SECCION: 50. PROTECCIÓN DE DATOS Y BIG DATA

LA PROTECCIÓN DE LOS MENORES EN ENTORNOS DIGITALES FRENTE A CONTENIDOS FALSOS. LA INTELIGENCIA ARTIFICIAL COMO TECNOLOGÍA POTENCIADORA.

José Rafael Chelala Riva
Abogado del ICAM

I. APROXIMACIÓN ÉTICO JURIDICA A LA PROBLEMÁTICA

Una de las palabras de moda del año 2024 ha sido "bulo" y que es adoptada por la Real Academia de la Lengua como "mentira, engaño, embuste, patraña, habladuría camelo, infundio, bola, trola, cuento, chisma, rumor, voz, hablilla, filfa". Y lo que es más importante, su antónimo que es solo uno: "verdad". Es una palabra que, si bien ha venido utilizándose desde hace mucho tiempo, adquiere gran relevancia ahora en relación a la difusión masiva de noticias falsas y en particular a través de la tecnología y su viralización a través de plataformas digitales.

Lo cierto es que la Inteligencia Artificial ("IA"), y con independencia de todo lo bueno que conlleva esta tecnología para la humanidad, es utilizado como un instrumento muy dañino en la generación de noticias falsas y de realidades absolutamente falsas: universos "fakes".

Herramientas tan al alcance de cualquiera como puede ser ChatGPT son capaces de generar informaciones falsas sobre cualquiera y sobre cualquier circunstancia, debate o realidad, a golpe de un único *prompt*. Y no solo eso, sino que de generar de esta noticia una cantidad de distintas versiones que versen sobre la nueva "realidad", y que es falsa, y que puede difundirse en internet y en las redes sociales, incluyendo imágenes y videos a través de la avanzadísima IA generativa para así conseguir una mayor sensación de que lo que se dice es real. Esto nos podría situar ante un internet en el que la mayoría de sus contenidos en un futuro próximo podrían ser contenido falso y del que la propia IA se

nutra para sus respuestas generando una absoluta desinformación, que es otra de las palabras de moda.

La mentira, que es esencialmente de lo que hablamos, no es que sea algo nuevo. Lamentablemente es inherente al ser humano y una de las acciones más dañinas para la sociedad y muchas veces para la dignidad de las personas ofendidas. Las mentiras, que son manipulaciones, han generado enormes injusticias. Hasta nos hemos llegado a creer que una mentira si no perjudica a nadie no es algo malo, generando una sociedad donde gran parte de la información que nos llega es falsa, y también la que transmitimos a terceros. Ponemos de excusa para no ir a un sitio que un hijo se ha puesto enfermo en vez de decir que estamos cansados o que simplemente no nos apetece ir. Un debate ético interesante y que no es una novedad porque también es cierto que las mentiras pueden salvar vidas y que podrían también ser una herramienta de supervivencia desplegada a favor de terceros. Pero, en cualquier caso, lo que no se discute es que debemos de conducir la información que generamos o que propagamos hacia la veracidad. Porque, además, ahora más que nunca, podemos generar una enorme confusión a través de las tecnologías cada vez más avanzadas también en la manipulación.

Con todo ello, y en relación a medios de comunicación, entre los que inevitablemente ya están las redes sociales, se han generado agencias de verificación de noticias *fact-checking* o *anti-fakes*. Noticias principalmente políticas que están sesgadas ideológicamente, y que también difunden sus propios *fakes* que incluso una vez comprobado que no son ciertos, no se desmienten. Pero lo más grave es que se propagan informaciones falsas sin una mínima base de información y movidos por un impulso muy alejando a la búsqueda de la verdad y sin contrastarse mínimamente a través de fuentes fiables o de una mínima espera que nos permita conocer lo ocurrido y no direccionarlo de entrada hacia donde nos interesa. Pero es que incluso los organismos de control de los gobiernos entran muchas veces en este juego, y no me refiero únicamente a gobiernos de dictaduras, sino que gobiernos que consideramos "democráticos". La perdida de la lucha por la verdad, en definitiva, que nos sumerge en la decadencia.

También debemos de tener en cuenta que no siempre la difusión de la verdad, o de la realidad es lícita y/o éticamente admisible. Así, por ejemplo, las realidades que vulneren el honor y la intimidad de manera intrusiva. Conocido y desencadenante de actividad

legislativa fue el caso de la política Olvido Hormigos en la practica denominado por su tipología en el argot anglosajón como *revenge porn* que modificó el Código Penal de España en el tipo de la revelación de secretos y en su artículo 197.7[1]. Con ello, aunque la grabación de una escena intima hubiese sido consentida, la difusión no autorizada es castigada por el daño que se genera a la intimidad de la persona que entendía que dicho contenido se iba a limitar al ámbito privado.

Tampoco pueden ser exhibidas otras realidades que son delictivas por denigrantes y vejatorias incluyendo la pornografía infantil o la difusión de otro tipo de maltratos. El caso concreto de la pornografía infantil tipificado y penado en el articulo 189 del Código Penal en los delitos de producción, distribución, difusión y visionado. O en el artículo 189 bis en relación a las captación y acercamiento con menores de fines sexuales *child groming* como tipo relacionado.

También la puesta a disposición de contenidos legales que, si bien podrían considerarse veraces, en cuanto a las personas que representan una ficción, puede suponer un problema, como la pornografía lícita que sin embargo debe de regularse y asegurarse instrumentos educativos y de restricción de acceso menores, principalmente mediante el establecimiento de mecanismos de *onboarding* (acceso) efectivos.

Centrándonos en la Inteligencia Artificial y este anhelo de verdad, que no es lo mismo que verosimilitud, hoy en día con una sola imagen de una persona, gracias a la inteligencia artificial, podemos hacer que esa persona se mueva y que hable con normalidad, apariencia de real e incluso resucitar a personas para fines como pueda ser que una bisabuela a la que conocimos en una foto en blanco y negro nos felicite el cumpleaños en video a todo color.

[1] El denominada *revenge porn* ha tenido casos muy conocidos internacionalmente y en particular en cuanto a la difusión de imágenes de mujeres que fueron grabadas habitualmente de manera consentida y distribuido el contenido sin autorización con incluso webs dedicadas exclusivamente a la puesta a disposición de estos contenidos. Casos conocidos en los Estados Unidos son los de la periodista deportiva Erin Andrews (2008) o la web *"Is Anyone up?"* (2010) por el que su creador Hunter Moore fue condenado a prisión y considerado uno de los hombres mas odiados de los Estados Unidos. También la filtración masiva *Celebgate* (2014) mediante un hackeo a cuentas de ICloud de celebridades y que cuyos contenidos tuvieron una gran viralidad a través de redes sociales.

El *deepfake* es un contenido multimedia creado con inteligencia artificial que altera o genera imágenes, videos o audios de una manera extremadamente realista a través de redes neuronales profundas[2]. Este anglicismo proviene de combinar *deep learning*, por la connotación de aprendizaje profundo de las que son capaces las redes neuronales, y *fake* que su traducción es "falso". Si bien esta tecnología es una revolución en ciertas industrias como puede ser la del entretenimiento o la medicina, genera importantes riesgos como lo son la duda en relación a la veracidad o la generación de actividades criminales tanto intrusivas (sociales), como económicas. En ámbitos criminales, este tipo de contenidos podemos difundirlo masivamente, porque además cuanto más falso sea lo que diga o haga, normalmente más viral será.

Así podría considerarse el conocido y reciente asunto criminal de los desnudos no consentidos de menores en el caso conocido como *"los falsos desnudos de almendralejo"*[3], a modo de ejemplo de criminalidad intrusiva, si bien técnicamente no se trata estrictamente de un *deepfake*, más bien obedeciendo al término *deepnude* en el que mediante el uso de software de inteligencia artificial se simulan desnudos de imágenes reales, en este caso de menores de edad, obedeciendo en todo caso al mismo propósito ilícito y generando alarma social.

Si es un caso de *deepfake* en el apartado de los delitos económicos el de la multinacional británica Arup en Hong Kong, que fue estafada en 25 millones de dólares a través de una video-llamada suplantado la identidad de un alto ejecutivo, que ordenaba una transferencia bancaria[4]. Esto nos ofrece una perspectiva de la envergadura del problema.

Desde el punto de vista de derecho penal, se abre un nuevo abanico delictivo o, mejor dicho, delitos existentes y tipificados la mayoría de ellos, se potencian de manera

[2] Principalmente los GAN (*Generative Adversarial Networks*) que es un tipo de inteligencia artificial cuya tecnología introducida en 2014 se basa, sintetizando mucho, en dos componentes competitivos: generador y discriminador. El primero genera contenidos que deben de ser lo suficientemente realistas para engañar al segundo cuya función será la de detectar las diferencias entre los datos reales y los generados.

[3] https://www.eldiario.es/extremadura/sociedad/caso-falsos-desnudos-menores-almendralejo-generados-inteligencia-artificial-llegara-bruselas_1_10667663.html

[4] https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

exponencial multiplicando los riesgos frente a victimas cada vez más vulnerables debido a la apariencia de veracidad de un sitio web, de un email, de una imagen, de una voz o de un video. Incluso provocando engaños a otros sistemas informáticos como puede ser Apps de banca electrónica. Y detrás de todo esto grupos criminales muy especializados y muy difíciles de localizar debido principalmente a las dificultades de rastreo y aplicación de legislaciones concretas: *country hop.* Y a la absoluta falta de contacto con la victima que genera una nula empatía con cualquier situación personal, desplegando los delincuentes los ataques como bombas, poniendo cebos y echando redes donde se pesca a quien caiga. De aquí que las estafas informáticas se las denomine *phishing* expresión que proviene del inglés *fishing* (pescar)[5].

Concretamente y en relación a los contenidos falsos a través de tecnologías de inteligencia artificial, se instrumentaliza de manera avanzada la realidad para la generación de información falsas. Se manipula precisamente gracias a la alteración de la realidad. Dentro de estas dinámicas criminales los mencionados *deepfakes* maliciosos que en nuestro ordenamiento se encuadrarían dentro del tipo del Art. 284.1. 2º del Código Penal.

Abre ello un nuevo campo de actuación y de investigación forense sobre la veracidad de los contenidos generados a través de inteligencia artificial ya sea a través de investigaciones humanas o de tratamientos automatizados. Utilizando a modo de ejemplo el *deepfake*, puede tratarse de la detección de movimientos oculares anómalos, parpadeos extraños, bordes o siluetas difuminadas, errores en la sincronización de voz en imagen. También mediante el uso de herramientas avanzadas cuyo propósito sea detectar estas manipulaciones incluyendo la utilización de test de empatía similares al estilo de la prueba de *Voight-Kampff* recreado en la película Blade Runner. En el caso de autentificaciones de acceso a sitios webs o aplicaciones (*Apps*), también cabe destacar el uso de sistemas aleatorios o las múltiples verificaciones de identidad.

[5] La "Ph" en lugar de la "F" proviene de la jerga de los hackers de las décadas de los ochenta y noventas. En aquella época, los *phreakers* eran hackers que manipulaban sistemas telefónicos. El término en la actualidad ha evolucionado hacia otras expresiones similares, relacionadas todas ellas con estafas informáticas. Entre ellas:
Spear phishing: se refiere a cuando un ataque va dirigido a personas o empresas concretas.
Whaling: ataques dirigidos a las cúpulas empresariales y grandes ejecutivos.
Smishing y Vishing: Estafas tecnológicas a través de textos o llamadas telefónicas.
Pharming: Redirección del tráfico a sitios web falsos.

Pero no toda manipulación mediante inteligencia artificial es constitutiva de delito estando las redes sociales plagadas de contenidos ficticios de gran realismo que pueden inducir a confusión especialmente a los menores, y no solo eso, sino que enganchar al menor a esa búsqueda sin límite de contenidos que llaman su atención generando problemas de adicción e incluso patologías y trastornos importantes que han llegado en algunos casos hasta el suicidio.

II. SOBRE LA PROTECCIÓN AL MENOR FRENTE A CONTENIDOS FALSOS O DAÑINOS EN PLATAFORMAS TECNOLÓGICAS DESDE LA PERSPECTIVA DE LA PRIVACIDAD Y DE LOS DERECHOS DIGITALES. INCIDENCIA DE LA IA.

El articulo 8 del Reglamento General de Protección de Datos (en adelante también "RGPD")[6], establece el umbral del consentimiento a partir de los 14 años para el tratamiento de los datos de carácter personal, lo cual ha sido adoptado en la legislación española en la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (en adelante también "LOPDGDD")[7] ,y el mandato que la Unión Europea atribuye a la Agencia Española de Protección de Datos (en adelante también "AEPD"), con competencias especificas en relación a la protección de menores en entornos digitales, incluyendo la exposición a contenidos que pueden ser perjudiciales.

Asimismo, el reciente Reglamento Europeo de Inteligencia Artificial[8] "IA Act", fija bases regulatorias en relación a la adopción de la IA buscando su utilización de una manera ética, segura y respetuosa con los derechos fundamentales y enfocado en los riesgos de la tecnología estableciendo niveles de riesgo e incluso prohibiciones de su uso.

[6] https://www.boe.es/doue/2016/119/L00001-00088.pdf

[7] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[8] https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079

Otro texto importante en el ámbito de la Unión Europea es el Reglamento de Servicios Digitales[9] (DSA) que regula la prestación de servicios digitales incluyendo a las plataformas de redes sociales, y que pretende un entorno digital más seguro, transparente y responsable.

No es objeto de este artículo desplegar las políticas actuales tanto europeas como de nuestra AEPD en materia de privacidad y de protección al menor, sino que ofrecer unas ideas de innovación jurídica en cuanto a cómo afrontar los problemas y cuestiones relacionadas con este asunto tan sensible, y en particular con el factor potenciador de la IA y a la aproximación realizada en el apartado anterior del artículo hacia la búsqueda de un contenido lícito y veraz. Tampoco pretendo discutir o dar mi opinión sobre si la IA es buena o mala para el ser humano, ya que no existe marcha atrás y la capacidad de maniobra es limitada en el ámbito regulatorio, por lo que debemos considerarla una nueva realidad en la vida actual y futura. Y que además jugará transversalmente en toda la sociedad y hasta el punto de que muy probablemente modifique definitivamente aspectos importantes de nuestras vidas. Por muy pesimistas que seamos o sean algunos en cuanto a su desarrollo, lo cierto es que habrá enormes esfuerzos aceleracioncitas de la IA que afectarán a todos. Y muchos desarrollos contribuirán a la solución de problemas sin resolver o a aumentar el bienestar de la sociedad.

Con ello, y esto es mi opinión adquirida por la observación y que no fue mi visión original, no debemos de generar una IA al servicio del ser humano y de sus pretensiones (*superalightment*), sino que una IA que proteja y principios éticos basados en derechos humanos fundamentales (*sentinent alighment*), y a poder ser mejorándolos. En definitiva, esfuerzos tendentes a que en este exponencial desarrollo de la IA se le dote de principios éticos y morales y en especial en cuanto a la toma de decisiones autónomas.

Volviendo a partir del principio de identificación de lo que es un contenido veraz del que no lo es, resulta claro que, si por ejemplo instituciones financieras con todos los sistemas de ciberseguridad que mantienen son engañadas sistemáticamente por aplicaciones

[9] https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573

maliciosas que utilizan la IA, la dificultad de identificación para un menor de edad en relación a la veracidad de un contenido es mucho más débil. Estando además el menor muy familiarizado con entornos y realidades digitales que fácilmente se confunden con lo real; lo que también puede ser considerado lo digital, ya que lo digital no deja de ser una realidad, que puede ser o no veraz, creíble o increíble.

Lo cierto es que los sistemas de acceso, *interfaz* de usuario, a contenidos, y en particular audiovisuales y en redes sociales han sido diseñados de una manera absolutamente intuitiva para la navegación de los menores y para generar el mayor confort cerebral, que tiende a acomodarse siempre al mínimo esfuerzo y por lo tanto al menor consumo energético, de ahí la dificultad de instaurar ciertos hábitos saludables. Con ello, resulta mucho más gratificante en lo que a esfuerzo se refiere para el menor de edad la navegación en contenidos audiovisuales que otras actividades como puedan ser la lectura o el deporte. Con ello se genera conductas, hábitos adictivos y de baja socialización del menor. Y además sin discernir si el contenido al que se exponen es falso o es auténtico, restando importancia a este factor tan crucial y considerando todo como un mero entretenimiento. Ello sin entrar en otras cuestiones relevantes como el acceso a contenidos inapropiados, pero sin olvidar que la adicción a ciertas redes sociales ya es de por si un problema de extremada gravedad.

Con todo ello hay ciertas propuestas legislativas que pueden ser interesantes tendentes a la protección del menor en el ámbito tecnológico y en particular en cuanto a tecnologías avanzadas como lo es la IA. Por supuesto que algunas de ellas se están implementando a través de organismos y legislaciones, pero lo que hay no es suficiente y en muchos casos no se ha abordado correctamente debido a distintas causas que se puede intuir a continuación:

1) **Educación en la identificación de contenidos falsos o manipulados**:

A través de la educación se debe de dotar al menor de mejores herramientas críticas para discernir si un contenido es falso o auténtico. Los ya abordados *deepfakes* o los textos automatizados dificultan aún en mayor medida la identificación de estos contenidos falsos o modificados. Debe de considerarse y educarse al menor en el sentido de que la mayoría de los contenidos son falsos o que pueden estar manipulados para llamar la atención del

espectador, y que salvo en ciertos entornos, todo debe de ser cuestionado. Con ello toman especial reverencia las fuentes fiables y los entornos seguros. Dentro de la formación se debe de incluir la alfabetización mediática y en particular en relación a entornos tecnológicos advirtiendo de los riesgos que se generan debido a sistemas de IA cada vez más avanzados. Algunos de estos proyectos han sido impulsados en España, a modo de ejemplo, Internet Seguro por Kids[10] (IS4K) del Instituto Nacional de Ciberseguridad de España (INCIBE), o Mentes AMI de la Fundación Atresmedia[11]. Pero se hace necesario una acción mucho más profunda integrándolo de manera obligatoria en los planes de estudio como sucede en países como Finlandia, Suecia, Australia o Japón. Poniendo como ejemplo a este último país, la alfabetización mediática es parte de la educación obligatoria y está orientada a desarrollar el pensamiento critico y el uso ético de los medios sociales. Por ejemplo, se enseña a los estudiantes a discernir entre información confiable y desinformación.

2) Generación de entornos digitales seguros para menores.

Es conocido, que la versión para China de *TikTok* (ByteDance) *denominado* ***Douyin*** tiene contenidos completamente distintos a la denominada versión internacional *TikTok*. La versión china es muy estricta en cuanto a sus contenidos y si bien controlados por el gobierno, se trata de contenidos que fomentan la educación, moralidad y el desarrollo cultural. En cambio, la versión internacional incluye todo tipo de contenidos sin limitarse a contenidos educativos, siendo una plataforma de contenido viral destinado a que el usuario permanezca en ella el mayor tiempo posible y donde el uso de la IA es cada vez más patente. En pocos casos es anunciado el uso de IA, exhibiendo contenidos no siempre aptos y que pueden generar impactos negativos. También la versión china de la aplicación tiene un límite diario de uso que es *(seuo)* de 40 minutos y está perfectamente delimitada por la plataforma para menores y definido por el algoritmo a las mencionadas finalidades. En países como los Estados Unidos se pretende la prohibición de la red social TikTok para el año 2025 ya que se ha considerado que incluso supone un riesgo para la seguridad nacional.

[10] https://www.incibe.es/incibe/informacion-corporativa/con-quien-trabajamos/proyectos-europeos/is4k

[11] https://fundacion.atresmedia.com/Mentes-AMI/

Se debería por tanto de fomentar el desarrollo de plataformas destinadas a menores que sean seguras y con contenidos educativos, garantizando un bueno uso de la IA. Debemos de tener en cuenta que estos contenidos son los que de manera significativa generan el desarrollo intelectual del menor y que resulta obvio que la educación genera una ventaja competitiva en el futuro desarrollo de la personalidad del menor, añadiendo los riesgos que suponen los contenidos que únicamente se guían por un algoritmo de satisfacción del usuario.

3) **Políticas de desconexión digital y restricciones en el uso de tecnologías avanzadas.**

Aunque no exista un tiempo de exposición máximo que podamos considerar universalmente aceptado, si que existen recomendaciones basadas en franjas de edad. Así por ejemplo al Organización Mundial de la Salud (OMS) considera que en menores de 2 años no debe de existir ningún tipo de exposición a pantallas, y que entre 2 y 4 años el máximo debe de ser de 1 hora diaria. Otras instituciones como el *Common Sense Media* (CMS) realizó un informe en el año 2021: "*The Common Sense Census: Media Use by Tweens and Teens*"[12] destinado a concienciar sobra la necesidad de desconexión digital por ejemplo antes de dormir, limitar los contenidos inapropiados o poniendo en evidencia que los adolescentes pasan mucho más tiempo delante de pantalla que el recomendado. Y así otras muchas instituciones se han pronunciado en sentido similar como la Academia Americana de Pediatría (APP) o UNICEF. También la AEPD ha desarrollado distintos informes para la protección de los menores en el entorno digital y de hecho en octubre de 2024 ha publicado el informa "Internet seguro por defecto para la infancia y el papel de la verificación de edad"[13], además de otros informes anteriores y todo ello en consonancia con las políticas europeas impuestas por el RGPD. Así también existen importantes estudios de otras agencias internacionales como por el desarrollado por la Oficina del Comisionado de Información del Reino Unido (ICO) que publico el *"Age Appropiate*

[12] https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021

[13] https://www.aepd.es/guias/nota-tecnica-internet-seguro-por-defecto-para-la-infancia.pdf

Design Code"[14] o por parte de la Comisión Nacional de Informática y Libertades de Francia (CNIL)[15] poniendo de manifiesto la necesidad de protección de los menores a través de directrices.

Sin embargo, pese a que en ocasiones por parte de la propia AEPD se ha llegado a manifestar que el consumo digital excesivo es peor que el tabaco y el alcohol, estas políticas no se transmiten, en mi opinión, de manera acertada interactuando por ejemplo con los padres y tutores que desconocen cómo gestionar y limitar los accesos de los menores a contenidos y exposiciones excesivas o cómo gestionar adecuadamente un incidente con un menor en el ámbito digital, muchos de ellos con connotaciones de abusos y/o sexuales.

Por otro lado, ha de indicarse que se debe de abrir la discusión a la limitación de tipos de dispositivos accesibles según la edad del menor o a la implementación de soluciones técnicas efectivas que dentro de la legalidad permitan concluir la edad real, y sin vulnerar la privacidad. Que permitan por ejemplo de forma automatizada gestionar contenidos de una manera adecuada utilizando como instrumento soluciones de IA. De hecho, ya existen ciertas soluciones enfocadas en este sentido como Bark, Qustodio, Google Family Link, SafeToNet o Canopy. Cada una con sus peculiaridades, pero todas con componentes de IA y que sin embargo son ampliamente desconocidas proponiéndose muchas veces por las instituciones públicas soluciones obsoletas o de muy difícil o imposible implementación.

También debemos de contemplar el debate existente no ya de la no utilización de los *smartphones* en las aulas, sino de restricciones o prohibiciones más amplias a este tipo de dispositivos hasta ciertas edades, evitando así conflictos y comparaciones entre los menores.

[14] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[15] https://www.cnil.fr/fr/thematiques/les-droits-numeriques-des-mineurs

4) **Políticas consensuadas y despolitizadas en relación al impacto de las tecnologías en los menores.**

Existe asimismo una necesidad de consenso político que puede ser perfectamente desplegado a través de instituciones como la AEPD y en particular en lo relativo al impacto de la inteligencia artificial en menores, haciéndose necesario un pacto de Estado a este respecto por el impacto en la privacidad de los menores. Pese a que este pacto parece que esta en marcha, es necesario que se implemente de una manera efectiva a la mayor brevedad y fuera de condicionamientos políticos buscando una posición de neutralidad para proteger al menor. Por ahora viene siendo un fiasco la adopción de soluciones de acceso a contenidos inapropiados, pero sin embargo es una necesidad que existan regulaciones claras y que permitan a todos los operadores desenvolverse con seguridad jurídica. Existen compromisos, pero no se ejecutan y esto genera un enorme daño a la sociedad, por no decir una injusticia hacia el conjunto de la ciudadanía. Pese a que el pacto aborda la inteligencia artificial como herramienta de protección del menor, lo cierto es que tarda en adoptarse sin que existan hasta la fecha compromisos políticos claros para una cuestión tan urgente, y priorizándose cuestiones ideológicas con debates de mucha menor importancia.

III. Conclusión.

El despliegue efectivo de estas cuatro ideas, sería un avance importante para no exponer a los menores a contenidos falsos o manipulados por IA, y también para implementar y desplegar la IA en beneficio de los menores. Por mucho que exista una legislación, esta debe de implementarse de manera efectiva y fuera de connotaciones políticas que muchas de ellas son absolutamente contradictorias con la protección del menor, como es el caso de ciertas políticas educativas de hipersexualización. Las instituciones públicas deben de actuar de manera responsable y ética apartando las ideologías y fomentando el normal desarrollo de la personalidad de los menores en un ambiente lo más seguro posible. Ahora más que nunca la veracidad de la información debe de ser protegida y para ello será necesario alejar los constantes sesgos políticos. La educación digital es fundamental tanto para adultos como para menores porque la tecnología forma parte de las actuales ciencias sociales. Si la cuestión no puede ser abordada por la administración pública de una manera efectiva, como está aconteciendo en algunos casos, se hará necesario que sean las

personas físicas y jurídicas las que asuman la responsabilidad para la propia supervivencia de nuestra sociedad. Todos formamos un grupo de interés frente a la desinformación y en la protección de la privacidad. En la medida de nuestras capacidades, responsabilidades y posibilidades debemos de defender la verdad, cueste lo que cueste, para que la tecnología no transforme nuestra sociedad en un caos de mentiras y de intrusión en la privacidad de las personas. Y así que la IA nos ayude a mejorar la forma en la que viviremos en el futuro.