IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los *deepfakes**

THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION OF GENDER CYBERCRIME: THE RISE OF DEEPFAKES

Irene González Pulido
Investigadora postdoctoral "Margarita Salas"
Área de Derecho procesal.
Universidad de Salamanca/ Universidad de Extremadura
irenegopu@usal.es 0000-0001-8098-350X

Recibido: 03 de noviembre de 2023 | Aceptado: 08 de diciembre de 2023.

RESUMEN

El auge de la inteligencia artificial generativa ha condicionado el devenir de los modus operandi de los ciberdelitos de género; destacando la utilización de los deepfakes. En la actualidad, preocupa la rápida adecuación y adaptación por parte de los ciberdelincuentes, en contraposición al lento desarrollo de una regulación de los diferentes sistemas de IA. El empleo de las tecnologías más novedosas para la comisión de ciberdelitos de género aumenta los obstáculos que ya encontraban las autoridades policiales y judiciales en la práctica de investigaciones en Internet. Estas cuestiones han determinado que en el presente estudio se apueste por analizar la necesidad de implementar los sistemas de IA generativa como herramientas de investigación tecnológicas, proponiendo diferentes líneas de actuación a corto, medio y largo plazo para conseguir materializar investigaciones salvaguardando todas las garantías y, por consiguiente, finalizar este tipo de procesos penales con éxito.

PALABRAS CLAVE

Inteligencia artificial
Generativa
Deepfakes
Ciberdelincuencia
Violencia de género
Investigación tecnológica

* Actualmente en el centro de destino del primer año: Área de Derecho procesal de la Universidad de Extremadura. Beneficiaria de una ayuda para la recualificación del sistema universitario español para 2021-2023, modalidad "Margarita Salas". Resolución Complementaria de 30 de junio de 2021 de la Universidad de Salamanca, en el marco del Real Decreto 289/2021, de 20 de abril, (BOE núm. 26 de 22 de abril de 2021), así como en la Orden del Ministerio de Universidades UNI/551/2021 de 26 de mayo. Instrumento Europeo de Recuperación («Next Generation EU»).

ABSTRACT

The rise of generative artificial intelligence has conditioned the evolution of the modus operandi of gender cybercrime, especially the use of deepfakes. Currently, there is concern about the rapid adaptation by cybercriminals, as opposed to the slow development of regulation of AI systems. The use of the latest technologies for the commission of gender-based cybercrime increases the obstacles already encountered by law enforcement and judicial authorities in the practice of Internet research. The present study focuses on analyzing the need to implement generative AI systems as technological research tools, proposing different lines of action in the short, medium and long term in order to carry out investigations that safeguard all the guarantees and, consequently, this type of criminal proceedings.

KEYWORDS

Generative artificial
Intelligence
Deepfakes
Cybercrime
Gender violence
Technological research

I. Aproximación a la inteligencia artificial generativa

Para realizar una aproximación a la inteligencia artificial generativa, tenemos que destacar tres ideas principales. La primera está relacionada con las funciones de la inteligencia artificial (en adelante, IA) y, en particular, con el alcance de la IA generativa, ya que solo de este modo podremos dar paso a las otras dos ideas, basadas respectivamente en su previsión legal y en su incorporación a los *modus operandi* de los ciberdelitos de género.

Como hemos señalado, la segunda de las ideas que se abordará en el presente estudio está relacionada con la apuesta por una regulación a nivel europeo que prevea unas condiciones y unas prohibiciones que permitan a la comunidad europea controlar los sistemas IA que se están implementando y que están siendo utilizados por su ciudadanía. Sistemas IA entre los que se han incluido algunas funciones relativas a la posibilidad de falsificación que ofrecen los sistemas de IA generativa y, más recientemente, la mención expresa de este tipo de IA, así como de los modelos fundacionales.

La tercera idea está relacionada con la acogida de estos sistemas por parte de la ciudadanía y con la adaptación de los ciberdelincuentes ante estas nuevas tecnologías. Por un lado, la utilización de este tipo de IA favorecerá el progreso tecnológico, su implementación a nivel de la UE, pero, por otro lado, también supondrá un obstáculo para la consecución de los objetivos de las autoridades policiales y judiciales que deben perseguir los ciberdelitos que se sirven de estas tecnologías; en el presente estudio atenderemos a los que han sido denominados ciberdelitos de género. El motivo de esta elección se debe a la tendencia al alza de la utilización de esta tecnología en los últimos meses (del Castillo, 18 de septiembre de 2023; Navarro, 21 de diciembre de 2022; Viejo, 3 de octubre de 2023) atentando contra los derechos de mujeres y niñas[1].

1. Sin perjuicio de que también los niños están siendo víctimas de algunas conductas delictivas de esta índole, la victimización es mayor en el caso de niñas. Véase, por ejemplo, el documento de enmiendas realizadas por la Comisión de Derechos de las Mujeres e Igualdad de género a la Propuesta

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

Desde hace varias décadas se han identificado múltiples funciones de la IA. En la Comunicación de la Comisión Europea de 2021 se destacaron, por un lado, como *software* sus funciones de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento facial y de voz, asistentes de voz, traducción de textos, generación de subtítulos, identificación y bloqueo de spam, etc. Y, por otro, se incluyó la posibilidad de incorporar la IA a dispositivos *hardware* desarrollando robots avanzados, automóviles autónomos, drones o aplicaciones del Internet de las cosas, etc. Desde este primer momento se identificó que podría favorecer, en general, a la Administración de Justicia y, en particular, la lucha contra la delincuencia, combatiendo incluso formas graves con mayor eficacia[2]. Por ejemplo, se manifestó que podría contribuir a la lucha contra la delincuencia organizada destacando su potencial para analizar grandes cantidades de datos y para la práctica de investigaciones en la *darkweb* (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025, 14 de abril de 2021). No obstante, desde el momento en el que se apostó por este tipo de tecnología también se detectaron los riesgos y las amenazas que podrían emerger del desarrollo y la expansión de la IA.

Con carácter específico, en atención a las enmiendas a la Propuesta de Reglamento de IA para la UE, aprobadas el 14 de junio de 2023 por el Parlamento Europeo, podemos definir la IA generativa como los "sistemas de IA destinados específicamente a generar, con distintos niveles de autonomía, contenidos como texto, imágenes, audio o vídeo complejos" (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023). Por lo tanto, en el marco de la IA generativa encontramos diversas herramientas diseñadas para la práctica de diferentes funciones, entre las que destacaremos algunas de las que se han considerado más relevantes para el presente estudio.

Por un lado, encontramos modelos de lenguaje generativo, entre los que desataca ChatGPT, que a priori no responde preguntas clasificadas como dañinas o ilícitas, pero sin embargo, se ha demostrado que utilizando algunas estrategias específicas para orientar los *prompts* o indicaciones se podrían eludir las medidas de seguridad. Continuamente se está desarrollando y mejorando la *prompt engineering* (Europol, 27

---

de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores. Enmiendas 46-536. 8 de mayo de 2023. 2022/0155(COD).

Las propuestas aquí analizadas perseguirán su implementación para la protección de todas las víctimas menores de edad, ya que como se ha incorporado en las enmiendas a la última propuesta de Reglamento en la que se apuesta por reforzar la lucha contra el abuso sexual de menores, nos encontramos ante una amenaza grave que afecta particularmente a la UE. Véase enmienda 286, de 30 de mayo de 2023, realizada por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior. 2022/0155(COD).

2. Se señaló que "La IA puede ayudar a luchar contra la delincuencia y el terrorismo, y permitir a las fuerzas o cuerpos de seguridad seguir el ritmo del rápido desarrollo de las tecnologías utilizadas por los delincuentes y sus actividades transfronterizas" (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Fomentar un planteamiento europeo en materia de inteligencia artificial, 21 de abril de 2021).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

de marzo de 2023). Por otro lado, encontramos aplicaciones que se sirven de sistemas IA que funcionan generando imágenes a partir de una entrada de texto; otras que sirven para manipular imágenes preexistentes; para combinarlas e incluso para superponer imágenes diferentes o para insertarlas en un vídeo específico; el desarrollo de este tipo de aplicaciones está siendo exponencial, las combinaciones son múltiples y los resultados cada vez están más mejorados, aproximándose cada día más a la realidad sin manipular[3].

En este marco de análisis tenemos que destacar el auge, a lo largo del último año, de algunas aplicaciones que se sirven de sistemas de IA generativa, ejemplo de ello lo encontramos en el "Chat GPT-4" o "Midjourney". Este auge y desarrollo exponencial de la IA generativa ha provocado que los expertos se cuestionen ante qué tipología de sistemas IA nos encontramos cuando implementamos estos programas que, día tras días, son más numerosos y variados. Parece que la propuesta de Reglamento original se redactó en términos de funcionalidad, es decir, persiguiendo evitar la obsolescencia de la tecnología apostando por clasificar los sistemas IA en función de su aplicación específica, bien haciendo referencia a un sector, como la Administración de Justicia, o bien en atención a la acción específica que permite, como podría ser la perfilación (Villatoro González y Camblor Echanove, 16 de junio de 2023).

No obstante, este planteamiento parecía no dar respuesta a este tipo de sistemas, por lo tanto, el Parlamento europeo ha apostado por aprobar una serie de enmiendas al respecto, el pasado 14 de junio de 2023. Se ha incluido, en primer lugar, la definición de los "modelos fundacionales", que caracterizan el funcionamiento de los sistemas de IA generativa[4], como modelos entrenados con grandes volúmenes de datos, diseñados para la producción de información y para la práctica de una gran variedad de tareas. En este mismo sentido se ha incluido la definición de "Sistema de IA de uso general" para dar cobertura jurídica a los que no se han diseñado específicamente para realizar una función concreta en un ámbito localizado, sino que "puede utilizarse en aplicaciones muy diversas". En este sentido se han recogido diversas funciones y obligaciones inherentes a los proveedores o implementadores de este tipo de sistemas de IA o modelos fundacionales.

En definitiva, tras dichas enmiendas a la Propuesta de Reglamento de IA de la Unión Europea parece clara la apuesta por la regulación de este tipo de sistemas de IA generativa, con el objetivo de que se cumplan los principios y las obligaciones necesarias para garantizar un uso de esta tecnología salvaguardando los valores de la UE y los derechos de su ciudadanía. Sin perjuicio de que esta propuesta esté en curso y se prevea que el próximo año estará vigente, la adecuación de la ciberdelincuencia de nuevo se

3. Desde Trend Micro se apuesta por clasificar estos *deepfake* en atención a la manipulación realizada: reemplazo de la cara de una persona por la de otra; reconstrucción facial; generación de rostros totalmente ficticios; generación de contenido de audio o de voz; creación de falsificaciones audiovisuales; etc.

4. Se hace mención expresa a esta vinculación de los modelos fundacionales y la IA generativa en el artículo 28 ter relativo a las obligaciones del proveedor de un modelo fundacional, en su apartado cuatro. (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

ha adelantado al desarrollo normativo y, en este sentido, continuaremos con la última idea de esta breve aproximación.

En este contexto, por lo tanto, tenemos que destacar que la IA se presenta como una oportunidad para los ciberdelincuentes; mejoran sus ataques, obtienen más beneficios en menos tiempo, acceden a nuevas víctimas, crean medios de ataque más innovadores, refuerzan su anonimato y pueden hacer uso de estos sistemas con pocos conocimientos técnicos, incluso pudiendo practicar técnicas de hackeo (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). En el marco de la ciberdelincuencia pura o de alta tecnología, la implementación de la IA podría favorecer la ocultación del *malware,* su activación y la práctica de ataques persistentes. Por supuesto, también se ha puesto de manifiesto la posible mejora de los *malware* empleados en el marco de la ingeniería social con la utilización de la IA (Europol, 2020). En este contexto delictivo, también va a ser relevante el desarrollo de la IA generativa, como analizaremos a continuación.

En este mismo sentido, se ha identificado que los ataques *ransomware,* posicionados en la cúspide de las ciberamenazas de alta tecnología y que también comprometen las infraestructuras críticas, si se acompañan por inteligencia artificial podrían tener efectos devastadores, ya que optimizaría la infección y sus efectos. En este sentido se podrían ver comprometidos servicios esenciales y tener graves consecuencias en la vida *offline* (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

En atención a la posibilidad de sortear mecanismos de seguridad con sistemas basados en IA, se ha identificado un *software* que permite atacar al sistema de seguridad CAPTCHA, favoreciendo el acceso automático a bases de datos, acceso de sistemas IA a esta información e incluso se emplea para el acceso automatizado a foros u otras plataformas de interacción. Junto a esto se podrían sortear los sistemas existentes para la detección de redes de *bots*, lo que favorecería la simulación de actividad humana en determinados contextos, cuando esta puede ser inexistente, por ejemplo, en redes sociales (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Este tipo de ciberataques basados en el engaño, como ha sido publicado por Trend Micro, también suponen una amenaza para la industria de los *eSport*, tanto con ánimo de lucro como con el objetivo de blanquear dinero. También los sistemas de los juegos en línea podrían ser atacados mediando la utilización de IA. Con esta misma finalidad, destacan las herramientas IA, generalmente *bots* que se utilizan para el comercio financiero, para el comercio de criptomonedas, empleando el análisis de estrategias de negociación y realizando predicciones de las operaciones (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). La obtención de financiación y el blanqueo de capitales han sido actividades clave para el mantenimiento de grandes organizaciones criminales, sin perjuicio de que puedan perpetrarse estos ataques por otro tipo de delincuentes al margen de dichas organizaciones. En este sentido, es destacable que la IA puede servir para potenciar la práctica de otras actividades transversales necesarias

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

para materializar los ciberdelitos de género, ya sea con carácter previo o posterior, entre las que destacan la ya citada financiación o el blanqueo de los beneficios obtenidos.

También se ha previsto por los investigadores la utilización de sistemas IA para la obtención de claves y contraseñas que pueden permitir el acceso a plataformas, aplicaciones o sistemas (Europol, 2020). Este tipo de actuación podría dar lugar a la comisión de toda una variedad de conductas delictivas, en atención al contenido al que se pudiera acceder (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020), incluyendo ciberdelitos de género entre las mismas.

La IA además puede ser utilizada para proteger la propia infraestructura delictiva y eliminar evidencias, permitiendo la programación y destrucción automática (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). Esta cuestión complicaría la práctica de investigaciones que impliquen diligencias de investigación tecnológicas complejas; como son el agente encubierto informático o el registro remoto. Sin perjuicio de que, con carácter general, se obstaculizaría la obtención de cualquier tipo de evidencia y, por consiguiente, se comprometería el éxito de la investigación y del proceso penal en su totalidad.

En definitiva, podemos afirmar que las funciones que ofrece la IA a la ciudadanía en general no han quedado al margen de la actuación de los ciberdelincuentes, sino que los últimos avances en materia de IA se están empleando para atentar contra múltiples bienes jurídicos, persiguiendo diferentes objetivos. De este modo, como hemos apuntado, las autoridades competentes para practicar la investigación de los delitos que se perpetren utilizando este tipo de sistemas encontrarán numerosas dificultades, añadidas a las que ya existían en el marco de la persecución de los ciberdelitos más tradicionales que se cometían a través de Internet desde su aparición.

II. IA generativa como método utilizado para la comisión de ciberdelitos

Como se ha señalado en la Propuesta de Reglamento de IA de la UE, esta tecnología puede servir para optimizar y personalizar las operaciones, incluidas las policiales y judiciales, pero también su desarrollo nos obliga a identificar nuevos riesgos. En particular, como se ha introducido en el epígrafe anterior, en lo que respecta a la IA generativa, detectamos cambios y adaptaciones en los *modus operandi* de determinados tipos delictivos.

En el reciente estudio elaborado por Europol se han identificado algunas utilizaciones de sistemas de IA generativa que pueden fomentar, facilitar o mejorar la comisión de determinados tipos delictivos. Como modelo de lenguaje generativo por excelencia destacamos de nuevo el ChatGPT, tanto su versión 3,5 como la 4, podría utilizarse con finalidades ilícitas; tanto para la práctica de algunas conductas más leves como de otras más graves, siendo útil para complementar delitos de terrorismo, de abuso sexual de menores o ciberdelitos que han sido considerados como puros (Europol, 27 de marzo

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

de 2023). Entre las funciones claves detectadas por Europol, por un lado, es destacable la capacidad de redacción de textos de un modo similar al que lo harían los humanos, siguiendo modelos específicos y adecuándose a necesidades o situaciones concretas. Por lo tanto, se puede favorecer la suplantación de identidad y del estilo de escritura y, por consiguiente, se pueden perfeccionar las técnicas de ingeniería social, el *phishing* y, de este modo, se mejoran algunas tipologías delictivas que llevan años practicándose, como los fraudes en línea; como puede ser el fraude del CEO. Asimismo, eludiendo las restricciones del sistema podría facilitarse la redacción de textos que fomenten la desinformación, la incitación al odio, el adoctrinamiento terrorista, etc. (Europol, 27 de marzo de 2023). Las estafas en las que se utiliza ingeniería social también podrían optimizarse, facilitando el trabajo y favoreciendo el éxito de los ciberdelincuentes (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Por otro lado, desde la aparición en noviembre de 2022 del ChatGPT, una de las cuestiones que más ha preocupado ha sido su capacidad para generar código en diferentes lenguajes de programación, esta función del ChatGPT podría ser utilizada con fines maliciosos para la comisión de múltiples actividades delictivas, incluso por personas que no son expertas en informática para el desarrollo de *malware*. No obstante, se apunta que en la actualidad el desarrollo de esta función es bastante sencilla, pero se estima que en un futuro este tipo de sistemas se mejoren, como ya se ha hecho con respecto a la primera versión que se publicó del chat (Europol, 27 de marzo de 2023). En la actualidad se ha detectado lo que se denominan "alucinaciones" de forma coloquial, debido a algunas imprecisiones en su uso habitual (Retana Gil, 19 de octubre de 2023).

La mejora de *malware* es una de las características que va a permitir aumentar la eficacia de las actividades ilícitas; por ejemplo, los sistemas de lenguaje o gramática generativa pueden ayudar a sortear los filtros del spam y acceder a un mayor número de víctimas sin ser identificados (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). Es decir, se podrá implementar este tipo de sistemas de IA generativa, basados en lenguaje, para eludir mecanismos de seguridad y control que llevan años establecidos. En este mismo sentido, investigadores han demostrado que se podría camuflar *malware,* pasando desapercibido ante los antivirus, incluso de aquellos que se sirvan de IA para mejorar su eficacia (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Desde el estudio de investigación que ha publicado Trend Micro respecto a las amenazas de la IA y al abuso de estos sistemas también se ha recogido como la IA generativa podría implementar las llamadas automáticas para cometer estafas de diversa índole, incluso simulando la voz de personas conocidas; para generar voces y quebrantar sistemas de seguridad que funcionan por autenticación de voz en entidades bancarias (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020); entre otras modalidades delictivas que podrían surgir del desarrollo y la evolución de este tipo de sistemas.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

Entre las posibilidades de empleo de la IA generativa, son destacables los *deepfakes* o vídeos ultra falsos que se ha identificado que son producto de la manipulación de material multimedia preexistente o bien de su generación a través de técnicas de *machine learning,* con el objetivo de reemplazar a otras personas, simulando que son reales; se pueden encontrar imágenes, vídeos, audio... Es decir, con este tipo de tecnología se puede conseguir mostrar de forma convincente a personas que existen, han existido o que nunca existieron, haciendo y/o diciendo cosas que nunca hicieron y/o dijeron (Europol Innovation Lab, 2022). En concreto, no podemos afirmar que no existiera esta técnica con carácter previo al desarrollo de la IA, sin embargo, sí podemos concretar que se ha facilitado, agilizado y extendido su posible práctica gracias a las ventajas de este tipo de sistemas (Simó Soler, 2023).

La generación de *deepfakes* es una de las utilidades de la IA que ha sido identificada como una de las más empleadas con fines maliciosos y como una de las más dañinas, advirtiendo de que el desarrollo y la evolución de esta tecnología dificulta que los seres humanos llevemos a cabo la diferenciación de este tipo de contenido artificial o simulado, con respecto a los auténticos u originales (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). La evolución y la mejora de la tecnología no cesa, sin embargo, la apuesta por herramientas y mecanismos que permitan su detección o utilización por autoridades policiales y judiciales no lo hace al mismo ritmo, de este modo el nuevo panorama de la ciberdelincuencia compromete los recursos de investigación preexistentes en la normativa vigente[5].

Esta tecnología, además, se sirve de herramientas que existen en el marco de Internet desde hace décadas y de las propias características inherentes al ciberespacio; se sirven de las redes sociales, aplicaciones de mensajería y otros canales de difusión para llegar en un corto plazo de tiempo a millones de personas situadas en diferentes lugares del mundo (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). En este mismo sentido, se identificó que mejora las técnicas que los ciberdelincuentes llevan décadas empleando; por ejemplo, como ya se han señalado, las relativas a ingeniería social (Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019). Asimismo, se ha mencionado la posibilidad de combinar el *Crime as a service* y el comercio con sistemas de IA o servicios de creación de *deepfakes* directamente a través de mercados ilícitos (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). Por lo tanto, la expansión de la IA y el desarrollo de múltiples aplicaciones favorece el acceso de cualquier persona a IA generativa, permitiendo y facilitando la generación de *deepfakes,* también con fines ilícitos.

Con la combinación de este tipo de tecnología con las ventajas que ofrece la actuación en el ciberespacio, algunas de las cuales han sido señaladas, se pueden perseguir múltiples finalidades maliciosas, entre las que destacan: destruir la imagen y la credibi-

5. Como afirman desde EUROPOL: "As a result, they are always one step ahead of law enforcement in their implementation, use and adaptation of these technologies" (Europol Innovation Lab, 2022).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

lidad individual; acosar o humillar a personas en línea; perpetrar extorsión y fraude; falsificar documentos de identidad; suplantar identidades en línea; falsificar y manipular pruebas electrónicas; distribuir desinformación; incitar a la violencia, odio u otros mensajes extremistas o terroristas; interrumpir mercados financieros; incluso podríamos encontrarnos con otras consecuencias que provocasen enfrentamientos entre diferentes Estados (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020).

Teniendo en cuenta el alcance y la repercusión de estas técnicas, en el siguiente apartado analizaremos algunas particularidades de estos *deepfakes* en atención a la comisión y a la investigación de ciberdelitos de género. Los *deepfakes* también han sido utilizados y aprovechados para atentar contra los derechos de las mujeres, siendo destacable el material pornográfico generado con diversas intenciones delictivas y persiguiendo toda una variedad de objetivos, como analizaremos más en profundidad a continuación (Secretaría General de la Organización de los Estados Americanos, s.f.).

2.1. IA generativa y ciberdelincuencia de género

Desde que surgieron los primeros instrumentos y desarrollos tecnológicos los delincuentes han sido rápidos adecuando su *modus operandi* para conseguir el mayor éxito delictivo. Como ha sido señalado, lo mismo ha ocurrido con la expansión y el auge de la IA generativa.

Tenemos que considerar que en este caso la tecnología se estaría utilizando para atentar contra los derechos fundamentales de las personas, para manipular a grupos vulnerables concretos, pudiendo provocar perjuicios psíquicos e incluso físicos en las víctimas. Por lo tanto, estaríamos ante prácticas prohibidas, catalogadas como de riesgo inaceptable en la propuesta de Reglamento IA de la UE. Siendo destacable todo el elenco de modalidades delictivas que podrán perpetrarse o complementarse con la utilización de la IA generativa.

En este sentido, podemos encontrarnos diferentes delitos que podrían cometerse, como los ciberdelitos de género. En primer lugar, definiremos la ciberdelincuencia de género como aquellos delitos cometidos a través de Internet por razón de género prevaliéndose el agresor del alcance y la especial lesividad de los medios tecnológicos, tanto en el ámbito público como en el ámbito privado, con independencia de la relación preexistente con la víctima (González Pulido, 2017). Por ejemplo, encontraríamos la generación de material de abuso sexual infantil o la generación y distribución de material sexual explícito de adultos, falso y sin consentimiento. Por lo tanto, algunas de las conductas que tendrían cabida en la citada definición están consideradas como graves y así se han contemplado en el marco de los instrumentos aprobados a nivel de la UE e incluso a nivel internacional.

En este momento, en atención a las apreciaciones realizadas, es oportuno comenzar a señalar que en la propuesta de Reglamento de IA de la UE, se supedita la utilización de algunos de los sistemas de IA previstos en su articulado a la gravedad y a la autorización

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

judicial[6], por lo que parecería que cuando nos encontremos ante determinadas conductas de ciberdelincuencia de género el Reglamento si favorecería la implementación de sistemas de IA policiales y judiciales para luchar contra estos fenómenos.

Como características más relevantes de la IA generativa para utilizarla para la comisión de este tipo de ciberdelitos de género destacan: la utilidad de modelos de lenguaje generativo para suplantar la identidad y la capacidad de estos modelos para favorecer que los ciberdelincuentes se ganen la confianza de las víctimas (Europol, 27 de marzo de 2023); la utilización de *deepfakes* basados en imágenes, vídeos o audio; también la posible combinación de diferentes técnicas de IA generativa buscando la mayor efectividad; entre otros. Sin perjuicio de que también pueda combinarse la utilización de otro tipo de sistemas de IA para obtener material o incluso para su difusión, en función de la conducta a realizar y el objetivo perseguido por el delincuente, ya se abordaron previamente algunas posibles ventajas de los *software* que se sirven de estas tecnologías.

En particular, es destacable en el marco de este estudio cómo preocupan a la comunidad internacional los sistemas de IA que han sido catalogados como multimodales, ya que son sistemas de IA capaces de integrar y procesar "múltiples modalidades de información o fuentes de datos de diversos tipos […]: texto, audio, imagen/vídeo, profundidad, térmica y movimiento" (Loredo, 2023). Estos sistemas de IA generativa pueden fomentar la creación de *deepfakes* muy convincentes y que pueden servir para la comisión de múltiples tipologías delictivas (Europol, 27 de marzo de 2023).

Estas funciones podrían mejorar y favorecer las prácticas de algunos ciberdelitos e incluso utilizar la posible generación de vídeo y audio para engañar o embaucar a menores o mujeres con el fin último de captar víctimas de otros eventuales delitos o bien directamente con el objetivo de perpetrar un delito sexual en el medio físico *offline*. No se trata de la aparición de nuevos delitos, sino de herramientas que agilizan y promueven su práctica, ya que la principal ventaja de la IA generativa es que facilita y mejora la calidad del material audiovisual.

Ejemplo de esta cuestión la encontramos en el análisis de la realidad actual, ya que pone de manifiesto que no nos encontramos ante ideas hipotéticas de futuro, sino que este tipo de criminales ya se están aprovechando de las ventajas de la IA generativa para poder perpetrar sus delitos, en particular, para la comisión de este tipo de ciberdelitos que atentan contra las mujeres, por el mero hecho de serlo, con una mayor incidencia. En particular, los *deepfakes* ya fueron identificados hace años como un riesgo para los derechos de las mujeres y como una manifestación más de la cosificación de las mismas (Cerdán Martínez, Padilla Castillo, 2019).

6. Véase, por ejemplo, el considerando 18 tras la enmienda aprobada el 14 de junio de 2023, que señala estos requisitos para la utilización excepcional de sistemas IA para la identificación biométrica en imágenes grabadas en espacios de acceso público. Indicando que deberá ser estrictamente necesario para investigar un delito grave, que ya se haya cometido, y solo previa autorización judicial. Cuestión regulada en el artículo 5, apartado 1, letra d quinquies.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

A finales del año 2017 ya encontrábamos el caso del usuario anónimo de Reddit que publicó vídeos de diferentes actrices famosas, en los que había superpuesto a cuerpos de otras mujeres sus caras para crear películas pornográficas, así como es destacable la consiguiente creación de *FakeApp* u otras aplicaciones (Cerdán Martínez, Padilla Castillo, 2019; Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019). Nos encontramos en este caso ante la utilización de IA generativa con fines de generación de material pornográfico no consentido. Es preciso apuntar que el desarrollo que han experimentado estas técnicas desde 2017 ha sido muy significativo, no obstante, es relevante recoger este mediático caso que pone de manifiesto el empleo de esta tecnología.

Además, el desarrollo de este tipo de aplicaciones generó la creación de algunas específicas como *Deepnude,* focalizada concretamente en desnudar a mujeres (Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019). Como señala el estudio de *Deeptrace Labs* sus creadores eliminaron el sitio web oficial pero el código quedó en Internet, e incluso se crearon nuevas versiones mejoradas que cobraban por su utilización.

Es preciso incidir en el mencionado informe elaborado por *Deeptrace Labs,* uno de los informes referentes en el marco de los *deepfakes,* publicado en el año 2019, en este se registró que la mayoría de los vídeos *deepfake* eran vídeos pornográficos, un 96%, frente al 4% que no lo eran. Además, destacaron que en este tipo de vídeos las protagonistas eran mujeres, frente a los vídeos que no tenían contenido pornográfico donde los protagonistas eran hombres (Aider, Patrini, Cavalli, Cullen (Deeptrace Labs), 2019).

Junto con las dificultades inherentes a la detección de los delitos que se sirven de la IA para su comisión, se ha destacado como la elaboración anónima que ofrecen las herramientas de IA generativa puede obstaculizar la actuación de las autoridades competentes (Europol Innovation Lab, 2022). Uno de los principales objetivos tras la detección de un hecho delictivo es la identificación de los responsables, cuestión que favorecerá también la represión del delito y la reparación del daño. En Internet, desde su aparición, esta cuestión se configura como una dificultad significativa y, además, parece agravarse con el uso de la IA.

En definitiva, cada vez son más numerosos los informes, los documentos o las noticias que de forma directa o indirecta identifican que nos encontramos ante una amenaza que favorece la ciberdelincuencia de género.

Además, se ha detectado que los sistemas de IA generativa se están implementando para cometer delitos contra víctimas menores de edad, siendo destacables el embaucamiento de menores o la creación de materiales relacionados con el abuso sexual infantil en línea. En estos casos podemos encontrar una amplia variedad de ejemplos en los que la IA generativa se ha utilizado para la comisión de estos hechos delictivos. En primer lugar, la simulación de una identidad falsa, bien de otra persona o bien de un menor de edad, ha sido empleada para favorecer el acercamiento y para ganarse la confianza de las víctimas menores, incluso para la obtención de material de contenido sexual explícito autogenerado por estos menores. De igual modo, ya se ha detectado y detenido a un sujeto en España que utilizaba un sistema de IA generativa en el que añadía una descripción de texto y se generaban imágenes en atención a las preferencias y descripciones que realizaba en el citado texto. Por lo tanto, empleaba este tipo de IA para la

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

producción de materiales relacionados con el abuso sexual infantil en línea, material pornográfico de menores; generaba archivos de "extrema dureza" en los que se "representaban imágenes reales de niñas de muy corta edad siendo violadas y utilizando órganos y juguetes sexuales desproporcionados" ("La Policía Nacional detiene a un pedófilo que utilizaba inteligencia artificial para crear material de abuso sexual infantil de extrema dureza", 21 de diciembre de 2022).

De igual modo, podríamos encontrarnos incluso con ciberdelincuencia de género en el marco de la delincuencia organizada, se ha identificado que los *deepfakes* pueden favorecer el fraude documental, lo que puede facilitar la práctica de otros delitos como la trata de seres humanos, el tráfico de personas e incluso algunas actividades relativas al terrorismo (Europol Innovation Lab, 2022), contribuyendo no solo a la captación sino también al transporte de mujeres y menores con diferentes fines.

En este sentido, la realidad actual pone de manifiesto la preocupación de la comunidad internacional por regular este fenómeno, tipificar estas conductas y favorecer la represión de las mismas. Podemos reseñar brevemente como se han incluido preceptos en recientes propuestas o se han registrado enmiendas en este sentido, sin perjuicio de las que ya han sido señaladas en la Propuesta de Reglamento de IA de la UE y que serán analizadas con más profundidad en los epígrafes posteriores.

En primer lugar, en la Propuesta de Directiva sobre la lucha contra la violencia contra las mujeres y la violencia doméstica se ha recogido, en el considerando 19 y en el artículo 7, la necesidad de tipificar la producción, manipulación o difusión no consentida de material íntimo o manipulado. Se ha incluido expresamente la alusión a la edición o fabricación de *deepfakes*[7].

En este mismo sentido, se han recogido enmiendas a la propuesta de Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual de los menores que identifican la necesidad de considerar que existe una mayor probabilidad de que las niñas sean víctimas, afectando "la desigualdad de género, la violencia estructural y la discriminación contra las mujeres" en algunas tipologías delictivas, como en el abuso sexual infantil en línea (Comisión de Derechos de las Mujeres e Igualdad de género a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores, 8 de mayo de 2023). Desde la aprobación hace décadas de otros instrumentos se ha considerado delictiva la representación visual o la existencia de imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita (Ratificación del Convenio sobre la Ciberdelincuencia, 17 de septiembre de 2010) o

7. Se hace referencia en el considerando 19 a "la fabricación de ultrafalsificaciones (deepfakes), en las que el material se parezca sensiblemente a una persona, a objetos, lugares u otras entidades o acontecimientos existentes, representando actividades sexuales de otra persona, y pueda dar a otros la impresión falsa de que es auténtico o veraz".

Además, se persigue la protección de la amenaza: "En aras de una protección eficaz de las víctimas de estas conductas, también debe regularse la amenaza de llevarlas a cabo".

(Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica. Estrasburgo, 8 de marzo de 2022)

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

imágenes realistas de los órganos sexuales de un menor con fines principalmente sexuales (Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, 17 de diciembre de 2011, artículo 2), casuística entre la que tendría cabida la creación de material a través de sistemas de IA generativa[8]. Sin perjuicio de que si se utilizan imágenes reales de menores o se manipula material audiovisual con esta tecnología también será considerada delictiva incluso su producción, oferta, difusión, adquisición o posesión, entre otras.

En definitiva, podemos afirmar que la IA generativa está siendo utilizada para perpetuar y facilitar la práctica de todo un elenco de ciberdelitos de género. Debido a ello, se están sumando algunas dificultades adicionales a las investigaciones tradiciones, las cuales debemos considerar como cuestiones urgentes a atender, ya que nos podemos encontrar ante fenómenos delictivos globales y graves. En los siguientes apartados analizaremos cuáles son las perspectivas de futuro existentes en el marco de la UE y qué desafíos no se han contemplado pero que son necesarios para poder aprovechar las ventajas tecnológicas de la IA con el objetivo de minimizar la impunidad y la cifra negra de estos ciberdelitos.

III. IA generativa como recurso para la investigación de autoridades policiales y judiciales

En algunos de los anteriores instrumentos señalados ya se recogieron medidas de investigación tecnológicas para hacer frente a diferentes ciberdelitos, por ejemplo, en el marco del Convenio sobre la ciberdelincuencia se incluyeron algunos tipos de interceptación, registro, conservación u obtención de diferentes tipos de datos (Ratificación del Convenio sobre la Ciberdelincuencia, 17 de septiembre de 2010). En este mismo sentido, a nivel europeo, se ha apostado por las órdenes europeas de investigación para la obtención de prueba transfronteriza, incorporando expresamente la intervención de las telecomunicaciones (Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, 1 de mayo de 2014), aunque quedándose escuetos en lo que respecta a la previsión exhaustiva de las diligencias tecnológicas más novedosas y óptimas para los ciberdelitos actuales. Por otro lado, en atención a otros instrumentos específicos, como los señalados en materia de abuso sexual infantil en línea o la reciente propuesta de Directiva relativa a violencia sobre la mujer, no han centrado su atención en lo que respecta a las diligencias de investigación tecnológicas, sin perjuicio de que instasen a los Estados a adoptar las medidas necesarias para su esclarecimiento y enjuiciamiento (Propuesta

8. Se hizo referencia a la denominada "pornografía virtual", como "creación artificial pero realista" (Circular 2/2015, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015, 19 de junio de 2015)

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica. Estrasburgo, 8 de marzo de 2022; Propuesta de Reglamento para prevenir y combatir el abuso sexual de los menores, 8 de mayo de 2023; Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, 17 de diciembre de 2011).

En atención a las propuestas existentes, podemos afirmar que la actuación de la Unión Europea está encaminada a establecer una regulación en materia de IA e incluso a contemplar las actividades delictivas en las que pueda mediar su utilización. No obstante, todavía no está suficientemente desarrollada la posibilidad de implementar los diferentes tipos de sistemas de IA para la investigación policial y judicial.

Desde la Unión Europea, entre las razones y los objetivos de la propuesta de Reglamento de IA se ha hecho mención a su intención de conseguir un equilibrio entre la apuesta por la tecnología y la salvaguarda de los valores, derechos fundamentales y principios de la UE (Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, 21 de abril de 2021). En el contexto de la investigación policial y judicial no se prohíbe su utilización, sino que se prevé su regulación en atención a la necesaria salvaguarda de todos los derechos y garantías inherentes al proceso. En este sentido continuaremos el presente análisis, centrándonos en la implementación de la IA en el marco de la actuación policial y judicial para hacer frente a la ciberdelincuencia de género.

Se abordará esta cuestión sin perjuicio de que también se haya identificado la necesidad de preparar a las autoridades competentes para conocer el alcance de la utilización de la IA tanto con fines maliciosos como con otra intención no delictiva; como hace referencia Europol en el marco de análisis de la técnica de los *deepfakes* (Europol Innovation Lab, 2022). Como ha ocurrido con otros desarrollos tecnológicos la capacitación y formación también es necesaria para poder actuar contra los fenómenos delictivos emergentes.

En el marco del proceso penal se han planteado múltiples posibilidades de aplicación de la IA[9]. En los últimos años, muchas han sido las apuestas por la utilización de la IA para la investigación policial y judicial, habiendo destacado en el campo de la predicción, prevención y actuación policial (Dolz Lago, 2022; González-Álvarez, Santos-Hermoso, Camacho-Collados, 2020; Martín Diz, 2020a; Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)), 24 de marzo de 2022). En particular, también se ha apostado por su utilización en el

9. MARTÍN DIZ (2020a) señala que existen múltiples posibilidades como su implementación para "la obtención de datos para la investigación criminal, la valoración o el razonamiento de los resultados de la prueba o el cotejo de la adecuación del perito y su dictamen en la prueba pericial junto a las posibilidades predictivas".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

marco de la investigación criminal a través de la identificación biométrica, la realidad aumentada e incluso se han implementado sistemas de IA para la investigación de la ciberdelincuencia y detección de amenazas (Cuatrecasas Monforte, 2022; Martín Ríos, 2022; Richard González, 2023). Asimismo, con carácter todavía más específico, ya se ha apostado por la utilización de la IA para mejorar la investigación policial en casos de violencia de género (Magro Servet, 2021).

Con carácter general, con la propuesta de Reglamento de IA en la UE se persigue el establecimiento de una base sólida que nos permita armonizar la normativa relativa al desarrollo, funcionamiento y utilización de los sistemas de IA. Además, establece diferentes categorías en base al riesgo, proponiendo unas líneas de actuaciones proporcionadas en atención al mismo.

En el considerando 38 de la propuesta de Reglamento de IA, incluso en las enmiendas, se reconoce que "procede considerar de alto riesgo a múltiples sistemas de IA diseñados para usarse con fines de aplicación de la ley", en atención concretamente a la "precisión, fiabilidad y transparencia" que se deben garantizar. Asimismo, enumeran algunos de los sistemas que se incluiría: "polígrafos y herramientas similares, en la medida en que su uso esté permitido conforme a la legislación de la Unión y nacional pertinente, para evaluar la fiabilidad de las pruebas en un proceso penal; para elaborar perfiles durante la detección, la investigación o el enjuiciamiento de infracciones penales, y para realizar análisis penales en relación con personas físicas" (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

De igual modo, entre los sistemas de IA de alto riesgo contemplados en el anexo III de la propuesta inicial se incluyeron otros que podrían utilizarse en el marco de la investigación que se ha encomendado por ley a las autoridades policiales y judiciales. En este sentido, destacaron los sistemas biométricos y basados en la biometría; sistemas IA de apoyo a las autoridades encargadas de aplicar la ley para examinar grandes cantidades de datos, disponibles en distintas fuentes o formatos, para detectar modelos desconocidos o descubrir relaciones ocultas; sistemas IA empleados por autoridades públicas para verificar autenticidad de documentos y detectar documentos falsos; sistemas IA para detectar ultrafalsificaciones; y, entre otros, en el punto ocho es destacable la mención a "sistemas de IA destinados a ser utilizados por una autoridad judicial […], o en su nombre, para ayudar a una autoridad judicial o un órgano administrativo en la investigación e interpretación de hechos y de la ley, así como en la aplicación de la ley a un conjunto concreto de hechos" (Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, 21 de abril de 2021). Aunque algunas citaciones concretas a estos sistemas IA al servicio de las autoridades encargadas de hacer cumplir la ley se suprimen, agrupan o modifican por parte del Parlamento europeo en las últimas enmiendas (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

Es importante la aclaración que se realiza en atención a que "los sistemas de IA de alto riesgo no están prohibidos ni deben considerarse indeseables", sino que apuntan

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

que "por el contrario, el cumplimiento de los requisitos de conformidad establecidos en el Reglamento hace que dichos sistemas sean más fiables y tengan más probabilidades de tener éxito en el mercado europeo" (Parlamento Europeo, 22 de mayo de 2023). En definitiva, no se está excluyendo a que autoridades competentes a nivel nacional puedan hacer uso de estos para la práctica de las investigaciones.

Destacan los sistemas de IA generativa, que se han incorporado en la propuesta de IA de la UE bajo la denominación de "robots conversacionales" o "ultrafalsificaciones", definiéndolos como "un contenido de sonido, imagen o vídeo manipulado o sintético que puede inducir erróneamente a pensar que es auténtico o verídico, y que muestra representaciones de personas que parecen decir o hacer cosas que no han dicho ni hecho, producido utilizando técnicas de IA, incluido el aprendizaje automático y el aprendizaje profundo", por lo tanto, incluyendo cualquier sistema de IA que genere o manipule de texto, sonidos o vídeos (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, artículo 3, apartado 44 quinquies). Para estos sistemas se han establecido unas obligaciones en materia de transparencia, enfocadas principalmente a la identificación de los mismos. Cuando los fines sean delictivos está claro que se omitirán estas obligaciones por parte de los ciberdelincuentes.

Por supuesto, ya se ha previsto que cuando sean las autoridades policiales y/o judiciales en el marco de sus funciones de detección, prevención, investigación o enjuiciamiento de infracciones penales, podrán omitir la obligación de que las personas que interactúan con determinados sistemas IA o material generado con esta tecnología conozcan realmente que se encuentran ante el producto o sistemas de IA generativa (Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, 21 de abril de 2021). Desde la aparición de la propuesta ya se detectó que, por ejemplo, podría estar pensado para la utilización de "materiales camuflados o creados artificialmente por agentes encubiertos informáticos" (Bueno de Mata, 2021).

Aunque esta aclaración parece haberse modificado con la aprobación de las últimas enmiendas, ya que se permite directamente obviar esta obligación cuando esté el sistema IA previsto y autorizado en la legislación vigente (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023), por lo tanto, sería idóneo contar con una legislación que habilitara expresamente a la utilización de esta tecnología, ya que se evitarían problemas derivados de la falta de exhaustividad y seguridad jurídica.

De igual modo, se ha señalado que no se impide que las autoridades competentes utilicen sistemas IA para detectar dichas falsificaciones y para prevenir, investigar y enjuiciar las infracciones penales relacionadas con su uso. Por lo tanto, parece que sí se está instando a la necesidad de perseguir los delitos que se sirven de la IA generativa, pero no se prevé expresamente que esta tecnología se incluya en el marco de las diligencias de investigación tecnológicas.

Por parte de Europol, también se han realizado apuestas específicas que instan al estudio de los nuevos modelos de IA, como pueden ser los modelos de lenguaje

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

generativo, en aras a implementarlos de un modo específico en el marco de sus actuaciones, entrenando a estos sistemas de IA generativa privados con sus propios datos y salvaguardando la integridad y confidencialidad de los datos utilizados para su entrenamiento (Europol, 27 de marzo de 2023).

Cuando se introduce la IA en la Administración de Justicia se requieren datos de calidad y una incorporación de los mismos con precisión, con el objetivo de implementar "buenas tecnologías" (Magro Servet, 2018). Por su parte, en el caso de que los sistemas de IA que se utilizarán para realizar investigaciones criminales se apuesta por un control de calidad mucho mayor, en atención a todos los derechos fundamentales pueden verse comprometidos (Cuatrecasas Monforte, 2022).

Es importante atender a la utilización de sistemas IA también para investigar otros sistemas y técnicas delictivas basadas en IA que simulan comportamientos humanos o de otra índole (Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI) and Europol's European Cybercrime Centre (EC3), 2020). La probabilidad de detección podrá ser mayor si se recurre a esta misma tecnología, debido a ello es importante plantearse la IA como herramienta también de investigación. Urge esta consideración en atención al desarrollo exponencial de la tecnología y al alto grado de adaptación que están demostrando los delincuentes y organizaciones.

Asimismo, en la propuesta de Reglamento de IA de la UE original estos sistemas de IA empleados para detectar las ultrafalsificaciones por parte de las autoridades encargadas de la aplicación de la ley, es decir, por parte de las autoridades policiales y judiciales, se incluían en el anexo III de un modo expreso como sistemas IA de alto riesgo. Sin embargo, en las enmiendas del Parlamento, los sistemas IA empleados por autoridades policiales en el marco de una investigación podrían tener cabida en el apartado 8, letra a), relativo a "la utilización de esta tecnología para la investigación o interpretación de hechos y de la ley". Sin perjuicio de la mención expresa en la modificación propuesta por el Parlamento del artículo 52, apartado 3 bis, que ha sido previamente señalada[10]. Quizá se persigue evitar la obsolescencia los sistemas de alto riesgo, pero sí se realiza en otros ámbitos una enumeración más detallada y exhaustiva que otorgaría una mayor seguridad y garantía a las autoridades competentes en materia de investigación de la ciberdelincuencia. No obstante, es destacable en este sentido que desde la propuesta inicial se ha previsto la modificación y actualización del anexo III, relativo a los sistemas IA de alto riesgo, cuando se detecte que en atención al riesgo, a la gravedad y a la probabilidad de ocurrencia sea relevante y proporcionada su incorporación, en ponderación con los perjuicios que se podrían derivar de la aplicación de dichos sistemas IA (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, artículo 7, apartado 1). En el caso de implementar sistemas de IA generativa en el marco de la investigación policial y judicial o bien sistemas para investigar los delitos

10. Se señala que "Asimismo, no impedirá que las autoridades encargadas de la aplicación de la ley utilicen sistemas de IA destinados a detectar ultrafalsificaciones y a prevenir, investigar y enjuiciar las infracciones penales relacionadas con su uso". (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

cometidos con IA generativa, en atención a la injerencia sobre los derechos fundamentales podría haberse condicionado su previsión específica en el anexo III. Sin perjuicio de que tenga cabida, como se ha señalado, en otros preceptos. Parece que la tendencia, tras las enmiendas del Parlamento, insta a una regulación genérica que necesitará una previsión legal exhaustiva a nivel nacional y en el marco de instrumentos de investigación transfronteriza.

En definitiva, la utilización de la IA generativa en el marco de la investigación de ciberdelitos de género corresponde a la implementación de sistemas IA de alto riesgo, por lo que deberá acogerse a los requisitos previstos en los artículos 8 y siguientes para este tipo de sistemas. Para ello, deberá implantar y mantener un sistema de gestión de riesgos; emplearán prácticas idóneas respecto a la gobernanza y gestión de datos; elaboración y mantenimiento de la documentación técnica y los registros actualizados; garantizarán un nivel elevado de transparencia, sin perjuicio de las citadas excepciones que se prevén para la práctica de investigaciones policiales y judiciales; se diseñarán en atención al requerimiento de que se pueda realizar una efectiva vigilancia humana de su actividad, previendo la minimización de las consecuencias negativas derivadas de la utilización de un sistema de IA generativa que puede suponer una injerencia sobre derechos fundamentales de las personas investigadas. Asimismo, estos sistemas deben contar con un nivel adecuado de precisión, solidez, seguridad y ciberseguridad, evitando y corrigiendo, asimismo, posibles sesgos (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, capítulo 2; Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión, 21 de abril de 2021, capítulo 2).

Es relevante el cumplimiento de todas estas cuestiones ya que en el marco de un proceso penal incoado por motivo de un ciberdelito, será importante también salvaguardar los derechos de las personas investigadas. En este sentido, en las enmiendas aprobadas con respecto a la propuesta de Reglamento de IA, se ha incluido que las autoridades competentes deben tener en consideración "el impacto del uso de herramientas de IA en los derechos de defensa de los sospechosos, en especial la dificultad para obtener información significativa sobre su funcionamiento y la consiguiente dificultad para impugnar sus resultados ante los tribunales" (Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo, 14 de junio de 2023, considerando 38, enmienda 69). Con carácter general, son muchos los derechos fundamentales y principios inherentes al proceso penal que se podrían ver comprometidos sino se incorpora este tipo de tecnología salvaguardando todos los requisitos relativos al funcionamiento de la IA y todas las garantías procesales (Martín Diz, 2020b).

Todas estas cuestiones deben considerarse sin perjuicio de que como también se ha señalado se pueda utilizar otro tipo de sistemas IA que favorezcan la verificación de material audiovisual o probatorio, como por ejemplo, se hace referencia por Europol a la necesidad futura de mejorar la detección de *deepfakes* comprobando una serie de marcadores de autenticidad (Europol Innovation Lab, 2022). No nos encontramos ante una novedad para las autoridades policiales y judiciales, ya que la elaboración de documentación o

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

material probatorio falso ya existía con carácter previo al desarrollo de la IA, no obstante, se requiere apostar por nuevas herramientas para hacer frente a técnicas que mejoran su práctica ilícita y que dificultan su detección. Por lo tanto, parece clave la utilización de la tecnología para también detectar lo que la tecnología ha creado.

Urge aprobar una regulación exhaustiva e internacional que contemple el funcionamiento y la utilización de todos los tipos de sistemas de IA, en particular de los sistemas de IA generativa en atención a las ventajas que ofrecen, ya que, como hemos señalado anteriormente, la falta de regulación de estas tecnologías va a suponer un mayor obstáculo para que fuerzas y cuerpos de seguridad puedan cumplir sus funciones y practicar investigaciones eficaces (Europol Innovation Lab, 2022).

IV. Líneas de actuación futuras para implementar la IA generativa: recomendaciones para actuar a corto, medio y largo plazo

Para finalizar el presente estudio se destacarán algunas líneas de actuación futuras que deben seguirse para poder implementar la IA generativa en el marco de actuación de las autoridades policiales y judiciales, pero también para que estas autoridades competentes en materia de investigación puedan atajar las amenazas que se están transformando debido a la implementación de este tipo de sistemas IA en los *modus operandi* de los diferentes delitos.

En primer lugar, ya se apunta desde Europol, que urge la necesidad de visibilizar el alcance de estos sistemas de IA generativa. Como ya se ha señalado, es necesaria la capacitación de las autoridades señaladas y la comprensión por estas de los nuevos fenómenos delictivos. Nos encontramos ante una realidad presente, que se ha magnificado en los últimos meses y solo de este modo se podrá avanzar hacia la consecución de una prevención, detección, investigación y enjuiciamiento eficaces (Europol, 27 de marzo de 2023). Es clave la capacitación y financiación para apostar por nuevas tecnologías que permitan atajar nuevas amenazas clave que perpetúan la desigualdad de género, como es este tipo de ciberdelincuencia.

Como también se ha apuntado a lo largo del presente estudio, el potencial que desarrollarán este tipo de sistemas de IA generativa en los próximos años favorecerá la actuación de los delincuentes, mejorando el éxito delictivo, principalmente protegiendo su identidad y obstaculizando las investigaciones delictivas, las cuales encontrarán mayores dificultades. La tecnología no cesa, la evolución y mejora de la IA y, en particular, de la IA generativa compromete la protección de los derechos de los internautas y las autoridades competentes deben contar con herramientas técnicas y legales que les permitan practicar actuaciones de alto nivel técnico, que sean eficaces y garantes.

A corto plazo, la implementación de los sistemas de IA generativa podría optimizar la utilización de algunas diligencias de investigación ya preexistentes; por ejemplo, la práctica del agente encubierto informático. En este sentido, sistemas multimodales podrían optimizar la actuación de las autoridades policiales y judiciales, favoreciendo la

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

protección de víctimas y de los propios agentes involucrados, por ejemplo, a través de perfiles e identidades falsas[11]. Por lo tanto, la tecnología se presenta ofreciendo unos recursos que permiten continuar con la adopción de técnicas de investigación que habían sido consideradas idóneas, por ejemplo, para la lucha contra la creación y distribución de material relativo a abuso infantil en línea.

En este concreto ejemplo, por un lado, nos encontramos con que se ha detectado la idoneidad de la utilización del agente encubierto informático y los diferentes tipos de registros, remoto y de dispositivos de almacenamiento masivo (Rodríguez Tirado, 2018), para la persecución de los delitos relativos a explotación sexual infantil en línea y a la distribución de material de abuso de menores y, asimismo, se ha identificado la necesidad de intercambiar material ilícito para obtener la confianza necesaria (Carou García, 2018) y poder acceder a los grupos u organizaciones, así como para concretar la autoría de este tipo de hechos delictivos. En este sentido también se han previsto epígrafes específicos en nuestra legislación vigente[12]. Encontramos en estos casos varios momentos en los que podríamos recurrir a la IA generativa; a sistemas que generen imagen, audio y vídeo para simular la identidad del agente; a sistemas de lenguaje para favorecer la interacción entre agente y presunto autor; e incluso a sistemas de IA generativa que generen el material que se requiere para intercambiar (Bueno de Mata, 2021).

Se ha detectado que la regulación preexistente en materia de diligencias de investigación tecnológicas podría servir como base para implementar este tipo de tecnología como herramienta en la investigación criminal, ya que se ha previsto la salvaguarda de los principios de especialidad, idoneidad, necesidad, excepcionalidad y proporcionalidad para autorizar su adopción con todas las garantías (Cuatrecasas Monforte, 2022). De igual modo, sería la opción más viable a corto plazo también para los sistemas de IA generativa.

En este mismo sentido podríamos enumerar otros ejemplos relativos a la utilización de esta herramienta para la investigación de los ciberdelitos de género que se cometan, por ejemplo, en el marco de organizaciones criminales. O bien se podría requerir la utilización de sistemas de IA generativa para el desarrollo de *software* policiales o judiciales que favorezcan la práctica de ciberrastreos u otras diligencias tradicionales; como puede ser el desarrollo de programas de detección de material de abuso sexual infantil en línea o bien *spyware* específicos para cursar registros remotos.

En atención a la complejidad y a las circunstancias del caso, se puede requerir que la investigación inicial que se está efectuando con un sistema de IA generativa se complemente con otras diligencias, que a su vez se pueden agilizar y mejorar utilizando otro tipo de sistemas IA. Por ejemplo, en el marco de actuación de un agente encubierto se puede necesitar la práctica de un registro remoto o un registro de dispositivos de

11. MARTÍN RÍOS (2022) ya señalaba: "En el marco de la represión policial de la pederastia, también se utiliza IA para construir perfiles falsos".

12. Véase artículo 282 bis 6 de la Ley de Enjuiciamiento Criminal española: "El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos".

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

almacenamiento masivo. En el citado ejemplo, el agente se podría beneficiar de la utilización de *malware* programado con tecnología IA para indagaciones remotas o bien de la capacidad de un *software* para tratar grandes cantidades de datos tras un registro físico u *online*.

La ausencia de fronteras y la inmediatez que ofrece Internet son dos características clave de las que se sirven los creadores y los que utilizan estas nuevas técnicas de IA, incluidos los delincuentes que perpetran ciberdelitos de género, los cuales ya identificaron estas particularidades como ventajas hace décadas. En este sentido, es preciso que se prevea con mayor exhaustividad la posibilidad de aplicar sistemas IA para realizar investigaciones transfronterizas. En el marco de análisis que nos ocupa, tenemos que destacar que la problemática de los *deepfakes* está consolidada en la actualidad a nivel global, expandiéndose de forma exponencial. En este mismo sentido, la práctica de investigaciones en Internet con frecuencia requiere el recurso a medios de investigación tecnológica que permitan la obtención de prueba transfronteriza. Sin perjuicio de que a corto plazo, como apuntamos a nivel nacional, se pueda utilizar la IA y la IA generativa para favorecer la práctica de estas diligencias ya preexistentes, sería oportuno que a largo plazo se concreten todos los requisitos, principios y extremos necesarios para poder implementar IA por parte de las autoridades policiales y judiciales. Incluso se puede aprovechar esta apuesta por la regulación de la IA como herramienta de investigación para crear nuevas diligencias, otorgando suficiente seguridad jurídica a estas prácticas que cada vez deberán ser más frecuentes y que tendrán que ser eficaces y salvaguardar los derechos fundamentales de las personas investigadas.

Por otro lado, también sería recomendable a medio plazo, debido a la complejidad que ello requiere, actualizar los instrumentos referentes en materia de tipificación y lucha contra la ciberdelincuencia; por ejemplo, el Convenio sobre la ciberdelincuencia. Y también apostar, a nivel regional, en la UE por concretar las propuestas en materia de regulación de los sistemas de IA de forma urgente, así como otras que de un modo más específico persiguen minimizar amenazas consolidadas que se están agravando debido al desarrollo tecnológico. Para ello, se requiere prestar atención a diferentes enmiendas que persiguen una lucha contra la ciberdelincuencia efectiva, sin dispersar las herramientas existentes o reiterar el desarrollo de las mismas, optimizando los recursos y agilizando la cooperación para este tipo de casos de investigación tecnológica.

La ciberdelincuencia, incluyendo en ella los delitos cometidos por razón de género que se dirigen con mayor frecuencia contra mujeres y niñas, se está convirtiendo en una herramienta clave para complementar otros delitos en el medio *offline* e incluso para la delincuencia organizada internacional. Ante esta realidad, podríamos encontrarnos ante el momento idóneo para apostar por la regulación de unas técnicas y medidas de investigación específicas para la ciberdelincuencia, que consideren todas las particularidades y obstáculos que se presentan en Internet y que se agravan con el desarrollo de los sistemas de IA. De este modo se unificarían los recursos disponibles y se podrían concretar los extremos necesarios para implementar los sistemas de IA en la investigación policial y judicial; en particular, debiéndose incluir los requisitos necesarios para cumplir con los principios y garantías procesales en este medio *online*.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

Bibliografía

AIDER, H., PATRINI, G., CAVALLI, F., CULLEN, L. (DEEPTRACE LABS). (2019). *The State of Deepfakes: Landscape, Threats, and Impact*.

BUENO DE MATA, F. (2021). "Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid". *La Ley Penal,* nº 150.

CAROU GARCÍA, S. (2018). "El agente encubierto como instrumento de lucha contra la pornografía infantil en Internet". *Cuadernos de la Guardia Civil,* nº 56, pp. 23-40. ISSN: 2341-3263.

CERDÁN MARTÍNEZ, V., PADILLA CASTILLO, G. (2019). "Historia del *fake* audiovisual: *deepfake* y la mujer en un imaginario falsificado y perverso". *Historia y comunicación social,* 24 (2), pp. 505-520. ISSN–e 1988-3056.

Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015. FIS-C-2015-00002.

Comisión de Derechos de las Mujeres e Igualdad de género a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores. Enmiendas 46-536. 8 de mayo de 2023. 2022/0155(COD).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Fomentar un planteamiento europeo en materia de inteligencia artificial. COM/2021/205 final. Bruselas, 21 de abril de 2021.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025. COM (2021) 170 final. Bruselas, 14 de abril de 2021.

CUATRECASAS MONFORTE, C. (2022). "La inteligencia artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional". *La Ley*.

DEL CASTILLO, C. (18 de septiembre de 2023). "Un negocio con lista de espera: la app usada para 'desnudar' a menores en Badajoz cobra 9 euros por 25 fotos". ElDiario.es.

Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo. «DOUE» núm. 335, de 17 de diciembre de 2011, pp. 1 - 14.

Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal. OJ L 130, 1 de mayo de 2014, pp. 1–36.

DOLZ LAGO, J.M. (2022). "Una aproximación jurídica a la Inteligencia Artificial". *Diario La Ley,* nº 10096.

EUROPOL. (27 de marzo de 2023). ChatGPT. The impact of Large Language Models on Law Enforcement. Luxembourg: Publications Office of the European Union.

EUROPOL (EUROPOL INNOVATION LAB). (2022). Facing reality? Law enforcement and the challenge of deepfakes. Luxembourg: European Union Agency for Law Enforcement Cooperation. ISBN 978-92-95220-40-9.

EUROPOL. (2020). Internet organised crime threat assessment (IOCTA). Consultado en: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (Fecha de consulta: 01/10/2023).

GONZÁLEZ-ÁLVAREZ, J. L., SANTOS-HERMOSO, J. & CAMACHO-COLLADOS. (2020). "Policía predictiva en España. Aplicación y retos de futuro". *Behavior & Law Journal*, 6(1), pp. 26-41.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

GONZÁLEZ PULIDO, I. (2017). "Avances y desafíos en materia de ciberdelincuencia de género a nivel europeo". *FODERTICS 6.0. Los nuevos retos del derecho ante la era digital*. Granada: Editorial Comares, pp. 149-160.

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. «BOE» núm. 226, de 17 de septiembre de 2010, pp. 78847-78896.

LOREDO, A. (14 de junio de 2023). "IA multimodales, metaverse y más". Consultado en: https://www.linkedin.com/pulse/ia-multimodal-metaverse-y-m%C3%A1s-all%C3%A1-alejandro-loredo/?trk=pulse-article&originalSubdomain=es (Fecha de consulta: 01/10/2023).

MAGRO SERVET, V. (2018). "La aplicación de la inteligencia artificial en la Administración de Justicia". *Diario La Ley,* nº 9268, sección doctrina.

MAGRO SERVET, V. (2021). "La inteligencia artificial para mejorar la lucha contra la violencia de género". *Diario La Ley,* nº 9898.

MARTÍN DIZ, F. (2020a). "Aplicaciones de inteligencia artificial en procesos penales por delitos relacionados con la corrupción". *Corrupción: Compliance, represión y recuperación de activos*. Valencia: Tirant lo Blanch, pp. 533-568.

MARTÍN DIZ, F. (2020b). "Capítulo XLV. Inteligencia artificial y proceso: garantías frente a eficiencia en el entorno de los derechos procesales fundamentales". Justicia: ¿Garantías versus Eficiencia? (Coord.: DE LUIS GARCÍA, E., BELLIDO PENADÉS, R., LLOPIS NADAL, P., JIMÉNEZ CONDE, F.). Valencia: Tirant lo Blanch, pp. 815-827.

MARTÍN RÍOS, P. (2022). "Empleo de *big data* y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras". *Revista de Internet, Derecho y Política,* nº 36, pp. 1-13.

NAVARRO, J. (21 de diciembre de 2022). "Detenido un pedófilo que usaba inteligencia artificial para crear material de abuso sexual infantil". *El País*.

PARLAMENTO EUROPEO. (22 de mayo de 2023). Informe sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. COM (2021) 0206.

PARLAMENTO EUROPEO. Ley de Inteligencia Artificial. Enmiendas aprobadas por el Parlamento Europeo el 14 de junio de 2023 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)). 14 de junio de 2023. Consultado en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.pdf (Fecha de consulta: 01/10/2023).

Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica. Estrasburgo, 8 de marzo de 2022. COM (2022) 105 final.

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión. Bruselas, 21 de abril de 2021. COM (2021) 206 final.

Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)). OJ C 132, 24 de marzo de 2022, pp. 17–26.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08

RETANA GIL, C. (2023). "Diálogos para el futuro judicial LX. IA Generativa y legalidad: ¿futuro o ciencia ficción? *Diario La Ley*, nº 10371.

RICHARD GONZÁLEZ, M. (2023). "Los sistemas biométricos de reconocimiento facial en la Unión Europea en el marco del desarrollo de la Inteligencia Artificial". *Justicia,* nº 1, pp. 147-281.

RODRÍGUEZ TIRADO, ANA M. (2018). "Las víctimas menores de delitos de pornografía infantil y de delitos de child grooming y su protección en el proceso penal. Las TICs y las diligencias de investigación tecnológica". *Justicia,* nº 1, pp. 137-199.

SECRETARIA GENERAL DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. (s.f.). *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*. ISBN 978-0-8270-7306-7

SIMÓ SOLER, E. (2023). "Retos jurídicos derivados de la Inteligencia Artificial Generativa: *deepfakes* y violencia contra las mujeres como supuesto de hecho". *InDret*. 2. DOI: 10.31009/InDret.2023.i2.11.

TREND MICRO RESEARCH, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI), EUROPOL'S EUROPEAN CYBERCRIME CENTRE (EC3). (2020). Malicious uses and abuse of Artificial Intelligence. *Trend Micro Research*.

VIEJO, M. (3 de octubre de 2023). "El caso de los desnudos con IA de Almendralejo se dispara: 26 menores implicados y 21 chicas afectadas". *El País*. 3 de octubre de 2023.

VILLATORO GONZÁLEZ, T., CAMBLOR ECHANOVE, G. (16 de junio de 2023). "La propuesta de reglamento europeo sobre inteligencia artificial para mitigar los riesgos de ChatGPT". *El País*.

—. (21 de diciembre de 2022). "La Policía Nacional detiene a un pedófilo que utilizaba inteligencia artificial para crear material de abuso sexual infantil de extrema dureza". *Gabinete de prensa de la Dirección General de la Policía*. Consultado en: https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=14981# (Última consulta: 01/10/2023).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 157-180
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.08