigurosos **basados en la evidencia** tanto técnica como científica (por ejemplo, con relación a la integridad física y mental de los NNA) y de **la gestión de riesgo** para los derechos de la infancia y para la protección de datos de NNA y usuarios en general, y no en intuiciones, modas o creencias. Por tanto, las decisiones para la gestión de estos riesgos para los NNA deberían basarse en una **evaluación de impacto para los derechos de la infancia (CRIA)**, y los tratamientos que se implementan para ello, en particular los de verificación de edad, dado el **alto riesgo** para los derechos y libertades de los individuos, en una **evaluación del impacto del tratamiento en la protección de datos personales** (EIPD) que debe realizar el responsable de dicho tratamiento de datos personales.

Para superar esta EIPD hay que cumplir, entre otros, con el principio de **minimización** de datos y, en el caso que nos ocupa, la verificación de edad no necesita, en ninguno de los casos de uso analizados, verificar una edad concreta ni una fecha de nacimiento, sólo la superación del umbral de edad necesario. Además, se deben adoptar todas las medidas razonables para que los datos tratados en los procesos de verificación de edad sean **exactos** con respecto a los fines para los que se tratan, es decir, debe garantizarse un nivel

de certidumbre suficiente cuando se verifica que un usuario está por encima del umbral de edad requerido, ya que esto es lo que permite cumplir la finalidad del tratamiento, proteger al NNA de los riesgos ya mencionados. Esto garantiza la idoneidad del tratamiento de datos personales que se realiza para verificar la edad.

En particular, no es suficiente incluir una capa de ciberseguridad sobre el ecosistema de Internet. Los proveedores de servicios en Internet tienen la **obligación** de evolucionar para **implementar los principios de protección de datos desde el diseño y por defecto**.

El ecosistema de Internet **no puede tratarse como un conjunto de islas independientes**. Para efectuar un cambio de paradigma en la protección de los NNA se requiere, no solo una **cooperación** entre los implicados en el ecosistema de Internet a la hora de diseñar soluciones, sino también una **comunicación efectiva** entre ellos ante la identificación de nuevas amenazas a través de un **marco de gobernanza.** Los implicados son los proveedores, fabricantes, intermediarios y resto de operadores de Internet, así como las autoridades de protección de datos, de consumo y las competentes en la regulación del mercado, especialmente de productos y servicios que se ofrecen en Internet. También las organizaciones gubernamentales y no gubernamentales que tienen como propósito la educación y la protección del menor, tanto españolas como europeas. Y por supuesto, los responsables de tratamientos de datos personales que consuman o utilicen dichos productos y servicios que se ofrecen en Internet y aquellos que ostentan la patria potestad o tutela de los NNA.

## XI. BIBLIOGRAFÍA


Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 06/12/2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual. BOE núm. 163, de 08/07/2022. https://www.boe.es/buscar/act.php?id=BOE-A-2022-11311

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679

DIRECTIVA (UE) 2018/1808 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de noviembre de 2018 por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32018L1808

REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022R2065

5Rights Foundation. (2024, March). The best interests of the child in the digital environment. https://5rightsfoundation.com/uploads/dfc-report-best-interests-of-the-child.pdf

5Rights Foundation. (2024, April). Enforcing the online safety act for children: Ambitions for the children's safety code of practice. https://5rightsfoundation.com/uploads/enforcing-the-online-safety-act-for-children-children-s-coalition.pdf

Cannataci, J. A. (2021). Artificial intelligence and privacy, and children's privacy: Report of the Special Rapporteur on the right to privacy. A/HRC/46/37. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/en/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy

Digital Trust & Safety Partnership. (2023, September). Age Assurance Guiding Principles and Best Practices. https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf

European Parliamentary Research Service. (2023, February). Online age verification methods for children. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf

eSafety Commissioner. (2023, December). Phase 1 Industry Codes (Class 1A and Class 1B Material) Regulatory Guidance. Australian Government. https://www.esafety.gov.au/sites/default/files/2023-12/Phase-1-Industry-Codes-%28Class-1A-and-Class-1B-Material%29-Regulatory-Guidance.pdf

Mukherjee, S., Pothong, K., & Livingstone, S. (2021, March). Child Rights Impact Assessment: A tool to realise child rights in the digital environment. Digital Futures Comission. https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf

Sas, M., & Mühlberg, J.T. (2024, February). Trustworthy age assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective. The Greens/EFA in the European Parliament. https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance

Shaffique, M. R., & van der Hof, S. (2024, February). Research report: Mapping age assurance typologies and requirements. Better Internet for Kids (BIK) project. https://op.europa.eu/en/publication-detail/-/publication/215f6c72-fe04-11ee-a251-01aa75ed71a1/language-en/format-PDF/source-search

UN Committee on the Rights of the Child. (2021, March). General comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

UNESCO. (2023, April). Safeguarding freedom of expression and access to information: guidelines for a multistakeholder approach in the context of regulating digital platforms. https://unesdoc.unesco.org/ark:/48223/pf0000384031

van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. The International Journal of Children's Rights, 28(4), 833-859. https://brill.com/view/journals/chil/28/4/article-p833_833.xml