Preguntas frecuentes (FAQ)

sobre las pruebas de concepto (PoC) de sistemas de verificación de edad y protección de personas menores de edad ante contenido inadecuado

Diciembre 2023

ÍNDICE

1. ¿Por qué se propone el decálogo de principios y las pruebas de concepto asociadas?

El acceso a Internet ya no es una opción completamente libre, sino que se ha convertido en una obligación para el desarrollo de la vida personal y económica de la ciudadanía.

Las personas menores han de estar protegidas en todos los aspectos. Los derechos fundamentales de todas las personas usuarias de Internet también, independientemente de su edad. La protección del menor no puede ser una excusa para vulnerar derechos fundamentales. Los derechos fundamentales, en particular de protección de datos, no se pueden usar como excusa para no proteger a las personas menores.

Un sistema de verificación de edad puede tener un gran impacto en la intimidad de las personas, en su derecho a obrar, pensar, informarse y educarse libremente, y en la vigilancia y supervisión de cada una de sus acciones.

La AEPD está obligada a proteger los derechos fundamentales de los ciudadanos con relación a la protección de datos.

Los principios establecen la manera de conciliar el interés superior del menor y los derechos fundamentales de la ciudadanía, y las PoC demuestran que es posible llevarlos a la práctica en escenarios reales, probando su viabilidad.

2. ¿Cuál es la principal ventaja de las PoC propuestas?

Las principales ventajas son la protección integral del menor, la garantía de los derechos fundamentales de los interesados, la universalidad, la auditabilidad y transparencia real, y la idoneidad de un método que genere confianza para que su uso sea extendido.

Otra ventaja es que son sistemas exportables a todo el mundo y que, a la vez, se alinean con los proveedores de identidad españoles y europeos que garantizan la identidad como un derecho universal.

3. ¿La App de verificación de edad la va a proporcionar la AEPD?

La AEPD es una Autoridad de Protección de Datos, es decir, una autoridad de control. Entre sus funciones no está la de proporcionar este tipo de soluciones o aplicaciones. Las aplicaciones desarrolladas para las pruebas de concepto son sólo prototipos o demostradores, no nacen con la intención de ofrecerse a la ciudadanía.

La *app* de verificación no es un nuevo mecanismo para proveer identidad. La identidad es un derecho de la ciudadanía, que en España está garantizado por el Estado a través del Ministerio de Interior o de otras entidades.

La *app* de verificación ha de estar proporcionada por entes públicos y/o privados con diferentes modelos y motivaciones para hacerlo. Y la AEPD tiene entre sus competencias que se cumplan todas las garantías de protección de datos y, por lo tanto, los derechos y libertades de la ciudadanía.

Al menos la Fábrica Nacional de Moneda y Timbre (FNMT) ya se ha comprometido a desarrollar la *app* de verificación de edad para uso público.

4. Verificar la edad ¿supone que los servicios de Internet deben conocer la identidad de la persona que accede a contenidos? o al menos ¿conocer qué edad tiene?

El propósito de la protección del menor es que éste no acceda a contenidos inadecuados, no que los proveedores de Internet conozcan la edad de las personas que acceden a contenidos o incluso su identidad. Aunque a primera vista parece que ambos son

equivalentes, el segundo escenario implicaría una forma intrusiva de conseguir el propósito real del tratamiento.

El decálogo, demostrado con las PoC, establece que no es necesario que los proveedores de contenidos en Internet deban conocer la identidad o la edad de las personas usuarias. La normativa tampoco establece que exista la legitimación para realizar ese tratamiento, ni por los proveedores de contenidos, ni por terceras entidades, cuando no sea necesario para la verificación de edad.

5. SI UN MENOR O UNA PERSONA ADULTA ACCEDE A UN CONTENIDO SERVIDO DESDE UN SERVIDOR FUERA DE EUROPA ¿DESVELA SU IDENTIDAD O SU EDAD?

Con los principios recogidos en el decálogo, la identidad se trata de forma independiente a la verificación de edad. En las PoC el tratamiento de verificación de edad se realiza en las *apps* instaladas en el propio dispositivo, sin acceder a servidores externos, por tanto, ninguna información se desvelaría a servidores externos, ni dentro ni fuera de Europa.

6. LA AEPD ¿PROPONE EN LAS PoC UN NUEVO SISTEMA DE GESTIÓN DE LA IDENTIDAD DIGITAL?

No. La AEPD muestra en las PoC que es posible independizar la verificación de edad de los proveedores de identidad, de forma que no sea necesario crear nuevos sistemas de identidad digital. Es suficiente con los proveedores de identidad que ya existen para el mundo físico o digital, fomentando la neutralidad tecnológica y el libre mercado de opciones. Por ello la solución propuesta en las PoC es compatible con un esquema basado en la cartera digital europea definida en eIDAS2 o con los medios de identificación nacionales u universales, como el pasaporte, ya disponibles.

7. CON LAS PoC PROPUESTAS, ¿DEBE UNA PERSONA DECLARAR ANTE UNA TERCERA ENTIDAD SU DESEO DE ACCEDER A CONTENIDOS DE ADULTOS?

No. Las PoC propuestas desvinculan la verificación de la edad de la declaración del propósito de acceder a contenidos de adultos (que se hace en el navegador o en una aplicación específica para el acceso a contenidos de un determinado proveedor, por ejemplo, de una red social). No es necesario un proceso en el que la persona se tenga que identificar para el propósito concreto de acceder a contenidos de adultos. Tampoco declarar ante una entidad tercera que se tiene ese propósito.

De esta forma, la decisión de acceder a contenidos de adulto se gestiona exclusivamente dentro del dispositivo de la persona usuaria, en el que se trata su condición de persona "autorizada a acceder", y así se crea confianza y el sistema cumple el principio de idoneidad, ya que, si no se usara ampliamente, no sería de utilidad.

8. ¿EL SISTEMA PROPUESTO EN LAS PoC PERMITE VINCULAR LA NAVEGACIÓN DE LA PERSONA USUARIA ENTRE DISTINTOS SERVICIOS?

No, no lo permite. La utilización de certificados de uso general, o de sistemas biométricos directamente en los servidores del proveedor de contenidos o de terceras entidades, sí lo permitiría, desvelando información sobre la persona usuaria y permitiendo su perfilado.

Todos los sistemas basados en una entidad tercera intermediaria, por ejemplo, conocen la navegación del usuario y la vinculan además con la verificación de su identidad, siendo muy intrusivos con la privacidad de las personas.

Pero en las PoC este tipo de vinculación no es posible porque no se sale del dispositivo de la persona usuaria para resolver la verificación de edad, y además esta verificación no conlleva la identificación de la persona.

9. ¿No son válidas soluciones adoptadas en otros países que hacen de intermediario entre el usuario y el servicio al que se quiere acceder?

Se han adoptado soluciones de verificación de edad que no impiden la localización de menores y la recogida masiva de datos. Algunas de ellas son muy intrusivas para la privacidad y monetizan los datos de navegación de las personas usuarias, las perfilan, las identifican y crean sistemas paralelos de identidad digital.

Las soluciones más populares basadas en terceros de confianza que actúan como intermediarios entre las personas usuarias de Internet y los contenidos a los que desean acceder, podrían implicar serios riesgos para los derechos y libertades de todas las personas en Internet. En particular, algunas de ellas podrían suponer un tratamiento de datos de menores con riesgos para ellos. Lo mismo ocurre con otras soluciones, ya disponibles en el mercado, que se basan en otros diseños o arquitecturas pero que también implican ese tipo de riesgo. Ninguna de las soluciones analizadas por la AEPD cumple con el decálogo de principios propuesto en su totalidad, cuando se ha demostrado que es posible gracias a las PoC.

La urgencia en la aplicación de sistemas de verificación de edad no puede ser la excusa para exponer a mayores riesgos a los menores, vulnerar derechos fundamentales, y construir sistemas paralelos de gestión de la identidad que no preserven la privacidad y que conviertan la identidad en un servicio, cuando es un derecho de la ciudadanía.

10. ¿Qué pasa cuando un menor no tiene un mecanismo para proveer su identidad?

El fundamento de los principios y la solución propuesta en las PoC es que el menor ha de estar libre de tener que ser identificado o sometido a supervisión. Por lo tanto, no hay que proporcionar a las personas menores mecanismos de identificación, no los necesitan.

Son las personas que están autorizadas a acceder a los contenidos las que han de utilizar los mecanismos que ya tienen para acreditar su edad.

11. ¿Un sitio de adultos no puede conocer la identidad de la persona usuaria?

Un sitio de adultos tendrá la legitimidad para conocer la identidad de la persona usuaria en el marco de un contrato de servicios con dicha persona, siempre que conocer determinados aspectos de su identidad sea imprescindible para establecer dicho contrato, y solo cuando sea necesario. También cuando así lo exija la ley.

Pero dicho proceso de identificación es distinto del proceso de verificación de edad que permite proteger a un menor ante los contenidos inadecuados ofrecidos en dicho sitio. Constituyen dos tratamientos distintos que han de ser independientes.

12. La acreditación de la edad de la persona usuaria mediante uso de certificados, carteras digitales, códigos QR u otros métodos ¿no podría implicar la exclusión de ciertas personas del uso de la solución?

La orientación de los principios es que se ha de permitir el uso de distintos proveedores de identidad, que las personas puedan elegir cuál es más adecuado en su caso, que estos proveedores no detecten que se desea acceder a un servicio de adulto y que no les identifiquen ante servicios de Internet. Todo ello basado en los derechos que tienen los

ciudadanos a su propia identidad y accesible tanto a ciudadanos europeos como del resto del mundo. Tienen que ofrecerse de forma simultánea para garantizar la confianza y la no discriminación digital. De esta forma el derecho a obrar en Internet no queda mediatizado por un conjunto limitado de servicios privados, sino que se garantiza como derecho en el mundo digital.

Por este motivo en las PoC se han separado los mecanismos de provisión de identidad de los de verificación de edad, en dispositivos Android, iOS y Windows, y se han utilizado diferentes medios para que se pueda verificar la edad de las personas usuarias de manera cierta: pasaporte, DNI/TIE, códigos QR, o emuladores de la cartera digital europea.

13. ¿Cuándo podría estar completamente operativo todo el sistema de protección del menor ante contenidos inadecuados?

Estos sistemas deberían estar ya en funcionamiento.

Los proveedores de contenidos y servicios, en colaboración con los intervinientes en el ecosistema de Internet y con la sociedad civil, disponen de una guía para el cumplimiento del principio de responsabilidad activa del RGPD y la aplicación de la protección de datos por defecto y desde el diseño.

14. ¿Los mecanismos presentados por la AEPD en sus PoC son los únicos permitidos?

Las PoC son una demostración de que existen formas de cumplir los principios y de que, por lo tanto, la AEPD puede exigir el cumplimiento de dichos principios. Una solución que siga lo señalado en las PoC respetando los principios será tan válida como cualquier otra aproximación que cumpla con los mismos principios.

Otros mecanismos y soluciones que cumplan los principios recogidos en el decálogo y que, por lo tanto, garanticen el cumplimiento de la normativa de protección de datos, y así la protección del interés superior del menor y los derechos y libertades de la ciudadanía, serán considerados adecuados desde el punto de vista de la AEPD.

15. ¿Se ha tenido en cuenta que habría que realizar un desarrollo adicional para que las PoC se conviertan en una solución que se pueda utilizar en Internet?

La AEPD ha estado trabajando en la definición de los principios recogidos en el decálogo, el diseño y la implementación de las PoC, con un gran esfuerzo de interlocución con múltiples intervinientes en el marco de un Grupo de Trabajo de Verificación de Edad creado en marzo de 2023 en el que han participado la Comisión Nacional de los Mercados y la Competencia, la Fábrica Nacional de Moneda y Timbre, el Ministerio del Interior y el actual Ministerio de Transformación Digital.

El papel de la AEPD, que es el de la autoridad de control, es el de dar paso a todo el ecosistema que forma la industria de Internet para asumir la responsabilidad de implementar los sistemas definitivos. Todo el material generado y puesto a su disposición les servirá de guía y orientación para que puedan aplicar los recursos necesarios.

16. En las pruebas de concepto hay aspectos que están pendientes de definir o mejorar. ¿Cuándo lo va a hacer la Agencia?

La AEPD es una Autoridad de Protección de Datos, es decir, una autoridad de control. Estas PoC son un demostrador de que se pueden cumplir los principios propuestos, no van a convertirse en productos finales, es decir, la AEPD no pretende por sí misma poner estas

soluciones en producción, sino impulsar que sea posible. Esto será una tarea de la industria, entes públicos y la sociedad civil; que además podrán proponer soluciones mejores.

17. ¿CADA VEZ QUE UNA PERSONA ADULTA QUIERA ACCEDER A CONTENIDO ETIQUETADO PARA PERSONAS ADULTAS VA A SER NECESARIO QUE SE ESCANEE UN CÓDIGO QR, SE ACCEDA A UNA CARTERA DIGITAL O SE LEA UN DOCUMENTO OFICIAL? ¿ESTE TIPO DE PROCESOS NO VAN A ENTORPECER LA NAVEGACIÓN?

Las soluciones propuestas hasta ahora en el mercado, en las que las personas usuarias se tienen que autenticar ante un servicio de una entidad tercera, a través de Internet y sin garantías de tiempos de respuesta, sí pueden ser limitantes.

El decálogo no realiza propuestas a bajo nivel con detalles técnicos de diseño o implementación, por lo que se puede cumplir con soluciones que requieran que la persona usuaria se dé de alta con su identidad solo una vez o con soluciones que requieran comprobar los atributos de identidad y/o edad mucho más frecuentemente. Probablemente los proveedores de las aplicaciones de verificación de edad intenten llegar a un equilibrio entre fiabilidad de la solución y usabilidad, ya que, efectivamente, pedir pruebas constantemente entorpecería la navegación por contenidos para personas adultas.

18. ¿NO ES LA AUTENTICACIÓN BIOMÉTRICA EN EL PROPIO MÓVIL UN MECANISMO POCO PRECISO?

La autenticación biométrica realizada por la propia persona usuaria en su propio dispositivo sin recurrir en ningún caso a recursos o servidores externos es una de las opciones que tendría que ofrecer una solución comercial para dar la oportunidad de comprobar que la persona usuaria que recupera un dato de edad de un documento de identidad oficial es la persona propietaria de dicho documento, comparando la fotografía recuperada de dicho documento con un selfi obtenido en tiempo real. Se ha incluido este caso de uso en las PoC para mostrar que se han de permitir mecanismos alternativos de forma simultánea que garanticen la confianza y la no discriminación digital, es decir, es uno de entre todos los posibles.

Aun así, la autenticación biométrica en los recursos del propio dispositivo móvil, en un tratamiento puramente personal, puede tener el rendimiento suficiente para muchas situaciones y personas usuarias. De no ser así, se tendría que recurrir a otro de los mecanismos posibles.

19. ¿POR QUÉ UN SISTEMA ESTIMATIVO NO SE CONSIDERA ADECUADO EN EL DECÁLOGO? ¿NO ES MENOS INVASIVO PARA LA PRIVACIDAD?

Existen diferentes razones que hacen que un sistema estimativo no sea adecuado desde el punto de vista de la protección de datos.

La mayoría de los que se encuentran en el mercado actualmente se han implementado de forma que incumplen la mayor parte del decálogo: permiten identificar menores, identifican a las personas adultas, recogen los hábitos de navegación, perfilan a las personas usuarias, dificultan la transparencia y la auditabilidad, implican sesgos y limitaciones no fundamentadas al derecho de la capacidad de obrar, permiten detectar a personas perteneciente a otros colectivos vulnerables, etc.

Por otro lado, sistemas estimativos ejecutados en el propio dispositivo (sin enviar datos a servidores externos) se encontrarían lejos de cumplir con el requisito de “verificación” fehaciente de la edad recogido como obligación en la normativa actual, en cuanto resultan sistemas probabilistas.

20. ¿CÓMO SE EVITA QUE LAS PERSONAS USUARIAS EXPLOTEN LAS VULNERABILIDADES DE LA APP DE VERIFICACIÓN? ¿O QUE SE ACABEN INSTALANDO VERSIONES MALICIOSAS DE ESTAS *APPS* DE VERIFICACIÓN DE EDAD? ¿SE PODRÍA CREAR UNA APLICACIÓN "FALSA" DE VERIFICACIÓN DE EDAD QUE PERMITIERA A UNA PERSONA MENOR MANIFESTARSE SIEMPRE COMO PERSONA ADULTA?

Por supuesto, un mecanismo de gobernanza del sistema global, como en todo sistema que se ha de implementar de forma segura, ha de tener presente que la seguridad al 100% no existe, y menos en dispositivos móviles. En particular, se han de gestionar de manera adecuada las vulnerabilidades o debilidades que seguro van a aparecer.

Obviamente quien proporcione estas *apps* debe mantenerlas adecuadamente dentro del marco de gobernanza, con actualizaciones que resuelvan las debilidades o vulnerabilidades que se descubran cuando ya estén en uso. Hay que plantearse que el marco de gobernanza de los sistemas de verificación de edad y protección ante el acceso a contenidos inadecuados, por su impacto, se incorporen en los procesos de notificación de incidentes y los procesos de supervisión establecidos en el marco de la Directiva NIS2.

En cuanto a las *apps* maliciosas, se pueden establecer mecanismos criptográficos que garanticen la legitimidad de las *apps* de verificación de edad (o de su origen) como ya se hace en el caso de otras que necesitan confianza (*apps* bancarias y de pago, herramientas de chat y mensajería, etc.).

21. ¿CÓMO SE GARANTIZA QUE TODOS LOS DATOS RELACIONADOS CON LA VERIFICACIÓN DE EDAD O EL ACCESO A LOS CONTENIDOS PARA PERSONAS ADULTAS NO ACABAN EN MANOS DE UN TERCERO QUE ACABE VIGILANDO O PERFILANDO A LAS PERSONAS USUARIAS? A TRAVÉS DEL FABRICANTE DEL DISPOSITIVO, DEL SISTEMA OPERATIVO, DE OTRAS *APPS*. LOS TELÉFONOS SON MUY INSEGUROS.

Es cierto que existen debilidades y vulnerabilidades en los teléfonos móviles que pueden llegar a exponer la privacidad de las personas usuarias. Hay que seguir avanzando para que la privacidad y la seguridad de los dispositivos se incremente significativamente.

En caso contrario, nada de lo que se está ejecutando actualmente en los dispositivos será ni privado ni seguro. La solución propuesta podría garantizar los mismos niveles de seguridad y privacidad que las *apps* en las que ahora ya confían las personas usuarias para realizar pagos, transacciones bancarias, comunicaciones, acceso a contenidos, etc. Se seguirían, como mínimo, las mismas prácticas y recomendaciones que ya se siguen actualmente para todas estas *apps*.

22. ¿QUIÉN VA A ETIQUETAR LOS CONTENIDOS PARA PERSONAS ADULTAS? ¿SE PUEDE CONFIAR EN ESTAS ETIQUETAS, QUIÉN LAS AUDITA? ¿ESTE MODELO DE ETIQUETAS ES ESCALABLE? ¿Y CÓMO SE AJUSTA A LA RELIGIÓN O A LA CULTURA DE CADA PAÍS, POR EJEMPLO?

La AEPD ha elaborado una nota técnica con una propuesta para este sistema de etiquetado basada en Age.xml, que surge del proyecto europeo MIRACLE. Esta solución es escalable, se puede ajustar a diferentes culturas y religiones y se basa en la autoevaluación (el etiquetado lo realizan los propios proveedores), que podría ser controlada o matizada por diferentes comités y comisiones formadas por autoridades, la industria, asociaciones de padres, etc.

Es el sistema que ya se utiliza, por ejemplo, en Alemania. Otros sistemas de etiquetado podrían ser válidos siempre y cuando fueran compatibles con el decálogo de principios propuestos.

23. ¿PERMITIRÍA QUE UNA FAMILIA IMPLEMENTASE MEDIDAS DE PROTECCIÓN ESPECÍFICAS EN CASO DE UN MENOR QUE NECESITA UNA PROTECCIÓN ESPECIAL?

El universo de Internet ha permitido la expansión de nuevos problemas psicológicos en los menores, como conductas obsesivas, trastornos de la alimentación, etc.

El sistema propuesto en las PoC, al realizar el filtrado de contenidos en el dispositivo, permitiría que los proveedores de contenidos incluyan en sus *apps* configuraciones para que la familia pueda incorporar protecciones adicionales sobre contenidos específicos, complementando (no sustituyendo necesariamente) las herramientas de control parental.

24. ¿SE LIMITA ENTONCES LA RESPONSABILIDAD DE LOS PROVEEDORES DE CONTENIDOS AL ETIQUETADO DE LOS CONTENIDOS QUE OFRECEN?

No, estos proveedores tienen que asumir sus responsabilidades en el tratamiento de datos completo que permite proteger a las personas menores de edad ante contenidos inadecuados.

En este tratamiento, el etiquetado de contenidos es una parte esencial, pero los proveedores de contenidos tienen que asumir también su parte de responsabilidad en lo que se refiere a los mecanismos de verificación de edad o a la ejecución de las políticas de acceso. Se trata de una responsabilidad compartida en un ecosistema complejo en el que participan otros operadores como pueden ser los proveedores de identidad, de *apps* de acceso a contenidos o navegadores, de soluciones de verificación de edad, etc. Pero esta complejidad no es razón para eludir dicha responsabilidad.

El modelo de gobernanza ha de garantizar la asunción de responsabilidades.

25. EN LA SOLUCIÓN PRESENTADA EN LAS PRUEBAS DE CONCEPTO, LOS PROVEEDORES DE LOS CONTENIDOS NO TIENEN QUE REALIZAR NINGUNA TAREA. ¿TODO EL SISTEMA DE PROTECCIÓN DEL MENOR RECAE EN LAS PERSONAS USUARIAS Y EN LA APP DE VERIFICACIÓN?

El funcionamiento de este sistema establece exigencias a los proveedores de los servicios y contenidos. Por un lado, la de etiquetar sus contenidos apropiadamente, o utilizar un formato común para determinar que todo el sitio tiene restricciones de edad (juego online, plataformas de contenido pornográfico, etc.), con etiquetas que sean adecuadamente interpretables por los navegadores u otras aplicaciones de acceso a contenidos.

Los mismos proveedores de servicios y contenidos, cuando ofrezcan sus propias aplicaciones de acceso a los contenidos, han de implementar los mecanismos de protección y de consulta a la *app* de verificación de edad. Los navegadores, igualmente, han de implementar los mecanismos de protección y de consulta a la *app* de verificación de edad en función del etiquetado de los contenidos que reciben.

Los mecanismos de protección mencionados habrán de incluir el filtrado de contenidos en el dispositivo.

Todos ellos han de implementar medidas de gobernanza para garantizar la transparencia y auditabilidad y evitar la suplantación de *apps*, la explotación de sus posibles vulnerabilidades o el acceso a servicios con contenidos no etiquetados, por mencionar algunos ejemplos.

26. ¿CÓMO PUEDE UN PROVEEDOR DE CONTENIDOS ASUMIR SU RESPONSABILIDAD EN LA PROTECCIÓN DE MENORES ANTE CONTENIDOS INADECUADOS SI NO RECIBE NINGUNA INFORMACIÓN SOBRE LA PERSONA

QUE INTENTA ACCEDER A SUS CONTENIDOS? ¿NO DEBERÍA RECIBIR ALGÚN ATRIBUTO RELACIONADO CON SU EDAD?

Las PoC desarrolladas por la AEPD demuestran que es posible que asuma esta responsabilidad sin necesidad de recibir ningún tipo de dato acerca de la persona usuaria, cumpliendo así con el decálogo de principios propuestos y evitando los riesgos y amenazas identificados en las soluciones de verificación de edad que actualmente se utilizan. Es posible realizar todo el tratamiento sin enviar datos fuera del dispositivo de la persona usuaria y, por lo tanto, no es necesario que el proveedor de contenidos reciba ningún tipo de dato acerca de la persona que accede a sus contenidos. De igual forma, el proveedor puede asumir sus responsabilidades sin necesidad de ejecutar ningún tratamiento en sus propios servidores o de desarrollar soluciones propietarias.

27. EN PLATAFORMAS QUE REQUIERAN LA CREACIÓN DE UNA CUENTA PARA EL ACCESO A CONTENIDOS Y EN LAS QUE HAY CONTENIDOS PARA PERSONAS MENORES DE EDAD Y PARA PERSONAS ADULTAS ¿SERÍA IGUALMENTE VÁLIDA ESTA SOLUCIÓN PARA LA VERIFICACIÓN DE EDAD QUE SE DESARROLLA EN LAS POC?

Sí, los contenidos aptos para todos los públicos serían accedidos con normalidad. Y solo en el caso de los contenidos inadecuados para personas menores (principio 4) se realizarían los procesos de verificación para saber si se debe proteger a un menor.

28. ¿CÓMO SE GARANTIZA QUE SON LOS QUE EJERCEN LA PATRIA POTESTAD LOS QUE FINALMENTE DECIDEN LO QUE LA PERSONA MENOR PUEDE VER Y LO QUE NO, DE MANERA EFECTIVA?

Según el decálogo de principios que se ha elaborado, mediante los mecanismos de gobernanza de las soluciones (principio 10), la auditoría de la ejecución del filtrado de los contenidos para personas adultas, y la participación activa en los sistemas de etiquetado de contenidos (principio 8).

29. ¿NO ES POSIBLE QUE LO QUE PASE AL FINAL ES QUE UNA PERSONA ADULTA SE DESCARGUE TODOS LOS CONTENIDOS Y LOS SIRVA DESDE UN SERVIDOR PROPIO DESDE DONDE LOS DISTRIBUYA PÚBLICAMENTE, SIN ETIQUETAS NI LIMITACIONES? ¿O QUE ALGUNOS PROVEEDORES DE CONTENIDO PARA PERSONAS ADULTAS, DIRECTAMENTE NO LO ETIQUETEN COMO TAL? ¿O QUE SE GENERE UNA INTERNET "PARALELA"?

En este punto es donde han de aplicarse el mecanismo de gobernanza, y las herramientas de autenticación de las *apps* de verificación de edad y las *apps* de acceso a contenidos/navegadores (estas últimas deben incorporar los mecanismos de protección y de consulta a la *app* de verificación de edad).

Cualquier solución que se presente como perfecta está faltando a la verdad, y minusvalora la imaginación humana. Los mecanismos de gobernanza han de vigilar de forma continua las nuevas vulnerabilidades y debilidades y reaccionar ante ellas.

En la Internet accesible para toda la ciudadanía a través de las herramientas y protocolos habituales (la denominada en ocasiones la "Clearnet") podrían buscarse estos servidores que, serán fáciles de detectar porque no usarán etiquetas de edad o las tendrán mal asignadas (etiquetando todo el contenido como apto para todos los públicos, lo que podría implicar reclamaciones constantes de los usuarios de Internet a los comités o comisiones que supervisen el autoetiquetado). Estas detecciones permitirían elaborar listas de bloqueo para herramientas de control parental o para servidores DNS, penalizar a estos sitios en los resultados de las búsquedas realizadas con los motores habituales (para que no salgan o

salgan con muy poca prioridad), podrían ponerse sanciones, etc. En cualquier caso, la existencia de métodos para sortear protecciones no justifica dejar de establecer medidas e intentar que sean lo más eficaces posibles.

30. ¿No es posible que surjan navegadores o aplicaciones de acceso a contenidos que se salten el filtrado por edad y no verifiquen la edad de las personas usuarias?

En este punto es donde han de aplicarse el mecanismo de gobernanza, y las herramientas de autenticación de las *apps* de verificación de edad y las *apps* de acceso a contenidos/navegadores (estas últimas deben incorporar los mecanismos de protección y de consulta a la *app* de verificación de edad). Hay que asumir que la tecnología no ofrece una garantía completa, sino que requiere de una adaptación continua. Por ello los mecanismos de gobernanza han de vigilar de forma continua las nuevas vulnerabilidades y reaccionar ante ellas.

Existen soluciones técnicas que permiten que los contenidos aptos para todos los públicos puedan ser accedidos desde cualquier navegador o *app*, pero los que son para personas adultas, sólo desde navegadores o *apps* que realicen verificación de edad. De nuevo, la existencia de métodos para sortear protecciones no justifica dejar de establecer medidas e intentar que sean lo más eficaces posibles.

Hay que plantearse que el marco de gobernanza de los sistemas de verificación de edad y protección ante el acceso a contenidos inadecuados, por su impacto, se incorporen en los procesos de notificación de incidentes y los procesos de supervisión establecidos en el marco de la Directiva NIS2.

31. ¿Qué ocurre si se utiliza una VPN para el acceso a contenidos para adultos?

El sistema propuesto en las PoC es más robusto ante la utilización de VPNs que otros que se emplean actualmente, ya que no se basa en saber desde dónde se realiza la petición de contenidos al servidor.

Por un lado, las políticas se establecen y ejecutan de forma local, al ser ejecutadas en el dispositivo, independientemente del servidor accedido o de dónde se origina la solicitud.

32. ¿No es posible que una persona menor acceda a contenidos inadecuados utilizando para ello el dispositivo de una persona adulta?

La acreditación, periódicamente o en cada reinicio del dispositivo, por ejemplo, de que la persona que usa el dispositivo es su propietaria y tiene la edad que verifica, evita esta circunstancia.

Siempre es necesario llegar a un equilibrio entre fiabilidad de la solución de verificación de edad y usabilidad (no se pueden pedir pruebas constantemente ya que esto entorpecería la navegación por contenidos para personas adultas).

La existencia de métodos para sortear protecciones no justifica dejar de establecer medidas e intentar que sean lo más eficaces posibles.

33. ¿No sería más sencillo el bloqueo de contenidos en la SIM como ya se hace en otros países?

Es necesario ser cuidadosos, porque este tipo de solución podría permitir fácilmente la detección de personas menores, que quedarían registradas de alguna forma al adquirir el teléfono, dar de alta la SIM, etc. como persona menor.

Además, la realidad nos muestra que muchos móviles para menores se adquieren sin señalar que el uso va a ser para una persona menor de edad, o que se heredan móviles de personas adultas.

En cualquier caso, cualquier solución debería cumplir con el decálogo de principios para garantizar el cumplimiento en materia de protección de datos y los derechos y libertades de la ciudadanía. Además, distintas soluciones se podrían aplicar simultáneamente para una mayor garantía.

34. ¿Cuál es el ámbito de aplicación de las PoC, serían válidas en el contexto internacional o sólo funcionan en España?

Serían válidas en el contexto internacional ya que permiten que la persona que accede a contenidos verifique su edad con diferentes mecanismos (código QR, cartera digital, documentos de identidad oficial en formato físico). Basta con que al menos uno de estos mecanismos esté disponible en el país de origen de la persona usuaria para que pueda realizar la verificación de edad de algunas de las maneras propuestas como, por ejemplo, recogiendo los datos del pasaporte, que se registran en un formato de aplicación universal.

35. ¿Es esta una iniciativa únicamente de España?

Este modelo se ha planteado a nivel europeo. Por iniciativa española ya existe un mandato del plenario del Comité Europeo de Protección de Datos para que el grupo *Key Provisions* trabaje en unos criterios de verificación de edad y será planteado en el conocido como “Grupo Berlín” de la Global Privacy Assembly.

36. ¿Son compatibles las PoC con la nueva normativa de identidad digital europea única, eIDAS2?

Sí, lo son. De hecho, una de ellas, la que permite el acceso a contenidos a través de un teléfono móvil con Android, se basa en una cartera digital, que podría ser en el futuro la que desarrollen SGAD y FNMT en España. Además, los principios recogidos en el decálogo son perfectamente compatibles (en lo que se refiere a la minimización de datos, a poner a la persona usuaria en el centro y controlando con quién comparte sus datos, etc.) con el espíritu de la norma eIDAS2.

37. ¿Respetan las PoC el principio de neutralidad tecnológica?

Tanto las PoC como los principios que demuestran son independientes de fabricantes de dispositivos, sistemas operativos, proveedores de identidad, etc. Los principios son completamente neutrales en este sentido.

En cuanto a las PoC, se han desarrollado tres para intentar mostrar cómo pueden trasladarse estos principios a escenarios reales empleando diferentes tipos de dispositivos, de diferentes fabricantes, con diferentes sistemas operativos, proveedores de identidad heterogéneos, etc. Cualquier sistema que respete los principios es válido, independientemente de las tecnologías o arquitecturas seleccionadas para su implementación.