



# Informe del CAA sobre inteligencia artificial

---

## ÍNDICE

1. Antecedentes.....	3
2. Marco jurídico.....	4
3. Reuniones con expertos.....	8
3.1. Introducción .....	8
3.2. Borja Adsuara (9/11/2023) .....	8
3.3. Ricard Martínez (28/11/2023) .....	11
3.4. Aníbal Astobiza (14/12/2023) .....	15
3.5. Alicia Troncoso (1/2/2024) .....	18
3.6. Conclusiones .....	19
3.6.1. Borja Adsuara .....	19
3.6.2. Ricard Martínez .....	20
3.6.3. Aníbal Astobiza.....	21
3.6.4. Alicia Troncoso.....	21
4. Informe técnico sobre aplicaciones de desnudos virtuales.....	23
4.1. Introducción y objetivo .....	23
4.2. Metodología.....	23
4.2.1. Aplicaciones web .....	23
4.2.2. Aplicaciones para móvil.....	24
4.3. Análisis.....	24
4.4. Conclusiones .....	24
4.4.1. Aplicaciones web .....	24
4.4.2. Aplicaciones para dispositivos móviles.....	25
5. Barómetro Audiovisual de Andalucía.....	27
6. Conclusiones generales .....	29
Igualdad de género .....	29
Derecho al honor y a la intimidad .....	29
Protección de los menores.....	30
<i>Fake news</i> y desinformación .....	30

## 1. Antecedentes

Este informe nace de los trabajos y debates realizados en el seno de la Comisión de Contenidos del CAA entre 2023 y 2024 acerca de los riesgos y de los desafíos planteados por el uso de la inteligencia artificial en el entorno audiovisual y de Internet. Estos trabajos se derivan de los realizados con anterioridad sobre la protección de los menores respecto a contenidos pornográficos o de cualquier otro tipo que no fueran adecuados, pero a los que los menores podían acceder con facilidad, según se puso de manifiesto en los siguientes acuerdos del CAA:

*[Acuerdo de 15 de marzo de 2023 por el que se traslada a la Comisión Nacional de los Mercados y la Competencia la relación de plataformas de intercambio de vídeos de pornografía establecidos en España que ofrecen contenidos con insuficientes sistemas de verificación de edad](#)*

*[Acuerdo de 11 de mayo de 2023 del Consejo Audiovisual de Andalucía en relación con los vídeos y otros recursos en los que se facilita información que permite a los menores acceder a contenidos pornográficos de diversas plataformas online.](#)*

*[Acuerdo de 19 de julio de 2023, en relación con el libre acceso de menores a contenidos inadecuados en plataformas de mensajería y otras redes como Telegram.](#)*

El desencadenante del estudio de los riesgos de la IA para los menores, pero también para el resto de la población, fue la alarma social suscitada a raíz de la denuncia, en octubre de 2023, de la difusión de imágenes de desnudos virtuales creados mediante IA de chicas adolescentes por parte de amigos también menores de edad en Almendralejo (Badajoz). A partir de ese momento, en la Comisión de Contenidos del CAA se acordó abordar esta cuestión mediante la consulta a expertos en la materia y la pesquisa de los propios servicios técnicos del órgano, entre las que destaca el informe realizado sobre las aplicaciones que permiten la realización de desnudos virtuales (punto 4 del presente documento), cuyas preocupantes conclusiones motivaron un nuevo acuerdo del CAA poniendo de manifiesto la cuestión:

*[Acuerdo de 13 de marzo de 2024 sobre los riesgos de los sistemas de inteligencia artificial en el ámbito audiovisual y digital; especialmente la generación de imágenes virtuales de cuerpos desnudos.](#)*

Este documento reúne todos los trabajos realizados hasta la fecha por el CAA sobre la cuestión de la IA, para permitir su difusión y seguir recabando la atención de la sociedad en general de cara a los riesgos que las nuevas tecnologías, más allá de sus evidentes beneficios, pueden también suponer.

## 2. Marco jurídico

El rápido desarrollo de la inteligencia artificial, la transformación digital que supone y los potenciales riesgos que conlleva, han puesto de relieve, una vez más, la importancia de que los poderes públicos ejerzan sus competencias para la protección de los derechos fundamentales de los ciudadanos y, especialmente, de los menores de edad en el entorno digital, garantizando su privacidad y seguridad. El derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la protección de menores y el libre desarrollo de su personalidad, la no discriminación y la igualdad entre hombres y mujeres y el derecho a la libertad de expresión, entre otros, justifican la imposición de restricciones al uso y comercialización de estos nuevos sistemas.

Es indudable los beneficios que aporta esta nueva tecnología, pero deben establecerse medidas para que los sistemas de inteligencia artificial sean seguros. Diversos estudios ponen de manifiesto que la IA podría ser utilizada para lanzar campañas automatizadas de desinformación y manipulación mediática y electoral. Por otra parte, dado que los algoritmos son entrenados con datos que pueden contener prejuicios y sesgos, permite la discriminación de ciertos colectivos sociales y minorías. Junto a ello, posibilita la vulneración de la privacidad de las personas y el libre desarrollo de la personalidad de los menores al permitir, entre otras cuestiones, su acceso a material inapropiado.

El CAA como la autoridad audiovisual independiente encargada de velar por el respeto de los derechos, libertades y valores constitucionales y estatutarios en los medios audiovisuales en Andalucía, así como por el cumplimiento de la normativa vigente en materia audiovisual y de publicidad,<sup>1</sup> emprendió una línea de trabajo para estudiar los riesgos que comporta el uso de esta nueva tecnología en el ámbito audiovisual. Todo ello con el objetivo de instar las medidas necesarias para la salvaguarda de los derechos de los menores, jóvenes, tercera edad, personas con discapacidad, inmigrantes y otros colectivos necesitados de una mayor protección, en lo que se refiere a los contenidos de la programación y publicidad en los medios. De esta forma, el CAA continúa con su labor de desarrollar campañas de educación y difusión sobre el uso seguro y responsable de Internet y las tecnologías de la información y la comunicación.

En el seno de la Unión Europea, en el año 2020, se adoptó el Libro Blanco de la Unión Europea sobre la inteligencia artificial. Se proponía desarrollar un marco jurídico que hiciera compatibles los valores y derechos que se constituyen como principios esenciales de la Unión Europea y el desarrollo de innovación científica. Ya en el 2019, el Consejo Europeo

adoptó unas [Conclusiones relativas al Plan Coordinado sobre la Inteligencia Artificial](#)<sup>1</sup> donde se destacó la importancia de garantizar los derechos de la ciudadanía europea y su adaptación a las oportunidades y retos de las nuevas tecnologías. Posteriormente, en el 2020, la Presidencia del Consejo de la Unión Europea formuló la [conclusiones sobre la Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital](#)<sup>2</sup> donde se abogaba por afrontar la complejidad, imprevisibilidad y sesgos derivados de ciertos sistemas tecnológicos.

La Comisión Europea, consciente del grave problema que suponen estas herramientas, presentó una propuesta de Reglamento del Parlamento Europeo y del Consejo, con el objetivo de asegurar el respeto de los derechos fundamentales de la ciudadanía y generar confianza en el desarrollo y la utilización de la inteligencia artificial. El citado Reglamento busca proveer a la Unión Europea de un marco normativo basado en los riesgos derivados de los sistemas de inteligencia artificial. La norma propone que los sistemas de IA que puedan utilizarse en distintas aplicaciones se analicen y clasifiquen según el riesgo que supongan para los usuarios. Los distintos niveles de peligro implicarán una mayor o menor regulación.

El Reglamento establece un listado de sistemas y de usos de la IA que se consideran inaceptables y, en consecuencia, prohibidos en la UE y otros de alto riesgo. Junto a ello, se ha abordado una regulación específica de sistemas de IA de propósito general y de los modelos fundacionales. Concretamente, por lo que refiere a los modelos fundacionales (esto es, sistemas capaces de llevar a cabo de forma competente un gran rango de tareas distintas como, por ejemplo, generar videos, imágenes o programar código), deberán cumplir con obligaciones de transparencia específicas, con anterioridad a su comercialización, y además de respetar los datos protegidos por derechos de autor, no puede generar contenidos ilegales.

En el ámbito nacional, son varias las normas en nuestro ordenamiento que establecen medidas de protección frente al uso ilícito de la inteligencia artificial<sup>3</sup> y, en breve, se ampliará más el marco regulatorio. Además, contamos con la **Estrategia Nacional de Inteligencia**

---

<sup>1</sup> <https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/es/pdf>

<sup>2</sup> <https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf>

<sup>3</sup> Entre otras, el Reglamento UE (2022/2065) del Parlamento Europeo y del Consejo, de Servicios Digitales, La Ley 34/2002, de 11 de julio, de los Servicios de la Sociedad de la Información y Comercio Electrónico, la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual, Ley 1/1996, de 15 de enero, de Protección Jurídica del Menor, Ley 8/2021, de 4 de junio, de Protección Integral a la Infancia y a la Adolescencia frente a la Violencia, la Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, Ley Orgánica 3/2007, de 22 de marzo, para la Igualdad Efectiva de Mujeres y Hombres, Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género y la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.

**Artificial (ENIA)**<sup>4</sup>, la **Carta de Derechos Digitales**<sup>5</sup> (que también se ocupa de IA) y, recientemente, se ha creado la **Agencia Española de Supervisión de Inteligencia Artificial (AESIA)**<sup>6</sup> que será el organismo competente para gestionar y liderar el ecosistema español de Inteligencia Artificial responsable.

Una de las principales preocupaciones del CAA ha sido el incremento del consumo de contenido audiovisual de carácter sexual por menores. Este acceso se ha agravado con la existencia de aplicaciones de IA generadoras de contenidos pornográficos falsos hiperrealistas que circulan por las redes a los que pueden acceder libremente los menores. El uso concreto de estas aplicaciones, sitios web o programas generadores de *deepnudes*, es principalmente ilegal dado que, en casi la totalidad de los casos, las imágenes son utilizadas sin autorización o consentimiento de las personas desnudadas. El diseño de una herramienta de inteligencia artificial no puede ser un instrumento para la comisión de delitos y, si existiese ese riesgo, se debe desplegar las máximas garantías en el proceso de contratación y uso de la misma. Cómo pueden existir en el mercado digital y ser accesibles para menores este tipo de aplicaciones generadoras de imágenes o videos pornográficos falsos. Existe una responsabilidad tanto por parte de los usuarios que las emplean, pero principalmente de las empresas desarrolladoras o intermediarias que las han colocado en el mercado.

La creación y posterior difusión sin consentimiento de estas imágenes y vídeos falsos de contenido pornográfico podría suponer la comisión de distintos tipos delictivos; como el de pornografía infantil (artículo 189 del Código Penal) y, en todo caso, suponen una violación grave de la intimidad e imagen de las víctimas (artículo 197 del Código Penal). Se trata de imágenes hiperrealistas que, según los expertos consultados, son penalmente trascendentes al no revelar, por su tosquedad, su condición de montaje. Los responsables de las empresas desarrolladoras podrían ser imputables penalmente, al amparo de lo dispuesto en el artículo 197 ter, por la producción de estas aplicaciones o programas para cometer los delitos contra la intimidad. Además, con la redifusión de dichas imágenes pueden existir delitos de acoso, extorsión, injurias o amenazas, al usarse ese material para humillar públicamente a las víctimas. Las redes sociales son un escaparate abierto al mundo y multiplican de forma inimaginable el daño y acoso social que se les produce al someterlas a un escarnio público.

Junto a ello, estas aplicaciones perpetúan y refuerzan estereotipos de género de carácter sexistas y favorecen la comisión de ciberviolencia de género. La mayoría están pensadas para desnudar a mujeres, no a hombres, y suelen utilizar publicidad sexista ilícita que atentan

---

<sup>4</sup> [https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/201202\\_ENIA\\_V1\\_0.pdf](https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/201202_ENIA_V1_0.pdf).

<sup>5</sup> [https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta\\_Derechos\\_Digitales\\_RedEs.pdf](https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf).

<sup>6</sup> El Real Decreto 729/2023, de 22 de agosto



contra la dignidad de las mujeres. Las nuevas tecnologías han cambiado las formas de provocar las agresiones de género. Con ellas se somete a las víctimas a nuevas formas de acoso, invadiendo su intimidad con un alcance mayor que la violencia real dada la inmediatez y facilidad de acceso a las redes sociales.

Por tanto, concurren en esta cuestión responsabilidades administrativas, civiles y penales. Por un lado, la de los usuarios, respondiendo los padres por los hechos imputables a sus hijos, pero la principal, en estas aplicaciones concretas, es la atribuible a las distintas empresas que intervienen en el mercado. No pueden descargar su responsabilidad en el usuario, a pesar de que así conste en los términos del servicio.

## 3. Reuniones con expertos

### 3.1. Introducción

El presente documento recopila lo recogido en las actas de la Comisión de Contenidos del CAA acerca de las cuatro reuniones mantenidas sobre los posibles problemas del uso de la inteligencia artificial para la protección de los menores en el entorno digital. A cada una de las reuniones se invitó a una persona experta de diversos ámbitos para discutir el asunto, a saber:

- 9 de noviembre 2023, Borja Adsuara, Dr. en Filosofía del Derecho. Profesor, Abogado y Consultor. Experto en Derecho, Estrategia y Comunicación Digital.
- 28 de noviembre 2023, Ricard Martínez, Ricard Martínez Martínez. Director de la Cátedra de Privacidad y Transformación Digital. Profesor Permanente Laboral Departamento de Derecho Constitucional, Ciencia Política y de la Administración, Universidad de Valencia.
- 14 de diciembre 2023, Aníbal Astobiza, licenciado en Filosofía por la Universidad de Deusto y doctor en Ciencias Cognitivas y Humanidades por la Universidad del País Vasco.
- 1 de febrero de 2024, Alicia Troncoso, presidenta de la Asociación Española de Inteligencia Artificial y profesora de la Universidad Pablo de Olavide de Sevilla.

### 3.2. Borja Adsuara (9/11/2023)

El consejero Rísquez da la bienvenida al profesor Adsuara, agradeciéndole su generosidad, y explicándole el interés del CAA por la inteligencia artificial en relación con las funciones y competencias del órgano.

BA comienza su intervención indicando que, más allá de las competencias que organismos autonómicos como el CAA pudieran tener sobre estas cuestiones, en cualquier caso la labor de divulgación que se está realizando es también imprescindible. Respecto a las competencias, además, opina que cuanto más descentralizadas estén, más posibilidades hay de difusión y de viralización de todas estas cuestiones, lo que es vital.

En cuanto a la IA, BA se refiere a los últimos modelos de móviles, cuyas herramientas fotográficas ya permiten el retoque y la generación de contenidos por IA en el mismo momento de la toma, lo que plantea un auténtico desafío para, por ejemplo, el valor probatorio de las imágenes en el ámbito judicial o para su valor informativo en el ámbito de los medios, y también se corre el riesgo de instituir sistemas de censura parecidos a los existentes en los regímenes autocráticos.

Respecto a la protección de la infancia, BA entiende que es necesario un trabajo de pedagogía por casos como los de Almendralejo, por cuanto los menores piensan que se trata de un juego, cuando dista mucho de serlo, y hay que hacérselo ver así, para que sean conscientes de las terribles consecuencias que estos actos pueden tener, y no importa si las imágenes son reales o realistas creadas con IA, porque el daño para las víctimas es exactamente el mismo, con una violación espantosa de su intimidad. En su opinión, ya existe en el Código Penal un instrumento perfectamente válido, aunque ahora mismo se ciñe a la pornografía infantil simulada o creada artificialmente, y bastaría con no limitarla a los menores, sino a cualquier persona que fuese víctima de falsificaciones de esta clase. Es más, el artículo 197 del Código Penal, que habla del uso de cualquier artificio técnico de reproducción de la imagen, sería perfectamente aplicable a usos delictivos de la IA, sin que sea necesario legislar ad hoc para cada nueva tecnología que se desarrolle.

BA explica que esta clase de delitos contra la intimidad se producen en dos actos, siendo el primero la creación y difusión de las imágenes, y el segundo el acoso social a las víctimas, multiplicado por las redes, y que, en su opinión, es el que produce un daño superior, llevando a algunas personas incluso al suicidio, como en el caso de la trabajadora de IVECO. Para este tipo de acoso en masa, que, en la práctica, resulta imposible de perseguir porque no se puede condenar a miles de personas, BA emplea el concepto de “delito en enjambre”, que resulta aún peor que el delito en manada. Dado que las consecuencias de estos delitos son terribles, BA aboga por hacer entender a las familias que deben evitar que sus hijos delincan, que se debe insistir en que esos comportamientos no son ningún juego, sino delitos muy graves que, incluso aunque los hijos puedan no ser imputables por razones de edad, pueden derivar en serias responsabilidades económicas para los padres por indemnización de los daños. Hay que explicarles a los padres que, aunque los hijos menores tengan derecho a la intimidad, existe jurisprudencia que justifica el que, en caso de sospecha de comportamientos delictivos de o contra sus hijos, los padres tienen derecho a invadir su intimidad para evitar un mal mayor. BA entiende que se insiste demasiado en los mensajes en positivo sobre el uso de la tecnología por los menores, obviando materias tan graves como las expuestas, y, por el contrario, es necesario endurecer el mensaje, hacerlo acorde a la gravedad de los delitos que pueden cometerse, para que tanto los menores como sus padres sean plenamente conscientes de las consecuencias.

De cara al nuevo Reglamento de Servicios Digitales, BA opina que, entre la censura de las redes y las competencias de la CNMC, existe una vía muy interesante de colaboración público-privada y de corregulación, mediante el uso de etiquetado inteligente, para lo que ICMedia y diversas empresas de IA ya están trabajando. Sería un sistema similar al de los alimentos, con un etiquetado obligatorio de los contenidos gracias al uso precisamente de la

misma IA que, por el otro lado, posibilita ciertos delitos. Por su experiencia en señalización de televisión y videojuegos, BA estima que es posible gracias a la IA la generación de etiquetas inteligentes, que describan adecuadamente los contenidos y que permitan una configuración personalizada a los padres, ya que no todas las sensibilidades son iguales. Para la gestión de un sistema así, BA aboga por la creación de organismos sectoriales de resolución extrajudicial de conflictos, al modo de Autocontrol en la publicidad, cuyo convenio se firmó cuando él era director general para el Desarrollo de la Sociedad de la Información, y que, en su opinión, ha dado unos resultados muy positivos, prácticamente eliminando la publicidad conflictiva, lo que debería aplicarse también a los contenidos, pues todo esto redundaría en una mayor seguridad jurídica para todas las partes implicadas, y en una considerablemente mayor eficiencia administrativa, máxime teniendo en cuenta la falta de recursos de la CNMC, que presumiblemente ha sido designada como coordinadora nacional de servicios digitales. Dado que el Reglamento ha entrado en vigor en febrero del 2024, BA señala que el retraso es ya patente, no habiéndose modificado el Estatuto de la CNM para ejercer las nuevas competencias, ni habiéndose decidido qué papel tendrían otras instituciones (como el CAA).

El consejero Rísquez agradece la completísima intervención del profesor BA, y le pregunta, al respecto de la última parte de la misma sobre la DSA, cuál sería el papel de un organismo como el CAA, teniendo en cuenta que las iniciativas sobre la pornografía han tenido una repercusión considerable, habiéndose incluso creado un grupo de trabajo sobre esta materia en el Parlamento andaluz. BA responde que, aparte del sistema de etiquetado de contenidos, está el problema de la verificación fehaciente de la edad, para lo que aboga por un sistema de identificación electrónica basado en terceros de confianza, en donde se emitiera un certificado digital a partir de un registro de atributos de la personalidad, evitando, además, de este modo, la cesión gratuita de datos personales (e, incluso, en algunos casos biométricos) a las grandes empresas de internet, que es lo que está sucediendo de momento. Sin un sistema de verificación de la edad eficiente, como el descrito, no tiene sentido el etiquetado de contenidos ni la prescripción de estos según edades, ni es posible garantizar la protección de los menores.

El consejero Rísquez se pregunta cómo es posible que existan aplicaciones y páginas web, de libre acceso, cuyo objetivo, empezando por el nombre de las mismas (como *Clothes Off*), no deja ninguna clase de dudas, mientras que la pornografía sí está sujeta a limitaciones. BA responde que, mientras no es razonable abogar por la prohibición de herramientas generales que incorporan la IA, como Photoshop, es evidente que *Clothes Off* y otras aplicaciones por el estilo tienen como objetivo la comisión de delitos y que el Código Penal español permitiría su prohibición y el bloqueo de uso en el territorio nacional, como ocurre con cualquier herramienta o dispositivo cuyo fin principal sea delinquir.

El presidente del CAA interviene para agradecer también a BA su aportación, señalando que compareció en el Parlamento andaluz para inaugurar el grupo de trabajo sobre pornografía, que ha sido impulsado por las jornadas sobre este asunto que el CAA organizó en dicha sede parlamentaria, y que en la comparecencia expuso cómo desde los poderes públicos hasta el último ciudadano todo el mundo habla tranquilamente de los peligros de las pantallas para los menores, sin una alarma verdadera. En este sentido, algunos reguladores, como el francés, llevan más camino andado con su certificado digital emitido por terceros, pero la tarea que resta es aún ardua, llamando la atención el agravio comparativo entre una televisión lineal perfectamente regulada y el ámbito de Internet, donde todo parece valer. BA responde que la educación es esencial y que el derecho tiene también una función educativa que hay que utilizar con los menores y sus padres para que comprendan la gravedad de los delitos y sus consecuencias, existiendo ya recursos legales en el Código Penal para perseguir estos delitos, de la misma manera que se persiguen los que atentan contra la propiedad intelectual. Si el Ministerio de Consumo, por ejemplo, bloquea páginas que publicitan la prostitución, es posible actuar contra las aplicaciones o webs que se han comentado en la reunión. BA aboga por hacer pedagogía en todos los ámbitos y por recordar la dimensión axiológica de la norma. El presidente del CAA pregunta sobre la necesidad de que se constituya un consejo audiovisual de ámbito nacional, indicando BA que existe un debate sobre la CNMC, su estructura y sus funciones, pero que confía en que se desarrollen los sistemas de autorregulación (regulada) y corregulación.

Finalmente, el profesor BA cierra su intervención indicando que la situación está ya madura y que existen herramientas tanto tecnológicas como legales para luchar contra los efectos indeseados de la IA o de otras tecnologías.

El consejero Rísquez despide a BA, agradeciéndole una vez más su participación y abogando por mantenerlo como colaborador en estas iniciativas del CAA, iniciándose a continuación un debate sobre la reunión, en el que, entre otros asuntos, la coordinadora jurídica informa de la presentación de una proposición de ley en el Congreso sobre IA.

### 3.3. Ricard Martínez (28/11/2023)

El consejero Rísquez agradece a Ricard Martínez (en adelante, RM) su colaboración y explica las preocupaciones del CAA, en el ámbito de sus competencias, por los posibles efectos del uso de la inteligencia artificial por menores o hacia menores, no entendiéndose, por ejemplo, que aplicaciones cuyo fin es explícitamente delictivo, como las que permiten desnudar virtualmente a personas, sean de libre acceso por cualquiera, incluidas personas menores.

RM se muestra de acuerdo en que eso no es admisible, anunciando que la semana próxima acudirá a una reunión del Centro de Estudios Políticos y Constitucionales del Ministerio de la Presidencia con la Fiscalía, en donde se expondrán estos problemas, pues, en su opinión, no es necesario ni conveniente esperar a una legislación específica adaptada a las nuevas tecnologías cuando el Derecho preexistente ya ofrece herramientas válidas. La legislación de otros países, como los EEUU por ejemplo, ya establecía la obligatoriedad de la verificación de edad para impedir el acceso a los menores a contenidos no adecuados en 1998, y la actual demanda allí contra Meta, en la que el asunto de los menores es esencial, es una buena muestra de que se puede actuar, ya que en Derecho debe prevalecer el superior interés del menor, exactamente igual que en otros campos como el del juego o el alcohol. RM, como firmante de la Carta de Derechos Digitales, indica que en su redacción se discutió mucho sobre el concepto de identidad digital que, algo que está en el núcleo del reglamento de inteligencia artificial de la Unión Europea, ahora en su fase final, pero hay ciertas discusiones los gobiernos de Francia y Alemania. Esta norma, en la última versión publicada por el parlamento, sitúa el análisis de riesgos para los derechos fundamentales en la posición nuclear de las tareas que tiene que hacer cualquier aplicación de inteligencia artificial que quiera obtener una verificación de conformidad. Una cosa es tu esfera de vida privada donde seguramente los tribunales dirán que en la vida sexual de una pareja o de un sujeto, nadie se mete. Ahora bien, el supuesto de una aplicación que permite desnudar a cualquiera sin su consentimiento es algo completamente distinto. Haciendo de abogado del diablo, del otro lado van a decir que, en realidad, esa no es tu propia imagen, sino una imagen sintética. Pero desde una perspectiva no tendrán razón, porque en el momento en que tú le pones la cara de alguien a un cuerpo desnudo, por sintético o imaginado que sea, nuestro modo de percibir la realidad asocia directamente esa cara a esa persona.

RM señala que en el derecho de los EEUU tiene una institución muy interesante que regula la privacidad, pues dentro de la garantía de la vida privada, establecen cuatro ilícitos civiles, y uno de ellos se denomina como False Light, que consiste en exponer a una persona de modo equivocado o mintiendo a la luz del escrutinio público porque se está dando una falsa imagen de esa persona ante la opinión pública. En España, por ejemplo, la Fiscalía considera pornografía infantil también a la sintética y enteramente generada de modo digital. Porque se debe aplicar una interpretación progresiva de la norma, y es evidente que en cuanto se use la cara de alguien de la forma que se está comentando se está violando su intimidad y si un medio de comunicación generara mediante inteligencia artificial una película falsa que atentara contra estos valores de protección del menor y la emitiera, daría igual que el menor no sea real y debería actuarse contra el medio desde el CAA o el órgano que tuviese las competencias.

RM entiende que en el ámbito de la de la protección de datos no cree que exista posibilidad de atacar una imagen completamente fake, porque no hay ningún dato personal en juego y el requisito, el punto de partida de la protección de datos es que el tratamiento de la información afecte a personas identificadas o identificables. Pero desde el momento en el que intencionalmente se pongan elementos identificadores para que el espectador atribuya o vincule una determinada imagen con un sujeto identificado o identificable, entonces operará la normativa de protección de datos. Así, por ejemplo, la AEPD no ha actuado hasta muy recientemente en materias que podían afectar a las libertades personales o al derecho a la información, pero si el tratamiento de datos es ilegítimo ahora ya sí lo está haciendo. Y si se trata de un particular a través de una red social, directamente están sancionando por protección de datos, siendo los padres responsables de esos menores.

El consejero Rísquez pregunta a RM por la reciente medida legal que se ha adoptado en Italia, por la que se ha acordado que las tarjetas SIM incluyan una especie de PIN parental que pueda evitar que los niños accedan a través de su móvil a determinados contenidos.

RM indica que se trata de algo que él viene defendiendo desde hace tiempo, por ejemplo en una comisión parlamentaria durante la presidencia de M. Rajoy, donde expuso que había un grave problema con las empresas de telecomunicaciones, ya que estas tienen abonados, pero no distinguen entre abonado y el titular de la línea, lo que significa que no se pueden establecer políticas o restricciones de acceso en función de criterios de verificación de edad, algo que sería sencillo si dichas empresas tuviesen claramente indexada cuál es la edad de cada cliente. Algo así supondría modos de articular protección no solo de los padres, sino del propio sistema.

No obstante, RM opina que resulta importante también cómo graduar los controles parentales con el libre desarrollo de la personalidad del menor, pues tener una constante monitorización de ellos (como permite por ejemplo la geolocalización), aunque pueda tener sentido a determinada edad, no parece que sea lo más adecuado para el libre desarrollo de su personalidad. Además, RM insiste en que se trata de políticas que exigen una fuerte inversión en la formación de los padres, para que estos sean capaces de modular adecuadamente el PIN parental, ya que en la actualidad se trata de sistemas poco sutiles, que pueden impedir a los menores el acceso a contenidos científicos o de otro tipo que necesiten. Se suele decir que los jóvenes son nativos digitales, pero lo cierto es que las herramientas verdaderamente útiles para gestionar el riesgo y también ser para ser futuros investigadores, innovadores y emprendedores en el mundo digital tampoco se están desarrollando.

Por estos motivos, a RM le preocupan los movimientos pendulares que van desde de darle un móvil abierto a un niño a los nueve años a prohibirlo hasta los dieciséis, siendo importante encontrar el punto de equilibrio, ya que la evitación de todo riesgo no es una estrategia aconsejable. RM insiste en el papel fundamental de la educación y en los educadores, indicando que en el título décimo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales hay un artículo que se dedica a los centros escolares, otro que se dedica a los padres, y otro a los planes de estudio, algo que, en su experiencia, no se está llevando a cabo, pues observa una seria falta de formación en competencias digitales tanto entre el profesorado como entre el alumnado universitario y de cualquier nivel. RM señala que quienes redactaron la Carta de Derechos Digitales eran perfectamente conscientes de la necesidad de una evaluación de impacto, es decir, de ver qué piensan los niños mediante un estudio científico, estadístico, del tipo que sea, pero un estudio que permitiera tener un mapa muy claro de cuál es la percepción y que nos permita diseñar políticas públicas, y no a través de una sucesión de escándalos como los casos recientes de Almendralejo o Ayamonte.

El consejero Rísquez comenta que el CAA hace todos los años una encuesta sobre el mundo audiovisual en Andalucía y que en la actualidad, como se está trabajando, sobre todo, en el asunto del acceso de los menores a la pornografía en Internet, se han incluido en el Barómetro varias preguntas estos últimos años que son bastante útiles, pero que no constituyen un estudio científico como el que reclama RM.

RM se refiere entonces a la demanda contra Meta en EEUU, señalando que una de las cuestiones de las que se acusó a Meta era tener pruebas empíricas de que la empresa sabía que sus aplicaciones generaban dismorfia entre los jóvenes, lo que se traduce en anorexia, bulimia y otras afecciones de la salud.

El consejero Rísquez plantea la cuestión de qué podría hacer un órgano como el CAA, respondiendo RM que, por su experiencia en la AEPD, y aun siendo consciente de las limitaciones que a veces imponen la política y las distintas esferas competenciales, sí ve espacio de maniobra para un regulador independiente como el CAA, en su condición de magistratura de autoridad, que puede impulsar la reflexión pública y la formación sobre estas materias, actuando más como un catalizador que como un regulador, más allá de sus competencias. En este sentido, RM indica que en su experiencia en la AEPD resultó muy útil organizar reuniones confidenciales con profesionales y responsables de los medios para discutir honestamente cuestiones delicadas e impulsar el apoyo de los medios a nuevas políticas.

El consejero Rísquez agradece la sugerencia, indicando que el ámbito del CAA en el mundo digital está de momento bastante limitado y como regulador las competencias están claramente en ámbito audiovisual, pero estas iniciativas se llevan a cabo por interés público, por el convencimiento de que una institución como esta tiene que estar en este debate. El consejero se despide, agradeciendo las aportaciones de RM, añadiendo que se mantendrá el contacto y que se le informará de los pasos que el CAA vaya dando en esta iniciativa.

### 3.4. Aníbal Astobiza (14/12/2023)

El consejero Rísquez da la bienvenida al invitado, agradeciéndole su participación y explicándole los antecedentes de la iniciativa.

Aníbal Astobiza (en adelante, AA) agradece que se haya pensado en él y empieza explicando el problema que puede suponer el uso de la inteligencia artificial (IA, en adelante) por un actor malicioso para suplantar personalidades, como está seguro de que va a ocurrir en las elecciones de los EEUU de 2024 y en general en cualquier proceso electoral, lo que supone un serio problema para las democracias, máxime en una situación de extrema polarización política como la que las redes han contribuido a crear. Pero, por otra parte, AA reflexiona también sobre el pánico moral que las nuevas tecnologías siempre han producido, desde el libro, hasta la bicicleta, la radio o la televisión, indicando que, a día de hoy, no existe evidencia científica concluyente, pese a la alarma social, de que el entorno digital e Internet produzcan efectos perjudiciales per se en la salud de los menores. En este sentido, AA hace referencia al comunicado de la Asociación Española de Pediatría sobre la edad de uso de dispositivos móviles en la infancia y la adolescencia, cuyas recomendaciones suscribe y que le parecen que son ponderadas y equilibradas, y en donde se señala que los estudios científicos no han demostrado, por el momento, que las prohibiciones indiscriminadas en el uso de los dispositivos móviles supongan un beneficio para la salud de los niños y adolescentes. Eso no quiere decir que no sea necesario, como reclama la propia AEP, que se cumpla la regulación actual en cuanto a la limitación de edad en el uso de las redes sociales y que se desarrollen sistemas para que exista una limitación real de acceso por parte de los menores a contenido adulto. No todas las familias tienen la capacidad ni el nivel educativo para proteger en la misma medida a sus hijos, una situación que afecta en mayor medida a las de entornos más desfavorecidos. Según AA la clave está en posibilitar un uso saludable de estos dispositivos y tecnologías, acorde con la edad de los menores y su nivel de madurez, buscando un punto de equilibrio entre la permisividad y la prohibición absolutas.

Abundando sobre el corpus científico al respecto de estas cuestiones, AA cita las investigaciones de Andrew Przybylski, profesor de la U. de Oxford, que no han hallado evidencia de efectos nocivos de la tecnología digital (Internet y videojuegos) para los

menores, destacando, además, que aquellos estudios donde sí se concluía dicho efecto negativo estaban mal diseñados y debían descartarse, ya que, aunque existan ciertas correlaciones (por ejemplo, con la depresión), correlación no implica causalidad. Por tanto, AA afirma que no hay correlaciones consistentes a nivel global en los metaestudios entre problemas de salud de los menores y uso del entorno digital.

Asimismo, AA se refiere a las obras *The Anxious Generation* y *The Coddling of the American Mind*, del psicólogo social Jonathan Haidt, quien opina que la sobreprotección de los jóvenes actuales los hace particularmente frágiles y propensos a sufrir problemas derivados de Internet y el mundo digital. Pero AA, aun cuando Haidt sea un autor muy reputado y sus puntos de vista muy interesantes, reitera que entiende que no hay evidencia científica concluyente sobre los efectos negativos de lo digital, lo que no quiere decir que el pánico moral al que se refería con antelación no nos afecte a todos en mayor o menor medida.

El consejero Rísquez indica que le parece muy interesante el punto de vista de AA, pero entiende que un órgano como el CAA no puede correr el riesgo de minusvalorar los posibles peligros de lo digital, algo de lo que puede que no haya todavía un corpus científico suficiente por su novedad, pues sobre otras tecnologías en sus comienzos, como la automoción por ejemplo, tampoco se tenía conciencia de sus efectos perniciosos e hizo falta un tiempo para que estos pudieran ser convenientemente descritos por la ciencia. En este sentido, el consejero Rísquez pregunta a AA su opinión sobre la utilidad de la reciente ley europea sobre IA y, en concreto, sobre la obligatoriedad de señalización de los contenidos creados con IA que esta norma introduce.

AA responde que entiende el punto de vista de un regulador como el CAA, que debe velar porque los contenidos sean veraces, y reflexiona sobre la distinta dificultad para identificar materiales creados por IA según se trate de audio, imagen o texto. AA entiende que es necesario encontrar un equilibrio en la regulación, descartando modelos autoritarios como el chino, y señalando la, en su opinión, excesiva reglamentación de la UE que está haciendo que Europa se esté quedando atrás en este campo vertiginoso, al que ponerle trabas burocráticas en el estilo europeo no sirve de mucho. De hecho, en la discusión del reglamento europeo hubo bastantes discrepancias, y Alemania, Francia e Italia defendieron que no se debía regular una tecnología, sino los productos y servicios derivados de ella. AA alerta de que la hiper regulación y el paternalismo son contraproducentes, pues no hay que decirle a la gente lo que puede o no puede hacer.

El presidente del CAA interviene para felicitar a AA por sus aportaciones, indicando que las evidencias científicas sobre este nuevo entorno digital no van a tardar décadas en

establecerse, puesto que ahora la evolución tecnológica es vertiginosa y entiende que, independientemente de que exista o no aún una evidencia científica al respecto, los menores están asumiendo riesgos en este campo muy por encima de lo que el sentido común aconseja, como se desprende por ejemplo de los informes de la Fiscalía de menores, encontrándonos todavía, pese a lo que establece la norma, en una situación en la que las grandes empresas tecnológicas no limitan el acceso de los menores a contenidos prohibidos por la ley.

El consejero Rísquez añade, a lo expuesto por el presidente del CAA, el caso de las aplicaciones, de acceso libre, cuyo fin es explícitamente ilegal, pues están específicamente diseñadas para desnudar virtualmente a cualquier persona sin su consentimiento.

A este respecto, AA responde que aplicaciones como esas, que arruinan la reputación de las personas y permiten la comisión de delitos contra la intimidad y el honor de manera flagrante, deberían estar claramente reguladas y prohibidas, que no hay duda en casos así, pero insiste en que no debe irse demasiado deprisa en la regulación, pues no hay evidencias científicas que respalden restricciones generalizadas de acceso. AA entiende que la posición de un regulador es complicada, pero defiende que no debe regularse la tecnología en sí, sino los productos, como las aplicaciones citadas, que están claramente diseñadas para fines espúreos o ilegales.

La consejera Jimeno opina que hay bastante coincidencia entre lo expresado por AA y el papel de un organismo regulador como el CAA, pero entiende que existe un problema con la desigualdad social, que hace que haya familias que no tengan recursos de ningún tipo para afrontar esta realidad y sus peligros, lo que refuerza la idea de una regulación que las proteja.

AA responde que las políticas públicas deberían basarse en informes rigurosos y en la evidencia científica, no en intuiciones.

El presidente del CAA interviene para reivindicar el modelo europeo, que incluye la regulación para la protección de los vulnerables, indicando AA que él es la primera persona en considerarse europeo y que le parece bien el modelo, pero que a veces hay que mirar lo que se hace en otros lugares con modelos muy distintos, como los EEUU, pues nos llevan una considerable ventaja tecnológica y, además, todas las grandes empresas del sector digital son de allí.

Finalmente, el consejero Rísquez agradece de nuevo a AA su participación, indicando que se mantendrá el contacto y que se le informará de los pasos que el CAA dé en esta iniciativa, dándose por concluida la reunión a las 12:20.

### 3.5. Alicia Troncoso (1/2/2024)

El presidente da la bienvenida a Alicia Troncoso (AT, en adelante), agradeciéndole su generosidad por participar en estas reuniones de trabajo y explicándole los antecedentes de la iniciativa de la Comisión sobre la inteligencia artificial (IA, en adelante) y la protección de los menores.

AT agradece la invitación, y explica que ella no es especialista en cómo afectan estas cuestiones a los menores, pero que entiende que en realidad las posibilidades que ofrece la IA no son nada nuevo en sí, que esas cosas ya se hacían con programas como Photoshop, aunque la diferencia es que ahora es mucho más sencillo, más rápido y más realista. Ante los peligros que el uso de estas tecnologías pueden suponer y para garantizar su buen uso, AT entiende que son indispensables tanto la educación en valores como la educación tecnológica.

El presidente le pregunta por el acceso universal a la IA, sin cortapisas, y si entiende que el uso de esta tecnología debería especificarse siempre.

AT opina que tiene que haber control y regulación, y que se está desarrollando de hecho todo el marco normativo y deontológico, porque está claro que usos como los que atentan contra la intimidad de las personas deben ser considerados delictivos. AT entiende que el control, más que del acceso a las aplicaciones, debería ser regulatorio, como por ejemplo exige la ley europea recién aprobada, que clasifica a las aplicaciones según su posible impacto, imponiendo unos requisitos tanto más exigentes cuanto mayor sea este. Respecto a las aplicaciones que permiten desnudar virtualmente a las personas, AT opina que deberían ser denunciadas y que, en el marco de la ley europea, deberían ser retiradas, pero es necesario que alguien las denuncie, ya que hasta ahora se han aprovechado de la falta de regulación.

El presidente le pregunta por cómo la AEPIA aborda el uso de esta tecnología, indicando AT que los estatutos de la asociación exigen el cumplimiento de las leyes y el sometimiento a guías éticas. La visión que tiene la asociación de la IA es lógicamente la de una tecnología que se use en beneficio de la sociedad, estribando el problema actualmente en que, al haber saltado la IA al mundo empresarial, el ánimo de lucro puede hacer que a veces su uso no sea ético.

La consejera Jimeno se interesa por la opinión de AT sobre el estado actual de la regulación en España, en relación sobre todo a las personas más vulnerables, más allá del reglamento europeo, dada la evidente lentitud de la legislación comparada con el desarrollo tecnológico. AT responde que entiende que los gobiernos son conscientes de estos problemas y se está en el proceso de regularizarlo, pero que la ciudadanía no puede estar tranquila todavía, pues

existe vulnerabilidad. En este sentido, aboga nuevamente por la educación y la concienciación, porque es necesario que estos asuntos permeen desde los ámbitos científico e institucional a la sociedad entera, aunque, en el estado actual de la cuestión, opina que todavía la ciudadanía no está segura ante los riesgos planteados.

El consejero Ybarra pregunta si la AEPIA promueve la divulgación y la formación en estas materias, respondiendo AT que el núcleo de la asociación es la investigación, y que existen muchas actividades formativas, además del congreso bianual, pero pero enfocadas en su gran mayoría a investigadores y desarrolladores de software (algo particularmente importante, para que éstos trabajen de manera ética), no en la población en general.

Finalmente, el presidente agradece de nuevo a AT su generosidad, ofreciendo la colaboración del Consejo, cuyo foco es lógicamente el entorno audiovisual, para cualquier asunto de la AEPIA en que se pudiera coincidir, y abogando por mantener el contacto e informarle de las conclusiones de estos trabajos y de las iniciativas a las que puedan dar lugar.

AT agradece el interés de una institución pública como el CAA por estas cuestiones, dado que es muy importante concienciar a la sociedad sobre ellas, y queda a disposición del Consejo para futuras colaboraciones.

Al término de la reunión se debate sobre la misma, así como sobre los siguientes pasos que podrían darse, quedando en manos de los servicios técnicos la redacción de las conclusiones con la adición de la pesquisa en curso sobre las aplicaciones.

## 3.6. Conclusiones

### 3.6.1. Borja Adsuara

- Necesidad de pedagogía con los menores y sus padres para que sean conscientes de las terribles consecuencias que puede tener un uso inadecuado de la tecnología, como en el caso de Almendralejo. Existe además jurisprudencia que justifica el acceso a los móviles de los menores por parte de sus cuidadores en caso necesario. Además, Se debe explicar a los padres que son responsables económicamente de los delitos que sus hijos cometan. Insiste en que hay que recordar la dimensión axiológica de la norma.
- El artículo 197 del Código Penal, que habla del uso de cualquier artificio técnico, sería perfectamente aplicable a usos delictivos de la IA, sin que sea necesario legislar ad hoc para cada nueva tecnología que se desarrolle.
- Se propone el concepto de "delito en enjambre" para ilustrar los peligros del acoso social masivo.

- Colaboración público-privada y etiquetado inteligente: se sugiere una vía interesante de colaboración entre el sector público y privado, mediante el uso de etiquetado inteligente para regular los contenidos digitales, similar al sistema utilizado en la regulación de alimentos. Se plantea la importancia de la verificación fehaciente de la edad para el etiquetado de contenidos, abogando por un sistema de identificación electrónica basado en terceros de confianza. Se insiste en la necesidad de acelerar todo este procedimiento, dada la entrada en vigor en febrero de 2024 del nuevo Reglamento europeo.
- Es evidente que *Clothes Off* y otras aplicaciones por el estilo tienen como objetivo la comisión de delitos y que el Código Penal español permitiría su prohibición y el bloqueo de uso en el territorio nacional, como ocurre con cualquier herramienta o dispositivo cuyo fin principal sea delinquir. El profesor Adsuara concluye que existen herramientas tecnológicas y legales maduras para abordar los efectos indeseados de la IA.

### 3.6.2. Ricard Martínez

- La legislación existente es una herramienta válida: RM opina que no es necesario esperar a una legislación específica adaptada a nuevas tecnologías, ya que el derecho preexistente ofrece herramientas válidas. Se menciona la obligatoriedad de la verificación de edad en la legislación de otros países, como los Estados Unidos.
- Protección de datos y falsificación de imágenes: se discute la importancia de la protección de datos en situaciones de falsificación de imágenes, y se destaca la necesidad de actuar contra la violación de la intimidad, incluso si las imágenes son sintéticas.
- Graduación de controles parentales y formación de padres: RM aboga por graduar los controles parentales para equilibrar la protección de los menores con su libre desarrollo. Se destaca la importancia de la formación de los padres para manejar eficientemente los controles parentales y para comprender las competencias digitales.
- Rol del CAA como catalizador en el debate público: Se sugiere que el CAA, a pesar de sus competencias limitadas en el ámbito digital, puede actuar como catalizador en el debate público, impulsando la reflexión y formación sobre temas sensibles, más allá de sus funciones regulatorias específicas en el ámbito audiovisual.

### 3.6.3. Aníbal Astobiza

- Impacto de la inteligencia artificial en procesos electorales: se destaca la preocupación sobre el potencial uso malicioso de la inteligencia artificial para suplantar personalidades en procesos electorales, lo cual se considera un serio problema para las democracias, especialmente en un contexto de polarización política.
- Pánico moral y efectos de las nuevas tecnologías en la salud de menores: se aborda el pánico moral asociado a las nuevas tecnologías, contrastándolo con la falta de evidencia científica concluyente sobre efectos perjudiciales de Internet y dispositivos digitales en la salud de los menores. Se menciona el comunicado de la Asociación Española de Pediatría sobre el uso de dispositivos móviles en la infancia y adolescencia. Se discute la falta de correlaciones consistentes a nivel global entre el uso del entorno digital y problemas de salud en menores, citando investigaciones de Andrew Przybylski y resaltando la importancia de distinguir correlación de causalidad.
- Regulación de la inteligencia artificial y contenidos generados: se aborda la regulación de la inteligencia artificial, destacando la necesidad de equilibrio y evitando modelos autoritarios. Se cuestiona la excesiva reglamentación de la UE, y se defiende la regulación de productos específicos, como aplicaciones diseñadas para fines ilegales.
- Desafíos de la regulación en entornos desiguales: se señala la desigualdad social como un problema en la protección de menores en entornos digitales, sugiriendo la necesidad de regulaciones que protejan a las familias sin recursos. Se destaca la importancia de basar políticas públicas en informes rigurosos y evidencia científica.
- Modelo europeo vs. experiencia de otros países: se discute la eficacia del modelo europeo de regulación, contrastándolo con la experiencia de otros lugares, como los Estados Unidos. Se plantea la necesidad de aprender de otros modelos y adaptarse a la rápida evolución tecnológica.
- AA advierte sobre la complejidad de regular el uso de la inteligencia artificial, especialmente en contextos sociales y políticos sensibles, y destaca la importancia de basar las regulaciones en evidencia científica sólida. También enfatiza la necesidad de equilibrar la protección de menores con la libertad y evitar regulaciones excesivamente restrictivas.

### 3.6.4. Alicia Troncoso

- Se aborda la preocupación por el uso de la inteligencia artificial y su impacto en menores. Se destaca la necesidad de control y regulación para garantizar un buen uso de la tecnología, especialmente en casos que atentan contra la intimidad de las personas.

- Educación en valores y tecnología: se enfatiza la importancia de la educación en valores y la educación tecnológica para abordar los peligros del uso de la IA. Se considera esencial que la sociedad comprenda y utilice esta tecnología de manera ética.
- Regulación europea y control de aplicaciones: se menciona el marco normativo y deontológico en desarrollo, destacando la Ley europea que clasifica aplicaciones según su posible impacto y establece requisitos más exigentes. Se aboga por denunciar y retirar aplicaciones que atenten contra la intimidad. Se señala la lentitud de la legislación española en comparación con el desarrollo tecnológico, especialmente en la protección de personas vulnerables. Se destaca la importancia de la educación y concienciación, pero se reconoce la actual vulnerabilidad ciudadana ante los riesgos planteados
- Ética en el uso empresarial de la IA: se discute la percepción de la IA en el ámbito empresarial y el riesgo de que el ánimo de lucro afecte la ética en su uso. La AEPIA busca que la IA se utilice en beneficio de la sociedad. Se informa de que la AEPIA se centra en la investigación y de que ofrece actividades formativas, incluyendo congresos bianuales, dirigidas a investigadores y desarrolladores de software para fomentar un trabajo ético.

## 4. Informe técnico sobre aplicaciones de desnudos virtuales

### 4.1. Introducción y objetivo

En el contexto de las reuniones mantenidas con expertos (véase el punto anterior de este documento) y de las deliberaciones sobre el caso de Almendralejo en el que se difundieron imágenes de desnudos virtuales de chicas menores de edad, en la sesión de la Comisión de Contenidos del Consejo Audiovisual de Andalucía celebrada el 8 de febrero de 2023 se acordó realizar un análisis en profundidad de las aplicaciones de desnudos virtuales con el fin de, eventualmente, alertar a la sociedad andaluza sobre los riesgos que estas aplicaciones entrañan.

### 4.2. Metodología

#### 4.2.1. Aplicaciones web

Se realizó una búsqueda activa, mediante el motor de Google, de aplicaciones web<sup>7</sup> específicamente de *deepnude*, o generación de imágenes virtuales de cuerpos desnudos a partir de una imagen de una persona vestida (en nuestra investigación siempre mujeres), conservándose el rostro que aparece en la foto aportada por el usuario. Algunas de estas aplicaciones también permiten la realización de *deepfake*, es decir, la mezcla virtual de dos imágenes aportadas con el usuario, normalmente un rostro y un cuerpo distinto al que se quiere añadir el rostro. Otro concepto usado en este informe es el de *IA sexting*, que consiste en la realización de *sexting*, o intercambio de imágenes y mensajes de texto con contenido sexual, pero con en vez de con una persona real, con un robot creado mediante IA.

Para la realización de todas pruebas en las aplicaciones se usaron imágenes de personas virtuales generadas por IA.

De cada aplicación se extrajeron los siguientes datos:

1. Verificación de edad.
2. Requisitos para entrar y realizar pruebas.
3. Posibilidad de generar otros contenidos además de *deepnudes* y *deepfakes*.
4. Determinar dónde se aloja la aplicación<sup>8</sup>.
5. Determinar dónde está registrada la aplicación<sup>9</sup>.
6. Términos y condiciones de uso de las imágenes que se utilizan y que se generan.

El análisis se realizó entre el 12 y el 26 de febrero de 2024.

---

<sup>7</sup> Una aplicación web es un software que se ejecuta en un navegador web, sin necesidad de instalar el programa en el dispositivo.

<sup>8</sup> De acuerdo con los datos que genera la web <https://hostingchecker.com/>

<sup>9</sup> De conformidad con la información generada por la web <https://www.whois.com/>

#### 4.2.2. Aplicaciones para móvil

Aunque este estudio se centró en las aplicaciones web, también se buscaron aplicaciones *deepnude* para descargar e instalar en dispositivos móviles, tanto con Android (Google Play) como con iOS (App Store de Apple). En este caso, se recabó la información que constaba en las citadas fuentes de software, sin que la metodología de la investigación permitiera la instalación y prueba de las aplicaciones.

### 4.3. Análisis

Se estudiaron, por un lado, 21 aplicaciones web, así como, por otro, la disponibilidad de estas u otras aplicaciones en las librerías de software para móviles a Apple y Google.

### 4.4. Conclusiones

#### 4.4.1. Aplicaciones web

- Las aplicaciones de *deepnude* encontradas estaban explícitamente enfocadas a la generación de imágenes femeninas. También se probó con imágenes masculinas, indicando el resultado de estas pruebas que estas aplicaciones no generan cuerpos masculinos realistas, lo que refuerza la idea de que se trata de herramientas cuyo fin es el producir desnudos virtuales femeninos. Por su parte, las aplicaciones de *deepfake*, al aportar el usuario tanto una imagen de un rostro como de un cuerpo, permiten la generación de cualquier tipo de contenido.
- Todas las aplicaciones web analizadas estaban escritas en inglés, aunque la mitad de ellas, al detectar la localización del usuario, eran traducidas automáticamente al español.
- Ninguna de las páginas analizadas tenía un sistema fiable de verificación de la mayoría de edad de las personas usuarias, pues, de hecho, en 13 de las 18 analizadas no había ni siquiera advertencia sobre la edad de uso. Las 5 restantes mostraban una advertencia y el usuario debía con una pulsación del ratón declarar que es mayor de edad.
- Algunas aplicaciones se podían utilizar directamente de forma gratuita sin necesidad de identificarse. En otras ocasiones era necesario inscribirse o darse de alta proporcionando un correo electrónico. En ambos casos el número de imágenes que podían generarse de forma gratuita estaba limitado, e incluso en algún caso no generaba desnudos gratuitos, sino que generaba imágenes con lencería o bikini, o desenfocadas.
- Algunas aplicaciones tenían un servicio que utiliza inteligencia artificial para crear imágenes pornográficas desde cero en diferentes estilos. Estas imágenes se

generaban señalando una serie de parámetros predeterminados, o bien haciendo una descripción con lenguaje natural. En otras web se utilizaba esta misma tecnología para aplicarla a un servicio de *sexting* generado por AI. No obstante, había algunas aplicaciones que sólo generaban *deepnudes* o *deepfakes*.

- Ninguna aplicación de las que se analizaron estaba alojada o registrada en territorio español. Toronto y Reikiavik son las ciudades que más se repitieron en las búsquedas que se realizaron, pero también hay otras como Kuala Lumpur, Nasáu, Arizona o Walnut.
- En el apartado relativo a los términos y condiciones de uso, las web analizadas realizaban una serie de advertencias al usuario acerca del buen o mal uso de la aplicación:
  - Respecto a la mayoría de edad, si no se ha advertido con anterioridad que el uso es exclusivo para mayores de 18 años, es en este lugar en el que indica esto.
  - Se recuerda al usuario que las fotografías deben tener los derechos de autor o de propiedad intelectual de las imágenes que utilice.
  - En relación con las imágenes generadas existe una advertencia de que su uso es privado, que no puede hacerse un uso comercial, y que ningún otro usuario tiene acceso a ellas.
  - En las web analizadas se señala claramente que el uso del servicio es por cuenta y riesgo de la persona que lo utilice y que la responsabilidad es exclusiva del usuario.
  - Respecto de los aspectos éticos del uso de la AI, algunas aplicaciones advierten de que un mal uso de la AI podría suponer la comisión de infracciones normativas.
  - La mayoría (11 de 18) de las aplicaciones web analizadas advierten en los términos de uso que se arrogan el derecho a usar las imágenes generadas en sus servidores (salvo petición expresa de los usuarios, y aun así el derecho de uso se ejerce hasta el momento en que se solicite lo contrario). Así, cada usuario, al generar cualquier imagen, está concediendo, lo sepa o no, a las empresas responsables de las aplicaciones una licencia de uso mundial no exclusiva y libre de regalías, como consta en los términos del servicio, más otras condiciones de uso variables, pero muy amplias, según cada sitio web.

#### 4.4.2. Aplicaciones para dispositivos móviles

Aunque, como queda dicho, en este análisis no se incluyó la descarga, instalación y funcionamiento de las aplicaciones Android e iOS halladas en las tiendas de Google y Apple, cabe reseñar que la oferta era bastante limitada (en comparación con la que se ha hallado



para las aplicaciones web) en el momento de la pesquisa, y que, de acuerdo a los comentarios de los usuarios, parece que en general su funcionamiento era bastante deficiente o, cuando no, no parecían centradas en la creación de material estrictamente pornográfico.

## 5. Barómetro Audiovisual de Andalucía

Aun cuando el BAA (edición 2023) no preguntaba a la ciudadanía andaluza específicamente sobre los posibles riesgos de la IA, hay en él elementos de gran importancia relacionados con la seguridad en Internet y la protección de los menores, entre otros asuntos vinculados al uso actual de la IA.

Así, por ejemplo, se pueden destacar los siguientes datos del BAA 2023:

- El 85% de las personas encuestadas reconoce acceder diariamente a Internet, ascendiendo dicho porcentaje al 99% entre los segmentos de edad jóvenes y medianos.
- El consumo diario de Internet declarado por los entrevistados es de 3:37 horas, superando a cualquier otro medio como la televisión o la radio.
- Internet es el segundo medio en importancia (32%) usado por la ciudadanía andaluza para informarse, solamente por detrás de la televisión (60%).
- Internet es el medio preferido por los encuestados para entretenerse (42% de las encuestas).
- Los datos muestran que la preferencia de Internet tanto para entretenerse como para informarse es superior cuanto más jóvenes son los encuestados. Asimismo, si se observa la evolución de este dato respecto a ediciones anteriores del BAA, se aprecia una curva claramente ascendente para Internet y claramente descendente para la televisión, su principal competidor como fuente de entretenimiento e información.
- El 50% de la población andaluza siente preocupación porque no se garantice la privacidad de sus datos cuando navega por Internet. Asimismo, un 48,5% reconoce preocupación ante la posibilidad de ser víctima de algún timo o fraude en la red. El robo de datos personales o bancarios es otra de las preocupaciones que comparte un 36% de la población andaluza. Y, en menor medida, un 10% de las personas consultadas dice tener preocupación ante la posibilidad de que le sea suplantada la personalidad. Sólo un 9% señalan preocupación por la protección de menores ante la pornografía. En esta misma proporción (9%) se manifiestan quienes se preocupan por la posibilidad de sufrir ataques y daños en el sistema y en los equipos informáticos. Los riesgos de la IA no son aún citados espontáneamente por la población andaluza, aun cuando su uso puede repercutir en las cuestiones

anteriores sobre las que se expresa preocupación, por lo que parece oportuno el papel del CAA al alertar sobre dichos riesgos.

- La población andaluza entiende que Internet es más plural políticamente que los medios tradicionales como televisión y radio. Esta cuestión es interesante por cuanto, aunque ningún medio está libre del posible efecto de *fake news* generadas mediante IA, resulta evidente que estas tienen su medio natural de propagación en las redes sociales tanto públicas como privadas.
- El 82,5% de la población andaluza hace uso de redes sociales, llegando este porcentaje casi al 100% entre los segmentos de edad jóvenes y medianos. El 75% de los usuarios de redes sociales le dedica, al menos, una hora al día.
- 3 de cada 4 encuestados reconocen que los menores usan Internet habitualmente en sus hogares.
- En Andalucía el 45% de la población menor de 18 años comienza a hacer uso de Internet antes de los 8 años. El 37% lo hace entre los 8 y los 10 años y el 21% entre los 11 y los 13 años. Solo un 2,3% lo hace a partir de los 13 años.
- El 42% de la población andaluza menor de 18 años se conecta a Internet de manera permanente y otro 42% se conecta 1 o 2 veces al día. Solo el 9% de la población menor de 18 años se conecta ocasionalmente.
- 2 de cada 5 menores andaluces están conectados a Internet al menos hasta las 10 de la noche, y uno de cada 5 hasta las 11 o las 12.
- 3 de cada 5 encuestados reconoce que los menores a su cargo tienen cuentas en redes sociales.
- Los anteriores horarios de uso de Internet deben sumarse a que más de la mitad de los encuestados (51,2%) reconocen que no usan ningún sistema de control parental para el acceso a Internet de los menores en su hogar.
- 3 de cada 4 personas con menores a su cargo piensan que estos no comparten datos personales o que no consumen pornografía en Internet, lo que contrasta con el escaso uso de controles parentales y puede alertarnos sobre un exceso de confianza y de deseabilidad social en estas materias.

## 6. Conclusiones generales

De los múltiples aspectos en los que un asunto tan complejo como la IA influye, en este documento se han agrupado las principales conclusiones extraídas de los distintos trabajos realizados en cuatro grandes áreas, teniendo en cuenta las funciones y competencias de un órgano como el CAA: igualdad de género, derecho al honor y a la intimidad, protección de los menores y desinformación.

### Igualdad de género

Las aplicaciones de inteligencia artificial (IA), particularmente aquellas que generan contenidos pornográficos falsos como los *deepnudes*, tienen un impacto significativo en la igualdad de género. Estas aplicaciones refuerzan estereotipos sexistas y perpetúan la ciberviolencia de género. Es notable que estas herramientas están diseñadas principalmente para desnudar a mujeres y no a hombres, lo que evidencia un sesgo de desigualdad de género inherente a la propia concepción de las mismas. La publicidad que acompaña estas aplicaciones suele ser sexista, presentando a las mujeres como objetos sexuales y vulnerables a la explotación digital.

Además, la tecnología ha cambiado las formas en que se cometen las agresiones de género, extendiendo el acoso a un ámbito digital que es a menudo más difícil de controlar y regular. La facilidad con la que se puede distribuir contenido generado por IA en las redes sociales amplifica el impacto del acoso, sometiendo a las víctimas a una invasión de su intimidad que puede ser más devastadora que la violencia física debido a su rápida y amplia difusión.

### Derecho al honor y a la intimidad

El derecho al honor y a la intimidad puede verse gravemente comprometido por las aplicaciones de IA que permiten la creación de *deepnudes* y de otros contenidos pornográficos falsos sin el consentimiento de las personas afectadas. Así, estas herramientas suponen una potencial violación de la privacidad y del honor de las personas, exponiéndolas a una vulneración de su intimidad que puede tener consecuencias devastadoras tanto a nivel personal como profesional.

La difusión de imágenes y de vídeos falsos creados por IA no solo afecta a la reputación de las personas involucradas, sino que también puede conducir a delitos de acoso, extorsión, injurias, amenazas. Las víctimas de estos actos no sólo sufren la invasión de su privacidad, sino que también enfrentan un escarnio público en redes sociales que multiplica el daño y el acoso social.

## Protección de los menores

La protección de los menores es una preocupación central para el CAA, especialmente en el contexto del acceso a contenidos audiovisuales de carácter sexual. Las aplicaciones de IA que generan contenido pornográfico falso representan un riesgo significativo para los menores, quienes pueden acceder a estos materiales sin las debidas restricciones de edad. Esta facilidad de acceso expone a los menores a riesgos de ciberacoso, explotación sexual y otros peligros asociados con el consumo de contenido inapropiado. Es necesario, por tanto, subrayar la necesidad de garantías y medidas de seguridad en el proceso de contratación y uso de tecnologías de IA para asegurar que los menores no puedan utilizar estas aplicaciones. En particular, es urgente la aplicación de medidas fehacientes de verificación de la edad, así como la promoción de una educación en valores digitales tanto para los menores como para sus padres y tutores. La educación debe centrarse en el uso seguro y responsable de las tecnologías de la información y la comunicación, así como en la comprensión de los riesgos asociados con el uso indebido de la IA, y las familias deben comprender la gravedad de los delitos que pueden cometerse contra la intimidad y asumir la necesidad de educar a los menores en valores digitales y en el respeto a la privacidad de los demás. Los datos recogidos en el Barómetro Audiovisual de Andalucía muestran que aún queda mucho camino por recorrer en la concienciación de las familias acerca de los riesgos del entorno digital, y no sólo de los derivados del uso de la IA.

Además, se recomienda una colaboración más estrecha entre las autoridades y las plataformas tecnológicas para asegurar que se apliquen y cumplan las medidas de protección necesarias para salvaguardar a los menores en el entorno digital.

## Fake news y desinformación

Las preocupaciones sobre el uso de tecnologías de IA para crear contenidos falsos también se extienden a la potencial creación y difusión de noticias falsas. La capacidad de la IA para generar textos, imágenes y videos altamente realistas presenta un riesgo significativo en términos de desinformación, ya que estos contenidos pueden ser utilizados para engañar a la ciudadanía, manipular a la opinión pública o propagar discursos de odio (sobre este último riesgo el Consejo ya emitió algún informe y sobre ello publicará el próximo número de sus *Cuadernos del Audiovisual que*, entre sus artículos de reputados investigadores, incluirá uno de aquellos informes).

La creación y difusión de noticias falsas mediante IA puede tener consecuencias muy serias, incluyendo la erosión de la confianza en los medios de comunicación y en las instituciones públicas, así como la polarización de la sociedad. Por lo tanto, es crucial que se establezcan



medidas regulatorias y de supervisión adecuadas para prevenir el uso indebido de estas tecnologías en la creación y difusión de desinformación. El CAA insiste, por tanto, en una de sus líneas principales de actuación en los últimos años: la promoción de la alfabetización mediática y digital entre la población para identificar y combatir la desinformación y en particular aquella generada por IA.

---

<sup>i</sup> Artículo 131 del Estatuto de Autonomía y Ley 1/2004, de 17 de diciembre, de creación del Consejo Audiovisual de Andalucía.