

Decálogo de principios

Verificación de edad y protección de personas menores de edad ante contenidos inadecuados

| Diciembre 2023



I. Marco de protección de la población menor de edad

La Convención de las Naciones Unidas de 20 de noviembre de 1989, sobre los Derechos del Niño, consagra el interés superior del menor como principio al que atenderán sus estados firmantes en todas las medidas que les afecten.

El Comité de los Derechos del Niño, que supervisa la aplicación de la mencionada Convención, en la Observación General núm. 15, de 2013, sobre el derecho de las personas menores de edad al disfrute del más alto nivel posible de salud, ya señalaba en su apartado 38, y en una fecha tan temprana, los problemas que un uso excesivo de Internet está generando en las personas menores de edad por:

“Preocupa al Comité el aumento de la mala salud mental en los adolescentes, en concreto trastornos en el desarrollo y la conducta, depresión, trastornos alimentarios, ansiedad, traumas psicológicos resultantes de (...) comportamientos obsesivos, como un uso excesivo de Internet y otras tecnologías hasta un punto adictivo y la autolesión y el suicidio.”

Y en su Observación General núm. 25, de 2021, sobre los derechos de la población menor de edad en relación con el entorno digital señala, en su apartado 96, la obligación de los Estados para proteger a las personas menores de edad en su uso de juegos digitales o redes sociales:

“Los Estados parte deben establecer normas para evitar los daños conocidos y tener en cuenta de forma proactiva las nuevas investigaciones y pruebas en el sector de la salud pública a fin de evitar la difusión de información errónea y de materiales y servicios que puedan dañar la salud mental o física de los niños. También puede ser necesario adoptar medidas para prevenir cualquier participación perjudicial en juegos digitales o en las redes sociales, por ejemplo, reglamentaciones que prohíban los programas digitales que menoscaben el desarrollo y los derechos de los niños.”

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece en su artículo 84.1,

“Protección de los menores en Internet”, el papel que también han de tener aquellos que ostentan la patria potestad en proteger a las personas menores de edad con relación al uso de Internet:

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

Algunos datos concretos pueden dar una idea de la situación actual en relación con el uso que hacen de Internet las personas menores de edad. Por ejemplo, la encuesta del Instituto Nacional de Estadística sobre el uso de Internet en los hogares en el 2022 muestra que el 90% de la población menor de 10 años usa Internet, porcentaje que se eleva al 98,3% con 15 años, y que un tercio de ellos usa Internet más de 5 horas al día. Transparency Market Research¹ estimó en 2021 que el mercado de marketing digital orientado a personas menores de edad ascendía a 2,9 mil millones de dólares, con una perspectiva de crecimiento del 21% anual.

Save The Children ha publicado estudios en 2020 que muestran que el 62,5 % de la población adolescente entre 13 y 17 años ha consumido pornografía, que la edad media de inicio en su consumo se establece en los 12 años, que el 54% consideran la pornografía una fuente de inspiración para sus relaciones sexuales y el 55% desea llevarla a la práctica, realizando sexting² un 20%. Esta situación está provocando problemas en el neurodesarrollo de la población menor de edad, en su capacidad de atención, en su aprendizaje, en su desarrollo emocional y en la aparición de actitudes agresivas de forma irreversible.

A la luz de esta situación, la AEPD ha impulsado, junto con la Fiscalía General del Estado, la propuesta de Pacto de Estado³ promovida por organizaciones de la sociedad civil implicadas en los derechos de la infancia y la adolescencia.

¹ <https://www.transparencymarketresearch.com/kids-digital-advertising-market.html>

² Envío a través del teléfono móvil u otro dispositivo de fotografías o vídeos producidos por uno mismo con connotación sexual.

³ <https://digitalforeurope.eu/pacto-personas-menores-de-edad-online>.

II. Verificación de edad en un sistema de protección de personas menores de edad ante contenidos inadecuados

La Comisión Europea en su Comunicación de 2022 sobre la nueva estrategia para un Internet mejor para la población menor de edad⁴, aboga por y apoya los métodos eficaces de verificación de la edad con carácter prioritario⁵. Las mejores prácticas y orientaciones de esta Comunicación deben ser tenidas en cuenta⁶, según establece 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 o DSA por sus siglas en inglés).

En España, la Ley General de Comunicación Audiovisual de 2022⁷ exige, como medidas para la protección de personas menores de edad frente a determinados contenidos audiovisuales, que los prestadores de servicios de intercambio de vídeos a través de plataforma han de establecer y operar sistemas de verificación de edad de las personas usuarias con respecto a los contenidos que puedan perjudicar el desarrollo físico, mental o moral de la población menor de edad y que, en todo caso, impidan su acceso a los contenidos más nocivos como la violencia gratuita o la pornografía⁸. La idoneidad de estas medidas deberá ser evaluada por la Comisión Nacional de los Mercados y la Competencia, previo informe preceptivo de la AEPD⁹.

A. Definición de términos

La Convención sobre los Derechos del Niño establece que:

Artículo 1 Para los efectos de la presente Convención, se entiende por niño todo ser humano menor de dieciocho años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad.

La DSA, en su Considerando 89, establece la exigencia de proteger a las personas menores de edad con relación a contenidos que puedan perjudicar su desarrollo físico, mental o moral.

A lo largo de este documento se utilizará el término “menor” o “menores” para aquellas personas que en función de su edad (menor de 14 años, menor de 18 años u otros casos según la situación) tengan que ser protegidas frente a contenidos inadecuados según su edad, y el término “adulto” se utilizará en sentido contrario.

El término “contenido inadecuado” se utilizará para aquellos sitios de Internet restringidos solo a personas adultas, contenidos calificados como “mayores de 18 años” (pornografía, violencia extrema), sitios de Internet limitados al acceso por mayores de 14 años, y contenidos perjudiciales, adictivos o publicitarios prohibidos a personas menores de edad.

⁴ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Una década digital para los niños y los jóvenes: la nueva estrategia europea para una internet mejor para los niños (BIK+). COM(2022) 212 Final, de 11 de mayo de 2022.

⁵ Apartado 5.1.

⁶ Considerando (71).

⁷ Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

⁸ Art. 89.1.e.

⁹ Art. 93.3

B. Sistema de protección de personas menores de edad ante contenidos inadecuados.

El propósito de la protección del menor en Internet es resguardarlo del acceso incontrolado a contenidos inadecuados, lo que supone que el objetivo final es distinto al de verificar su edad o de someterlo a vigilancia y seguimiento. Los contenidos inadecuados para personas menores de edad han de ser libremente accesibles para aquellas personas usuarias de Internet que, habiendo decidido consultarlos, pueden demostrar que cumplen las condiciones de edad establecidas.

La verificación de la edad de la persona usuaria es solo el primer paso en un sistema cuyo objetivo sea proteger a personas menores de edad ante contenidos inadecuados. Este sistema estará formado básicamente por los siguientes elementos:

- Por un mecanismo de verificación de edad, que proporcionará una información cierta sobre la autorización de acceso a contenidos orientados a personas adultas.
- Unas políticas de calificación de sitios y contenidos por razones de edad, que permitirán tener un criterio de qué sitios en Internet, o qué contenidos en sitios generalistas, son considerados contenidos orientados a personas adultas o tienen establecidos unos requisitos de limitación de acceso por edad.
- Una calificación de los sitios, o de los contenidos, en función y aplicación de las políticas previamente establecidas. Esta calificación supone la aplicación de las políticas anteriores.
- Una ejecución de las políticas de acceso en función de las políticas establecidas, la calificación de los contenidos y de la autorización de acceso de la persona usuaria, que realizará el filtrado de los contenidos. Esta ejecución debe implicar, no solo a las entidades responsables de los sitios web y de las redes sociales, sino también a los buscadores en Internet, las empresas de telefonía móvil y los fabricantes de videojuegos o dispositivos, entre otros.

C. Protección del interés superior del menor.

El considerando 89 de la DSA incide en que la obligación de los prestadores de plataformas y de motores de búsqueda de gran tamaño no se reduce solo a una verificación de edad, ni a la protección frente a contenidos inadecuados para personas menores. Dicha obligación tiene que abarcar la protección del interés superior del menor en todas sus facetas:

“Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben tener en cuenta el interés superior de los menores a la hora de adoptar medidas como adaptar el diseño de su servicio y su interfaz en línea, en especial cuando sus servicios se dirijan principalmente a menores o sean utilizados predominantemente por ellos.”

El interés superior de las personas menores de edad ha de guiar el diseño y la implementación de sistemas de protección teniendo en cuenta, entre otros, su derecho a la privacidad y la intimidad, limitando la exposición de su condición de menor para evitar riesgos que son distintos y podrían ser más graves que el acceso a dichos contenidos. Por lo tanto, dichos sistemas no se pueden plantear con una visión estrecha enfocada en la limitación de acceso, o solo centrados en la verificación de edad, sino que debe tener en cuenta la complejidad del contexto del tratamiento y la necesidad de proteger dicho interés superior, así como el marco general de los derechos fundamentales. Entre otros, es necesario proteger a las personas menores de edad de la captación ilegítima, continuada y masiva de sus datos personales, así como de su perfilado y de la permanente exposición de este colectivo vulnerable a la publicidad que enriquece estos sitios.

La implementación de un sistema de protección de personas menores de edad ante contenidos inadecuados requiere la cooperación de múltiples intervenientes con un compromiso real de proteger los intereses fundamentales del menor en todas sus dimensiones y los derechos fundamentales de todas las personas usuarias de Internet con relación a la protección de sus datos personales. Tales intervenientes son todas aquellas personas e instituciones responsables legalmente de la salud de las personas menores de edad, organismos regulatorios, asociaciones y fundaciones para la protección del menor, proveedores de contenidos

y servicios de Internet, entre otros. Un sistema efectivo, objetivo y ecuánime difícilmente puede, ni debe, ser implementado de forma unilateral. Igualmente, en la medida que suponen un alto riesgo para toda la ciudadanía, se han de realizar las necesarias Evaluaciones de Impacto, tanto para la Protección de Datos de todos los interesados, como para la protección de la salud y el desarrollo de las personas menores de edad.

D. Protección de los derechos de la ciudadanía en internet

Los sistemas de protección de las personas menores de edad ante contenidos inadecuados, aunque estén pensados para su protección, en la práctica se aplican a toda la ciudadanía que accede a Internet, por lo tanto, estos sistemas han de estar diseñados para respetar los derechos fundamentales de todos ellos. Es más, deben estar orientados a ser usados por personas adultas, y no por personas menores de edad, ya que son los que tienen que acreditar su condición de “persona autorizada a acceder”.

Estos sistemas de protección, en la medida que supongan un tratamiento de datos personales, han de estar legitimados, ser idóneos, necesarios y proporcionales. En particular, hay que tener en cuenta las prohibiciones de tratar categorías especiales de datos (artículos 9 y art.22 del Reglamento General de Protección de Datos (RGPD), de 2016) como la identificación y autenticación biométricas, y sus excepciones.

En ese sentido, en el artículo 28 de la DSA “Protección de los menores en línea”, establece que

la verificación de edad, y la protección del interés superior del menor, no es una base jurídica que legitime el tratamiento adicional de datos de una persona menor:

“3. El cumplimiento de las obligaciones establecidas en el presente artículo no obligará a los prestadores de plataformas en línea a tratar datos personales adicionales a fin de evaluar si el destinatario del servicio es un menor.”

Los sistemas de protección de personas menores de edad ante contenidos inadecuados implican tratamientos de alto riesgo para los derechos de las personas individualmente, pero también pueden tener un gran impacto para la sociedad en su conjunto. El alto riesgo de estos sistemas implica que las estrategias más adecuadas para gestionarlo son aquellas que preservan el anonimato de la persona usuaria de cara a los proveedores de servicios de Internet y terceras entidades en el marco de la verificación de edad. Además, han de proporcionar herramientas transparentes, auditables, bajo el control de la persona usuaria para acreditar la autorización para el acceso a contenidos inadecuados y que generen confianza. Todo ello sin perjuicio de la obligación de implementar todas las medidas de privacidad necesarias que resulten de la realización de una evaluación de impacto para la protección de datos y superar un análisis de idoneidad, necesidad y proporcionalidad.



III. Principios que ha de cumplir un sistema de protección de personas menores de edad ante contenidos inadecuados

Los sistemas de protección de personas menores de edad ante contenidos inadecuados han de seguir los siguientes principios para garantizar el interés superior del menor y los derechos fundamentales con relación al tratamiento de los datos personales de todas las personas usuarias de Internet.

PRINCIPIO 1:

El sistema de protección de personas menores de edad ante contenidos inadecuados debe garantizar que no es posible la identificación, el seguimiento o la localización de menores a través de Internet.

PRINCIPIO 2:

La verificación de edad debe estar orientada a que las personas con la edad adecuada acrediten su condición de “persona autorizada a acceder”, y no permitir la acreditación de la condición de “menor de edad”.

PRINCIPIO 3:

La acreditación para el acceso a contenidos inadecuados debe ser anónima para los proveedores de servicios de Internet y terceras entidades.

PRINCIPIO 4:

La obligación de acreditar la condición de “persona autorizada a acceder” estará limitada únicamente al contenido inadecuado.

PRINCIPIO 5:

La verificación de edad se debe realizar de forma cierta y la edad categorizada a “persona autorizada a acceder”.

A la hora de ser aplicados, estos principios no se han de entender de forma independiente, sino que deben ser **abordados de forma conjunta**.

PRINCIPIO 6:

El sistema debe garantizar que las personas no pueden ser perfiladas en función de su navegación.

PRINCIPIO 7:

El sistema debe garantizar la no vinculación de la actividad de una persona entre distintos servicios.

PRINCIPIO 8:

El sistema debe garantizar el ejercicio de la patria potestad por los progenitores

PRINCIPIO 9:

Todo sistema de protección de personas menores de edad ante contenidos inadecuados debe garantizar los derechos fundamentales de todas las personas en su acceso a Internet.

PRINCIPIO 10:

Todo sistema de protección de personas menores de edad ante contenidos inadecuados debe tener definido un marco de gobernanza.

En el desarrollo de los principios, que se realiza a continuación, se ofrecen algunos ejemplos de soluciones para las cuestiones que plantean, y que no pretenden excluir otras posibles opciones.

PRINCIPIO 1:

El sistema de protección de personas menores de edad ante contenidos inadecuados debe garantizar que no es posible la identificación, el seguimiento o la localización de menores a través de Internet

Un sistema de protección ha de preservar el interés superior del menor. Dicho interés es mucho más amplio que únicamente limitar su acceso a contenidos inadecuados, sino que, entre otros, ha de preservar su intimidad, su seguridad, su salud física y mental, su educación y su derecho al libre desarrollo de su personalidad y sus capacidades personales¹⁰.

Los sistemas de protección de personas menores ante contenidos inadecuados han de impedir identificar entre las personas usuarias de Internet a aquellas que son menores, de forma que potenciales agresores, pederastas, esquemas adictivos o cualquiera que pretenda localizar o emitir contenidos específicos para personas menores de edad con propósitos maliciosos sean incapaces de construir servicios engañosos para localizarlas. Cualquier sistema que esté basado en que la persona menor tenga que revelar su condición de menor, debe ser evitado.

La obligación que pueden tener distintos intervinientes de verificar la edad de aquellos que desean acceder a contenidos inadecuados no es una base legal para el tratamiento de datos de personas menores de edad. Un sistema basado en la recogida de datos del menor implica un tratamiento de datos de una persona menor que en sí mismo ha de estar legitimado, ser idóneo, necesario y proporcional.

Los sistemas basados en el perfilado de las personas usuarias de Internet en servidores de los proveedores de servicios, o de terceras entidades que actúan como intermediarios entre la persona usuaria y el contenido, permiten identificar personas menores de edad. Igualmente, sistemas basados en el reconocimiento facial o información



biométrica ejecutados en dichos servidores, no exclusivamente en el dispositivo personal, tienen el peligro de ser incorporados en servicios maliciosos con el propósito de identificar personas menores de edad. Estos sistemas pueden incurrir en riesgos adicionales cuando se construyan utilizando bases de datos centralizadas en las que se acumule gran información relativa a la identidad y hábitos de navegación de gran parte de la ciudadanía y, en particular, de las personas menores de edad.

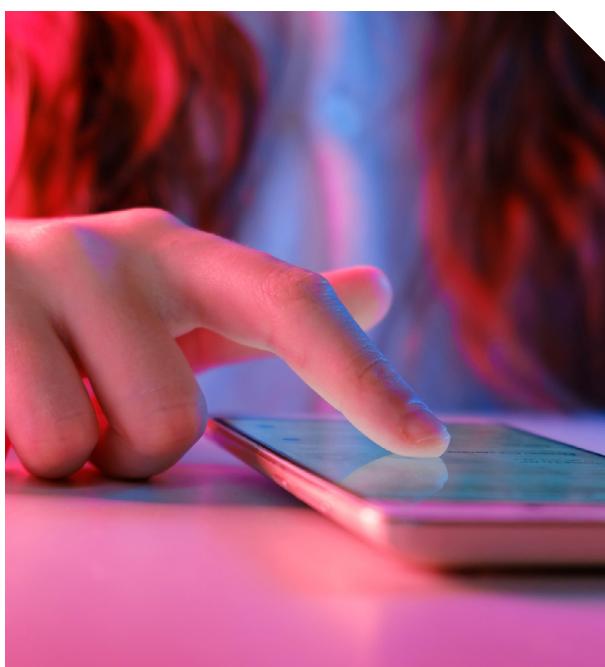
Al aplicar políticas de limitación de acceso a contenidos, el tratamiento de la información “persona autorizada a acceder” a un contenido inadecuado debe tener la menor difusión posible para evitar la detección de personas menores de edad. Es decir, el hecho de que no se ha verificado la condición de “persona autorizada a acceder” ha de ser tratado de forma que impida inferir que se está ante una persona menor, tanto en el proceso de acreditación de la autorización de acceso, como en el proceso de filtrado de contenidos, o analizar su navegación.

También hay que eliminar, desde el diseño, el impacto que podrían suponer brechas de datos personales de personas menores de edad que estuvieran en manos de servicios de verificación de terceras entidades o en los propios servicios de Internet.

¹⁰ En este sentido se establece en el considerando 89 y el artículo 28.3 de la DSA.

Una posible solución es tratar en los dispositivos en poder de las personas la información de identidad, la de “persona autorizada a acceder”, y la ejecución de políticas de limitación de acceso, sin necesidad de recurrir a los servidores de los proveedores de los servicios o a terceras entidades intermediarias. En este sentido, debe tenerse en cuenta lo relativo a las exigencias que el artículo 25.2 del RGPD con relación a la minimización de datos personales.

Ejemplo de garantía adicional podría ser que el sistema proporcione información nula, o como mucho la condición de “persona no autorizada a acceder”, en múltiples circunstancias: cuando una persona adulta ha decidido no acreditarse, cuando el sistema de protección no está presente en el dispositivo, cuando la verificación de edad ha sido fallida, cuando se trata de una persona que no cumpla los requisitos de edad, o que la condición “persona autorizada a acceder” se aplique a más casos (que dependerían del tipo de servicio). Otra garantía posible es que la navegación de las personas usuarias pueda enmascararse u ofuscarse para que no existan patrones de acceso que permitan identificar a las personas menores de edad¹¹.



PRINCIPIO 2:

La verificación de edad debe estar orientada a que las personas con la edad adecuada acrediten su condición de “persona autorizada a acceder”, y no permitir la acreditación de la condición de “menor de edad”

El propósito de los sistemas de protección no debe ser la constatación de la edad de las personas menores. La verificación de la condición de “menor de edad” supondría que se han de construir mecanismos orientados a validar la identidad de personas menores de edad, con las capacidades de acreditación de edad de las personas menores y adecuadas al uso por las personas menores.

Estos mecanismos podrían incluir análisis biométrico, perfilado, u obtención de credenciales de personas menores de edad. Todos ellos pondrían en riesgo al menor, bien al exponerlo a servicios maliciosos, bien recogiendo datos excesivos, o bien identificando a una persona como menor ante proveedores de servicios o terceras entidades intermediarias entre la persona usuaria y el contenido. Además, suponen un tratamiento de datos de personas menores de edad, que tendría que estar legitimado y cumplir con otros requisitos del RGPD relativos, entre otros, a la información específica al menor o las limitaciones a la obtención del consentimiento y realización de contratos de servicio.

Por lo tanto, los mecanismos de verificación han de estar orientados a su uso por aquellas personas que pueden acreditar tener una “autorización de acceso”, es decir, no deben ser herramientas para las personas menores de edad, que los expongan a tratamientos adicionales, ni condicionadas a que dispongan de recursos de acreditación y verificación de identidad, que sí están disponibles para personas adultas¹².

¹¹ Por ejemplo, si una persona menor pretende acceder a un contenido inadecuado que es bloqueado en una app del móvil, que se genere un patrón de tráfico de datos que no permita distinguir esta situación de una en la que el contenido no se bloquea.

¹² En casos de personas menores de edad de 18 años que se encuentren en los rangos que permitan el acceso a determinados contenidos, la obtención de tales documentos es posible y, en muchos casos, el recurso a los mismos puede estar bajo la responsabilidad de quien ejerza la patria potestad.

PRINCIPIO 3:

La acreditación para el acceso a contenidos inadecuados debe ser anónima para los proveedores de servicios de Internet y terceras entidades

El sistema de protección debe garantizar la privacidad de las personas en su navegación por Internet, no ha de exponer su identidad, especialmente la de las personas menores de edad. La aplicación de este principio ha de realizarse sin perjuicio de que, para otros tratamientos ofrecidos por el servicio de Internet, como una venta de productos, sea necesaria la identificación del cliente, o porque así lo exija el Derecho de la Unión o de los Estados Miembros. La acreditación para el acceso a contenidos inadecuados para personas menores y la acreditación de identidad ante terceras entidades son dos tratamientos distintos. El tratamiento por proveedores de servicios de Internet y terceras entidades de la acreditación de acceso a contenido inadecuado ha de ser anónimo e independiente del tratamiento para otros propósitos legítimos.

Los contenidos para personas adultas pueden ser muy variados: videos, textos, libros, audios u otros productos. Hay que tener presente que el acceso a servicios y productos por Internet no es una opción residual, sino cada vez más, la única opción para gran parte de la ciudadanía de desarrollar su vida personal y económica. Por lo tanto, cualquier registro o seguimiento de estos puede tener un gran impacto en su privacidad en general. En particular, cuando se desarrollan sistemas de identidad digital específicamente orientados al acceso a contenidos inadecuados para menores.

La pérdida de anonimidad puede ocurrir cuando se verifica la identidad ante el servicio de Internet, cuando haya terceras entidades intermediarias involucradas, o cuando un proveedor de credenciales de identidad o credenciales de acceso tenga la posibilidad de vincular la generación de credencial con el acceso efectivo a un servicio o contenido. Un caso, por ejemplo, puede darse cuando la persona usuaria se ha de acreditar ante un tercero y este a su vez envía un valor positivo o negativo, en cuanto al resultado de la autorización para el acceso, al proveedor del servicio de Internet. Otro caso se puede producir cuando la persona usuaria



se acredita ante una tercera entidad y asocia a la persona un identificador único que permite acceder a los servicios. Aunque las terceras entidades puedan ser de confianza, no se encuentran libres de la intervención de autoridades judiciales, servicios de inteligencia, brechas de datos personales, futuros cambios normativos, cambios en el accionariado de las mismas, etc. Es más, aquellas terceras entidades que presten el servicio a título oneroso tendrían la obligación de implementar la trazabilidad y la auditoría de accesos con propósitos de contabilidad y facturación.

El anonimato se perderá cuando se utilicen certificados o atributos firmados que estén asociados a identificadores únicos vinculados con una persona identificable, en vez de certificados o atributos que no puedan ser vinculados con la persona usuaria. El anonimato estará aún más expuesto cuando terceras entidades procesen rasgos biométricos (a través de fotos o videos, por ejemplo) para extraer plantillas biométricas.

El sistema de protección de personas menores de edad ante contenidos inadecuados debe evitar que terceras entidades hagan de intermediarios entre la persona usuaria y el proveedor del servicio de Internet utilizando estrategias que permitan la identificación, seguimiento de la navegación y/o perfilado de la persona. Esto se podría conseguir, por ejemplo, proporcionando herramientas para que el dispositivo personal sea el que ejecute los mecanismos de verificación sin utilizar recursos externos, incluyendo en el mismo dispositivo la ejecución de las políticas de limitación de acceso a contenidos. También podría ser una estrategia que las entidades proveedoras de identidad, cuando proporcionen la acreditación de la condición de "persona autorizada a acceder", lo hagan mediante atributos que impidan la vinculación con la persona usuaria, que en la propia solicitud del atributo no quede constancia de la intención del acceso a tales contenidos y que el proceso de solicitud no genere metainformación vinculada a la persona.

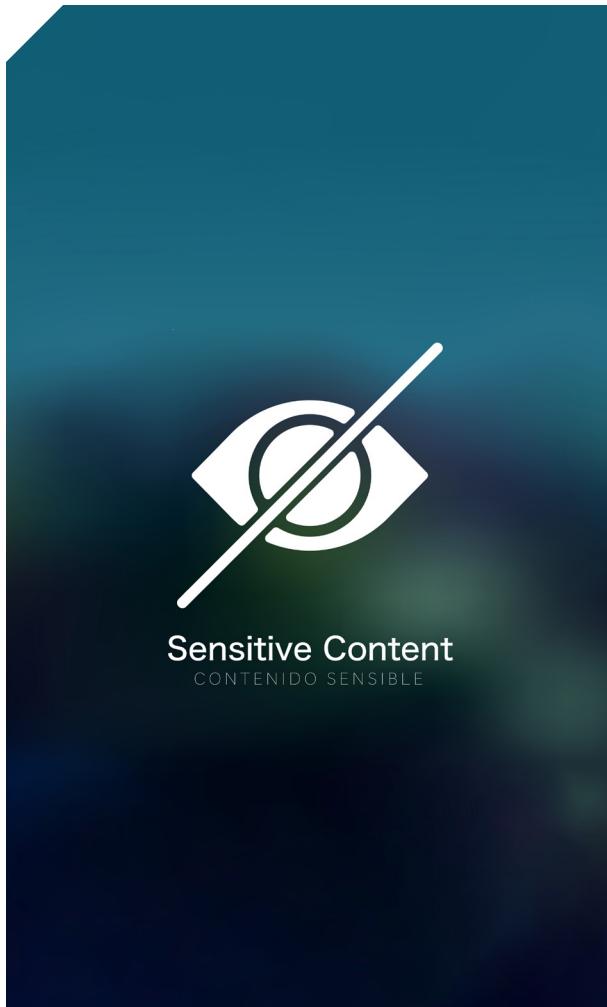
PRINCIPIO 4:

La obligación de acreditar la condición de “persona autorizada a acceder” estará limitada únicamente al contenido inadecuado

El que toda persona tenga que acreditar su condición de “persona autorizada a acceder” para cualquier tipo de contenido no cumpliría con los principios de minimización de datos, tampoco con el requisito de necesidad, e identificaría a todos las personas menores de edad que acceden a Internet por defecto. La regla general debe ser la navegación libre y anónima sin tener que acreditar ninguna condición. Únicamente en el caso de querer acceder a sitios específicos con limitación de edad, o a contenido inadecuado para personas menores, es cuando se debería requerir la condición de persona autorizada a acceder por ser mayor de 18 años, o de 14 años como, por ejemplo, en el caso de acceso a una red social.

Por ejemplo, los sistemas de protección basados en el perfilado de las personas usuarias de Internet para determinar si son personas menores, suponen un tratamiento sistemático de datos personales. Este tratamiento vincularía a cada persona que accede a Internet un análisis del histórico de actividad, relaciones, conversaciones, reacciones ante contenido, etc. El uso de técnicas de perfilado implica la supervisión continua de todas las personas incluso cuando no están accediendo a contenidos inadecuados para personas menores, y supone un tratamiento desproporcionado de datos personales.

Por lo tanto, un sistema de protección ha de permitir que una persona no tenga la obligación de definirse como “persona autorizada a acceder” en toda ocasión. En un servicio que proporciona contenidos tanto para personas adultas como contenido sin restricciones de edad, solo debería ser necesario acreditar la condición de “persona autorizada a acceder” cuando se está accediendo a contenido de personas adultas.



Un aspecto importante que debe evitarse es el de interpretar la protección ante contenidos inadecuados de forma expansiva. La protección no debe afectar sistemáticamente a contenidos culturales, de forma que se utilice para la aplicación de políticas más allá de la estricta protección de las personas menores de edad, no puede producir una limitación a la libertad, a la diversidad de pensamiento o a la labor educativa de las familias.

PRINCIPIO 5:

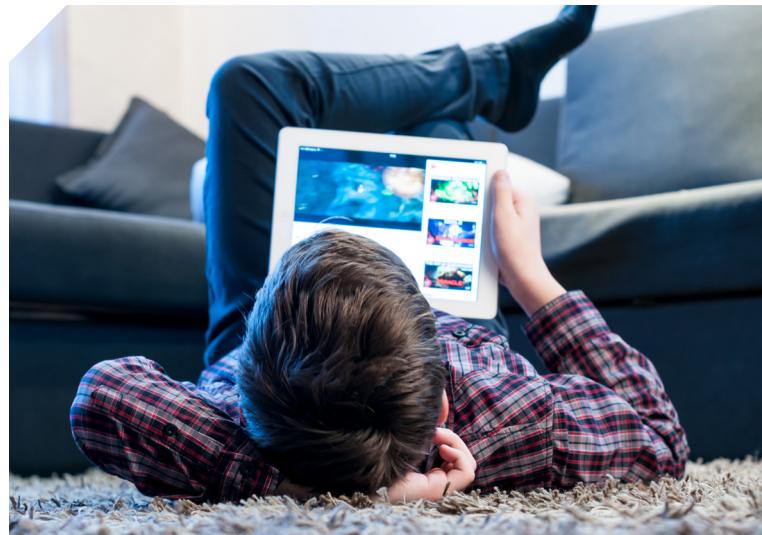
La verificación de edad se debe realizar de forma cierta y la edad categorizada a “persona autorizada a acceder”

La verificación de edad se ha de realizar de forma cierta, no probabilística o estimada, así como orientada a la categorización como “persona autorizada a acceder”. En ningún caso debe suponer la revelación concreta de la edad o de la fecha de nacimiento.

Por un lado, verificar (como está establecido en distinta normativa) es un término distinto de estimar. Además, la estimación de edad está sujeta inevitablemente a errores, sesgos y discriminación¹³, e incluso suele necesitar de la comprobación de más información sobre la persona (sexo, raza, etc.) para ser lo suficientemente precisa.

Verificar la “autorización para acceder” es distinto a dar el valor de edad o la fecha de nacimiento. La generación de atributos cuantitativos sobre la edad supone un gran riesgo en el caso de personas menores de edad, sobre todo en los casos entre 14 y 18 años, pero también un riesgo para el caso de personas de edad avanzada. Todo ello sin perjuicio de que en tratamientos con otros propósitos sea necesario recabar con precisión la edad, tratamientos que deberán ser independientes de la verificación de edad para la protección de personas menores de edad ante contenidos inadecuados.

Hay que tener en cuenta, también, que estrategias de verificación de edad de personas menores de edad por tramos (por ejemplo, menor de 14 años, y entre 14-18 años) tienen que ser implementadas de forma que no se puedan relacionar con una misma persona los intentos de acceso a contenido de adulto que sean no autorizados con los intentos de acceso con éxito a contenido entre 14-18 años, desvelando de esa forma información del tramo de edad (o incluso la condición de menor).



Por lo tanto, los mecanismos de verificación de edad deben dar un valor cierto, categorizado únicamente como “autorizado para acceder” y en ningún caso permitir que proveedores de servicios o terceras entidades traten la edad concreta de una persona, o que esta se pueda inferir.

PRINCIPIO 6:

El sistema debe garantizar que las personas no pueden ser perfiladas en función de su navegación

Para determinar que un sitio o contenido concreto solo es apto para una persona adulta es necesario algún tipo de etiquetado. Este etiquetado se puede realizar mediante una calificación “apto/no apto”, como es el caso de la aplicación de restricciones de edad en sitios web. También se puede realizar asignando múltiples etiquetas a cada contenido (“violento”, “sexo explícito”, “racista”, “consumo de sustancias tóxicas”, etc.¹⁴) para realizar una valoración de si el contenido es inadecuado para personas menores de edad. El etiquetado de sitios o contenidos podría ser realizado por revisores humanos o de manera automática¹⁵, y de forma estática o mediante análisis dinámico (esto último, por ejemplo, en chats).

¹³ Algunos de los sistemas estimativos no tienen la misma precisión en función del color de la piel del sujeto.

¹⁴ De igual forma que se califican las películas en los servidores de video o plataformas de streaming.

¹⁵ Como, por ejemplo, con herramientas de inteligencia artificial.

En algún punto entre el servidor, que proporciona el contenido, y la persona usuaria, que solicita el contenido, se ha de ejecutar la política de limitación de accesos. La ejecución de dicha política en los propios servidores, o en tercera entidades intermediarias entre la persona usuaria y los sitios web, conlleva riesgos para la privacidad. Entre estos riesgos están los que se derivan del perfilado o monitorización de la persona que accede, que en este tipo de contenidos podrían incluir categorías especiales de datos. El añadir varias etiquetas al contenido accedido por una persona podría suponer construir un perfil que la etiquete en función de los contenidos a los que ha accedido. El riesgo será mayor cuando una misma tercera entidad filtre todo el tráfico correspondiente a la misma persona. El perfilado y la monitorización, en particular con categorías especiales de datos, además de tener que levantar su prohibición de tratamiento con carácter general y de necesitar una legitimación, es un tratamiento de alto riesgo que tendría que superar una evaluación de proporcionalidad.

La ejecución de las restricciones de acceso a sitios web de forma local en los dispositivos de las personas usuarias de Internet permitiría eliminar los riesgos de perfilado o monitorización. El filtrado de contenidos de forma local es viable desde el punto de vista técnico, como demuestran los sistemas existentes de protección contra el malware o algunas herramientas utilizadas para control parental. La protección local mediante la comprobación del atributo “persona autorizada a acceder”, incluso el etiquetado dinámico en local, sería posible en los propios dispositivos. O bien en sus sistemas operativos o mediante la adaptación de las aplicaciones (apps) de los servicios de Internet (ya sean redes sociales, buscadores, chats, etc.). Incluso permite desarrollar estrategias más eficaces como la aplicación de criterios regionales, culturales o familiares en el proceso de etiquetado e interpretación de las etiquetas. Sin perjuicio de la utilización de las anteriores estrategias, se podría realizar el etiquetado dinámico, incluso el filtrado, en routers domésticos o de centros educativos. El objetivo sería siempre el mismo, que se ejecute la protección en función de la edad con minimización de los datos de las personas que se tratan para evitar el riesgo de localización de personas menores o de perfilado general.

PRINCIPIO 7:

El sistema debe garantizar la no vinculación de la actividad de una persona entre distintos servicios

Un sistema que permite vincular la actividad de la persona usuaria de Internet en diversos servicios puede llegar a identificarla y perfilarla, infiriendo características comportamentales del sujeto interesado.

Los sistemas que, para la verificación de edad, utilizan códigos únicos para utilizar entre múltiples plataformas permiten el seguimiento de la persona entre distintos servicios. De igual forma ocurre con los sistemas basados en atributos firmados que incluyen identificadores únicos. Hay que tener en cuenta que la interacción de la persona usuaria con el servicio suele ser más compleja que solo el acceso a contenidos, por ejemplo, puede permitir comentarios o conversaciones, o en algunos servicios concretos se requerirá la identificación de la persona (por ejemplo, en sitios de juego online). Cuando los sitios web o los servicios que ofrecen contenidos calificados como inadecuados para personas menores se extiendan a múltiples ámbitos de la vida digital, la vinculación de los accesos puede permitir, no solo un perfilado muy intrusivo, sino incluso desvelar más atributos de identificación.

Esto también puede ocurrir con cualquier tipo de identificador único que se reutilice entre servicios, plataformas o contenidos, como podrían ser los patrones biométricos¹⁶. Incluso se pueden dar situaciones más complejas, cuando el contenido de personas adultas esté vinculado al acceso a determinados locales y la descarga de credenciales para la verificación de edad recoja información de geolocalización, por ejemplo.

Por lo tanto, en el sistema se han de evitar los identificadores únicos comunes a distintos servicios y la utilización de mecanismos que desvelen metadatos que permitan identificar al usuario tanto de manera directa como con la agregación de informaciones adicionales.

¹⁶ Ya se ha demostrado que patrones generados utilizando distintos sistemas biométricos pueden vincularse entre sí.

PRINCIPIO 8:

El sistema debe garantizar el ejercicio de la patria potestad por los progenitores

Cualquier sistema de protección de personas menores de edad ante contenidos inadecuados debe velar por el derecho de quienes ejerzan la patria potestad a participar activamente en la educación de las personas menores a su cargo, manteniendo el respeto a su diversidad cultural, política y de creencias, así como de las condiciones particulares del menor. La protección ante determinados contenidos va a formar parte de esa educación.

Las familias, las instituciones educativas, las asociaciones y fundaciones de protección del menor, los investigadores y expertos en educación y el Estado tienen el derecho a participar activamente en el establecimiento de los criterios de lo que consideran inadecuado. No cabe que sea una entidad comercial quien dicte los contenidos a los que una persona menor puede acceder. La realidad es que, en muchos casos, podría primar el interés económico de dichas entidades y la monetización de los datos de las personas menores de edad, permitiendo e incluso fomentando contenidos inadecuados ellas.

Por ello, los sistemas han de establecer las políticas teniendo en cuenta a las familias, o bien directamente, o a través de sus representantes, asociaciones y fundaciones orientadas a la protección de las personas menores de edad.



PRINCIPIO 9:

Todo sistema de protección de menores de edad ante contenidos inadecuados debe garantizar los derechos fundamentales de todas las personas en su acceso a Internet

La importancia que tiene la vida digital, potenciada cada día desde todas las instituciones, implica que cualquier limitación o control sobre el desarrollo digital, si no es aplicado correctamente, pueda suponer una limitación de los derechos fundamentales, tanto de las personas adultas como de las personas menores de edad.

Así, se produciría una intromisión al derecho fundamental a la intimidad personal siempre que los sistemas de protección de personas menores de edad ante contenidos inadecuados permitan vincular un contenido con una persona identificable, permitan perifilar sus aspectos íntimos, o vincularlos con otra información extraíble de los metadatos que se generan en las entidades intervenientes del sistema de protección. Incluso, la mera declaración de que una persona ha querido acceder a contenido inadecuado para personas menores puede constituir una intrusión a su intimidad.

Con relación al derecho a la libertad personal, de información, de pensamiento, de conciencia y de religión, todos ellos derechos también de las personas menores de edad, un sistema de protección no puede coartar el acceso a determinados contenidos por un exceso de celo, o por la aplicación de determinados valores, intereses o creencias. Hay que tener en cuenta que en el contenido inadecuado para personas menores de edad podrían incluirse libros, opiniones o material educativo. Cuando los sistemas sean tan intrusivos para la privacidad que generen autocensura se podrá estar en casos de limitación de la libertad de información. La autocensura también aparecerá cuando el deseo de acceso a contenidos inadecuados tenga que acreditarse ante terceras entidades. También en el caso en que se estén utilizando sistemas probabilistas o con sesgos que impidan a determinadas personas, por ejemplo, aquellas en edades límite o pertenecientes a minorías, el acceso a contenidos a los que tienen derecho a acceder.

En el mismo sentido, y como se ha comentado anteriormente, el concepto de contenido inadecuado para personas menores no debe tener un carácter expansivo que regule todos los aspectos de los contenidos digitales, como los contenidos culturales, ni que sea establecido por servicios comerciales o Estados atendiendo a ideología.

Con relación al derecho a la integridad personal, es evidente que la posibilidad de que los sistemas permitan localizar personas menores de edad a través de Internet puede suponer un riesgo físico para su integridad personal, pero también puede posibilitar la identificación de personas adultas en situación de vulnerabilidad, especialmente psicológica, que estén siendo perfilados por sus hábitos con relación a ciertos contenidos.

Con relación al derecho a la propia imagen, se restringirían los derechos de los ciudadanos en aquellos sistemas de protección que almacenan o tratan la imagen personal mediante sistemas de reconocimiento facial por el proveedor del servicio de Internet o por terceras entidades, cuando técnicamente no es necesario realizar dicho tratamiento, y cuando podría ejecutarse, en cualquier caso, en los dispositivos bajo el control de las propias personas usuarias.

El derecho a la capacidad de obrar, como la aptitud para realizar de forma válida actos jurídicos, ejercitar derechos y asumir obligaciones, está muy vinculado a la identidad y la posibilidad de identificación de la persona. Actualmente, gran parte de la capacidad de obrar se debe desarrollar en el entorno digital. Por lo tanto, se podría vulnerar este derecho en sistemas que limiten la capacidad de obrar en función de condiciones de un servicio y sin tener una fundamentación jurídica¹⁷.

Con relación al derecho a la no discriminación, entre otros ejemplos, estos sistemas no han de impedir el acceso a contenidos a las personas adultas de edad avanzada o a cualquier otro colectivo simplemente por la elección de determinadas opciones tecnológicas que no acepten la diversidad. Tampoco se ha de permitir que los sistemas de verificación o el acceso a información adicional de identidad permitan o implementen sesgos por razón de género, raza, edad, nacionalidad, etc.

PRINCIPIO 10:

Todo sistema de protección de personas menores de edad ante contenidos inadecuados debe tener definido un marco de gobernanza

Todo sistema para la protección de personas menores de edad ante contenidos inadecuados debe tener definido un marco de gobernanza para garantizar el cumplimiento de estos principios, la protección de los derechos fundamentales y articular la participación de los que ostentan la patria potestad, las instituciones educativas, las asociaciones y fundaciones de protección del menor, los investigadores y expertos en privacidad, el Estado o los proveedores tecnológicos y de servicios de la sociedad digital, entre otros.

Para ello, el marco de gobernanza ha de asegurar que el sistema de protección se implemente y se despliegue con tecnologías que preserven la privacidad. También que cumpla con un nivel mínimo de eficacia, asumiendo que ningún sistema tecnológico es perfecto. Dicha eficacia ha de ser evaluada de forma objetiva y con espíritu crítico, incluyendo en el análisis los efectos colaterales en las personas y la sociedad. El sistema, en su uso y su forma de operar, ha de ser transparente para las personas usuarias, en particular con relación a la anonimidad de la navegación y a los criterios de limitación de contenidos, además de auditável de forma efectiva por autoridades y terceras entidades independientes.

Un sistema que no tenga una mínima eficacia no cumplirá con los requisitos de idoneidad del tratamiento. Un ejemplo claro son aquellos sistemas basados en la declaración de edad realizada por la propia persona usuaria que solo han servido para dar garantías jurídicas puramente formales a los proveedores de servicios de Internet. Otro ejemplo es el de algunos de los sistemas de control parental actualmente en servicio, que en muchos casos no se han validado correctamente en su robustez frente a la manipulación. También aquellos sistemas que generen desconfianza y sean rechazados por la ciudadanía.

¹⁷ Artículo 322 del Código Civil

Los efectos colaterales que la aplicación de los sistemas de protección de personas menores de edad ante contenidos inadecuados pueda tener han de ser evaluados con sentido crítico. En particular, hay que evaluar qué impacto tendrán las brechas de datos personales que se puedan producir en cada una de las entidades intervenientes. Esto será particularmente grave cuando servicios de terceras entidades, tanto de verificación de identidad o de edad, de acreditación de la condición de “persona autorizada a acceder”, así como de filtrado de contenidos sufran brechas de seguridad, corrupción o chantaje para el robo de credenciales o intervención por Estados.

Otros efectos colaterales se pueden producir cuando los sistemas de protección discriminen a personas que, por cualquier razón, no puedan o no sean capaces de utilizar esos sistemas, o bien los sistemas no interactúen correctamente con ellos por incorporación de algún sesgo. En particular, con relación a las personas con diversidad funcional o las personas adultas mayores.

El sistema de protección requiere disponer de distintas opciones, solapadas o no, que den respuesta a las distintas plataformas y situaciones sociales. También ha de contemplar su integración con los presentes y futuros sistemas de gestión de identidad nacionales y europeos, como es el caso de la Cartera Digital establecida en la propuesta eIDAS¹⁸.

Un aspecto clave para la eficacia es la confianza de las personas usuarias, a las que no se les puede exigir una fe ciega en los servicios tecnológicos. Por ello, los sistemas han de configurarse para que puedan ser auditables tanto por autoridades supervisoras como por centros de investigación independientes con plena competencia para realizar dicha tarea. La auditabilidad, de estos sistemas y de las plataformas sobre las que se ejecutan, ha de permitir obtener evidencias de que no existe manipulación, falta de diligencia, que no es posible ni se está realizando perfilado o seguimiento de la actividad de las personas, que no existe discriminación, que no son sistemas vulnerables y que se aplican todos los principios, derechos y obligaciones establecidos en el RGPD, en particular el de responsabilidad proactiva. La concentración en

unos pocos servicios de terceras entidades que no son accesibles a supervisión independiente para su auditoría aumenta los impactos de las brechas, los efectos colaterales y la dificultad de una supervisión efectiva.

IV. CONCLUSIONES

La protección de las personas menores de edad compete a la sociedad en su conjunto. Todos sus intervenientes deben conformar la red de cuidado, defensa, ayuda y acompañamiento del menor en el camino para su desarrollo como persona adulta. La protección del menor es compleja, y se extiende a muchos más aspectos que el filtrado de los contenidos en Internet. El buscar simplificaciones basadas en “solucionismos tecnológicos” que ignoran disfunciones sociales básicas podría agravar los problemas que éstas originan.

La tecnología puede ser un gran apoyo en la defensa del menor si se integra en un marco general de protección con implicación de todos los intervenientes sociales: las familias, las autoridades, las instituciones educativas, las asociaciones y las fundaciones de protección del menor, los investigadores y expertos en privacidad, los proveedores tecnológicos y los servicios de la sociedad digital, etc.

La tecnología perfecta no existe. Pero sí existe la tecnología adecuada que actúa armoniosamente con los elementos educativos, culturales, sociales, de responsabilidad y de seguridad para proteger de forma efectiva el interés superior del menor y los derechos fundamentales de la ciudadanía.

La educación de las personas menores de edad, en particular en el entorno digital, y la selección de contenidos adecuados es una responsabilidad compartida entre las familias, los Gobiernos que deben impulsar políticas públicas eficaces y normativa de protección en este ámbito y la industria. Es urgente la adopción de medidas de protección a la infancia y la juventud en el entorno digital, en la línea de las acciones planteadas en el Pacto de Estado ya mencionado.

¹⁸ Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea.



www.aepd.es

X AEPD_es

in AEPD

O @aepd.es