IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

El uso de la inteligencia artificial en la investigación policial y judicial de delitos de *online child sex grooming* en España

Marc Salat Paisal
Universitat de Lleida

Fecha de presentación: julio 2024
Fecha de aceptación: enero 2025
Fecha de publicación: marzo 2025

Resumen

El uso de la inteligencia artificial en la investigación de delitos de *online child sex grooming* se presenta como una herramienta prometedora para mejorar la eficacia en la detección y persecución de estos delitos. Este fenómeno, que afecta a un número creciente de menores, plantea desafíos significativos para la policía debido al volumen de información que deben analizar. La legislación española, en consonancia con directivas europeas, establece la obligación de adoptar medidas que faciliten la investigación del *grooming*, permitiendo el análisis de material pornográfico infantil en el ciberespacio. Asimismo, desde la aprobación del Reglamento de Inteligencia Artificial se permite de forma clara el uso de herramientas de IA en el ámbito del sistema de justicia penal. Este estudio examina la viabilidad jurídica de incorporar la IA en la investigación policial y judicial de casos de *grooming*, destacando la necesidad de un marco normativo que apoye su uso y promueva la protección de los derechos de las víctimas.

Palabras clave

online child grooming; inteligencia artificial; investigación policial; sistema de justicia penal

The use of artificial intelligence in the police and judicial investigation of online child sex grooming crimes in Spain

Abstract

The utilization of artificial intelligence in the investigation of online child sex grooming offences emerges as a promising tool to enhance the efficacy in detecting and prosecuting these crimes. This phenomenon, affecting an increasing number of minors, presents significant challenges for law enforcement due to the vast amount of data they must analyse. The Spanish legislation, in alignment with European directives, mandates the adoption of measures that facilitate the investigation of OCSG, permitting the analysis of child pornographic material in the cyberspace. Moreover, following the approval of the Intelligence Artificial Act 2024, the use of AI tools within the criminal justice system has been clearly sanctioned. This study examines the legal viability of incorporating AI into police and judicial investigations, underscoring the necessity for a regulatory framework that supports its use and advocates for protecting the victims' rights.

Keywords

onlonline child grooming; artificial intelligence; police investigation; criminal justice system

Introducción

El *online child sexual grooming* (OCSG) es un fenómeno a través del cual el victimario mediante las tecnologías de la información y la comunicación consigue que un menor acceda, bien a concertar un encuentro presencial para luego atentar contra la integridad sexual de este último, bien a que le facilite material pornográfico. El atentado contra la libertad sexual se consigue principalmente a través del embaucamiento, de ganarse la confianza del menor. Este proceso permite al agresor sexual, antes de cometer el abuso sexual, poder seleccionar una víctima, obtener acceso al menor y aislarlo, desarrollar confianza con el menor y desensibilizar al menor al contenido sexual y al contacto físico. Incluso después del abuso, el delincuente puede utilizar estrategias de mantenimiento de la víctima para facilitar el abuso sexual futuro o evitar la divulgación (Winters *et al*., 2021).

Aunque las cifras de victimización varían según los países y la metodología utilizada, se estima que la prevalencia de OCSG se sitúa entre algo menos del 10 % (Bergen, 2014) y el 38 % (Soldino y Seigfried-Spellar, 2024). No obstante, en el caso español, la mayoría de las investigaciones que se han realizado al respecto indican que entre el 10 y el 15% de los adolescentes menores de 16 años han sido víctimas de algún tipo de solicitud sexual online por parte de algún adulto (Montiel *et al*., 2015; De Santisteban y Gámez-Guadix, 2017; Villacampa y Gómez, 2017).

En un estudio realizado recientemente en España con datos policiales (Soldino y Seigfried-Spellar, 2024) se indica que la mayoría de los ofensores son hombres (97,3 %), de unos 27 años de media, la mayoría de ellos de nacionalidad española (68,6 %), siendo la diferencia media de edad entre ofensor y víctima de 13,5 años. En la mayoría de los casos, los *groomers* consiguen embaucar a sus víctimas bien involucrándolas en conversaciones de connotación sexual (77 %), pidiéndoles directamente imágenes de naturaleza sexual de ellas mismas (94 %) u ofreciéndoles imágenes sexuales a las víctimas (52 %). Las principales plataformas utilizadas son Instagram y WhatsApp, que a su vez son las que mayormente utilizan los jóvenes españoles (Soldino y Seigfried-Spellar, 2024). Las víctimas son principalmente chicas (85,9 %), de unos 12,5 años de media y de nacionalidad española (90,3 %). Estos datos confirman los resultados obtenidos previamente en otros estudios sobre la dimensión y frecuencia con que se cometen este tipo de conductas delictivas (DeHart *et al*., 2017; Villacampa y Gómez, 2017; Gámez-Guadix y Mateos-Pérez, 2019; Bragado, 2020; van Gijn-Grosvenor y Lamb, 2021), si bien existe algún otro estudio que pone de relieve que el porcentaje de hombres es mayor, incluso cercano al de mujeres (Riberas *et al*., 2024; Save the Children, 2023).

Así pues, puede afirmarse que el OCSG es un problema social que afecta a un colectivo vulnerable, como es el caso de los menores de edad, en el que el Estado tiene una obligación

especial de protección, lo que obliga tanto a castigar como a prevenir estas conductas, así como a proteger a las víctimas.

Desde un punto de vista jurídico-penal, los distintos Estados europeos, entre ellos el español, han regulado como delito las conductas consistentes en el OCSG. De hecho, a nivel internacional existen dos instrumentos normativos clave: el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, hecho en Lanzarote el 25 de octubre de 2007 (en adelante, Convenio de Lanzarote); y la 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. En el caso español, ello se ha transformado en el actual artículo 183 del Código Penal mediante el cual se castiga a aquel que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con este a fin de cometer un delito de agresión sexual (art. 181 CP) o de pornografía (art. 189 CP), siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento. También cuando el propósito del autor sea embaucar al menor para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor.

Sin embargo, junto con el castigo, tanto el Convenio de Lanzarote (art. 23) como especialmente la Directiva 93/2011 (art. 15) establecen la obligación de que los Estados adopten las medidas necesarias para garantizar que la investigación o el enjuiciamiento de estas conductas pueda llevarse a cabo de forma satisfactoria, incluso sin la necesidad de depender de la denuncia de la víctima. En concreto, la mencionada Directiva establece (art. 15.4) que:

> «Los Estads miembros adoptarán las medidas necesarias para permitir a las unidades o servicios de investigación identificar a las víctimas de las infracciones contempladas en los artículos 3 a 7, en particular mediante el análisis de material pornográfico infantil tal como fotografías y grabaciones audiovisuales transmitidas o accesibles por medio de las tecnologías de la información y la comunicación».

Así pues, el Estado español en tanto que miembro del Consejo de Europa y de la Unión Europea tiene no solo la obligación de regular penalmente el OCSG, sino también la de adoptar todas aquellas medidas necesarias para prevenir estas conductas y facilitar su investigación. Entre ellas, destaca la mención expresa que hace la Directiva a que debe permitirse a la policía el análisis del material pornográfico infantil que está en el ciberespacio.

No obstante, el principal problema para cumplir con lo que establece la Directiva respecto a la prevención y a la efectiva persecución de los casos de OCSG está en la capacidad por parte de los agentes encargados de su persecución de poder analizar la gran cantidad de chats que estos reciben como posibles casos de OCSG; que, como se ha visto, es la principal vía a través de la cual se cometen estos delitos. El problema se magnifica si además se tiene en cuenta que en los últimos años se aprecia un aumento muy considerable del número de casos de OCSG. Así, por ejemplo, en un informe publicado en 2022 en el Reino Unido apunta que entre 2016 y 2021 se detectó un incremento de los casos conocidos por la policía del 450 % (Skidmore *et al*., 2022). Este mismo 2024, otro informe publicado por la National Society for the Prevention of Cruelty to Children (2024) en el Reino Unido apunta a un incremento que, aunque mucho menor que el mostrado por el informe de 2022, resulta igualmente alarmante (un 89 % de casos entre el 2018 al 2024). A este incremento importante de casos, debe sumarse un más que probable porcentaje de cifra negra, lo cual lleva a que los agentes encargados de la persecución de estos delitos no den abasto a investigar todos los casos que conocen (Chiu *et al*., 2018; Seigfried-Spellar *et al*., 2019; Soldino y Seigfried-Spellar, 2024).

Así pues, teniendo en cuenta la realidad fenomenológica del OCSG, junto con las exigencias normativas y la dificultad práctica para llevarlas a cabo, en la presente investigación se pretende analizar si desde un punto de vista jurídico es posible la incorporación de herramientas dotadas de inteligencia artificial (IA) que sirvan para automatizar las tareas consistentes en el análisis de las imágenes y chats, que permitan la identificación de aquellas variables asociadas a casos de OCSG. Específicamente, se pretende analizar si el recientemente aprobado Reglamento europeo (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (RIA) permite el uso de la IA en este ámbito y si la legislación española regula o limita su uso. Mediante estas herramientas, justamente, lo que se pretende es agilizar el proceso de investigación judicial e incrementar el número de casos que la policía es capaz de perseguir (González-Álvarez, *et al*., 2020; Seigfried-Spellar *et al*., 2019).

Aunque posteriormente se hará referencia con más detalle, cabe mencionar que cuando hablamos de IA nos referimos, de acuerdo con la definición del RIA, a un:

> «[S]istema basado en máquinas diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales».

Junto con estas herramientas, no obstante, existen otras que parten de algoritmos para realizar su predicción, pero que en ningún caso son capaces de tomar decisiones de forma autónoma.

Con todo, antes de proceder con el análisis jurídico sobre el uso de la IA en la investigación policial y judicial de los casos de OCSG, se pretende hacer un breve repaso de las herramientas de IA, así como otras herramientas basadas en algoritmos, que actualmente son utilizadas en España y en el extranjero en el marco del sistema de justicia penal. El objetivo de ello es conocer las distintas posibilidades para, posteriormente, poder analizar si su uso puede ser legal en nuestro ordenamiento para la investigación policial y judicial de los casos de OCSG.

1. Las herramientas de IA y su uso en el marco de los sistemas de justicia penal

En la actualidad existen multitud de herramientas basadas en algoritmos e incluso algunas en IA que están siendo utilizadas por parte de los operadores jurídicos que trabajan en el ámbito del sistema de justicia penal, incluso en el estado español.

A nivel policial, en Estados Unidos, por ejemplo, se utiliza una herramienta llamada COMPSTATS u otra que lleva por nombre Risk Terrain Modeling las cuales parten de datos geográficos y localización de los delitos cometidos para mapear la actividad delictiva y desarrollar estrategias de aplicación de la ley. La recopilación de estos datos, posteriormente, permite a la policía identificar tendencias y patrones de crimen (Zavrsni, 2020). Un instrumento de esta misma naturaleza, asimismo, está siendo utilizado por la Policía Nacional española para identificar lugares en los que existe una concentración de hechos delictivos (Camacho Collados, 2016; González-Álvarez *et al*., 2020). La policía utiliza también otras herramientas basadas en IA para la prevención y la persecución de la delincuencia. En este sentido, la IA es utilizada, por ejemplo, para reconocer el calibre de un arma con tan solo escuchar el sonido de un disparo (Raponi *et al*., 2022) o para el reconocimiento facial de delincuentes (Smith y Miller, 2022), entre muchas otras finalidades. En España es famosa la herramienta VeriPol, que permite estimar la probabilidad de que una denuncia por robo sea falsa (Quijano Sánchez *et al*., 2018; Martínez Garay et al., 2024). Igualmente, existe el sistema VioGén, el cual es utilizado por la policía para predecir el riesgo de reincidencia en casos de violencia de género, lo que a su vez lleva aparejado medidas policiales para la protección y seguridad de estas víctimas (Presno Linera, 2023). Esta última según parece, está en tránsito para incorporar tecnología basada en IA para realizar sus predicciones (Europa Press, 2024).

A nivel judicial también se utilizan herramientas basadas en IA. Estas existen, por ejemplo, para sistematizar toda la documentación del proceso, para predecir el fallo de la sentencia e incluso para determinar la duración de la pena (Miró Llinares, 2018; Rodger *et al*., 2022). En el ámbito de la ejecución de penas es habitual el uso de herramientas de predicción del riesgo. Estas se utilizan tanto para clasificar penados como para decidir sobre la concesión o no de permisos, y entre las herramientas más famosas, aunque realmente estas no están basadas en IA, podemos encontrar COMPAS, HART o RisCanvi (Martínez Garay, 2016).

Incluso, específicamente para casos de OCSG, existen diversas herramientas pensadas para perseguir de forma más eficiente a los presuntos autores de estas infracciones penales. En este sentido, en Estados Unidos se ha desarrollado la herramienta basada en IA llamada *Chat Analysis Triage Tool*, que permite a la policía hacer una priorización de las denuncias que reciben por delitos de OCSG (Seigfried-Spellar *et al*., 2019). También el Child Safe AI, que monitoriza el contenido de la web en busca de imágenes de pornografía infantil, o el PrevBot, que sirve para controlar las conversaciones de chatrooms en internet con el objetivo de predecir posibles casos de abuso sexual infantil (Zavrsni, 2020; Pasha *et al*., 2022). Asimismo, existe la herramienta Sweetie, que es un *chatbot* con apariencia de niña, creado por la organización Terre des Hommes en 2013 y que tiene como objetivo captar posibles *groomers* o abusadores (Agustina y Vargas, 2019).

2. La legislación europea sobre el uso de la IA en la investigación de delitos

En lo que respecta a la legislación sobre inteligencia artificial y su posible uso en la investigación policial y judicial de delitos, es importante destacar que hasta el 13 de marzo de 2024 no existía una normativa a nivel de la Unión Europea, momento en el que el Parlamento Europeo aprobó el ya mencionado RIA.

Previamente, el Parlamento Europeo, en una Resolución 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)), había reconocido la posibilidad de utilizar herramientas basadas en IA en el ámbito del sistema de justicia penal, siempre que se cumplieran con una serie de exigencias. Entre las más importantes, la Resolución exige la obligación de que exista control democrático de la herramienta y que ésta cumpla con el principio de proporcionalidad. En este sentido, el documento, de hecho, prohíbe de forma expresa el uso de la IA con el objetivo de realizar vigilancias masivas. Por lo que respecta a los propios algoritmos, la Resolución establece la obligación de que estos sean transparentes, explicables, trazables y comprobables. Asimismo, la Resolución alerta que es necesario que se tenga en cuenta el potencial sesgo de las herramientas basadas en IA en este ámbito, así como la necesidad de respetar el principio de contradicción en el proceso penal. Finalmente, establece que debe garantizarse la intervención humana, de modo que los operadores jurídicos sean los que tomen las decisiones.

Asimismo, por parte de la UE y con carácter previo al RIA se habían aprobado normativas que, a pesar de no regular de forma específica el uso de la IA en el ámbito que nos ocupa, sí que, bien de forma directa, bien indirectamente, tienen incidencia en la respuesta a la pregunta de investigación que se plantea en el presente trabajo. Por una parte, la Directiva (EU) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos, y por la que se deroga la Decisión marco 2008/977/JAI del Consejo, en la que en su artículo 11 establece la prohibición de que se tomen decisiones basadas en el análisis de datos de forma automatizada en el ámbito del sistema de justicia penal. Por otra parte, el mismo día se aprobó también el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), mediante el cual se prohíbe (art. 22) que se tomen decisiones basadas únicamente en el tratamiento automatizado de datos que produzcan efectos jurídicos.

Por lo que respecta al RIA y su afectación al objeto de la presente investigación, el concepto de IA (art. 3 RIA) se define, tal como se ha indicado *supra*, como aquel:

> «[S]istema basado en máquinas diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales».

La ley, además, reconoce que la IA puede emplearse en diversas aplicaciones, entre las que destaca el ámbito del sistema de justicia penal, si bien su uso requiere ser analizado y clasificado según el riesgo que implique para los usuarios y ciudadanos en relación con sus derechos fundamentales. En relación con la clasificación de riesgo, el RIA (arts. 5 y ss.) establece cuatro niveles:

1) no existe riesgo o este es mínimo,

2) riesgo limitado,

3) riesgo alto, y

4) riesgo inaceptable.

Por lo que se refiere al objeto del presente trabajo, el artículo 6, junto con el anexo III del RIA 2024 establecen que los sistemas de IA que sean utilizados por parte de los agentes del sistema de justicia penal para evaluar la robustez de las fuentes de prueba obtenidas durante una investigación policial o un proceso penal deben ser considerados de nivel de riesgo alto. Parece, pues, que justamente las herramientas de IA como las que se plantean aquí, dirigidas a automatizar las tareas consistentes en el análisis de las imágenes y chats que permitan la identificación de aquellas variables asociadas con casos de

OCSG, entrarían dentro de la clasificación de alto riesgo, más si posteriormente los agentes de la policía o el Ministerio Fiscal utilizan el resultado de la IA como clave para determinar la comisión de un delito. Aunque en aquellos casos en que el análisis de datos solo se utilizare como filtro previo, para determinar en cuántos de los casos que llegan a las manos de la policía existe alguna probabilidad de que nos encontremos ante un delito de OCSG, en tanto que ello puede, en la práctica, tener una influencia directa en la toma de decisiones (art. 6.3 RIA, entendido a *sensu contrario*), también debería considerarse que este es un uso de alto riesgo.

La clasificación de una herramienta de IA, como las que se propone, de alto riesgo implica que debe satisfacer muchos más requisitos que un sistema de IA de riesgo menor. Entre ellos, la obligación de cumplir con unos estándares de seguridad y transparencia, lo que implica que previamente a su uso deba documentarse de forma detallada toda la información sobre el sistema de la IA y su finalidad para que las autoridades evalúen el cumplimiento de los requisitos exigidos. Una vez autorizado, se exige la necesidad de documentar los elementos, proceso y fases de la IA, así como que pueda trazarse cómo se llega al resultado final. Igualmente, se deben crear sistemas de evaluación y mitigación de los riesgos de la IA. Se exige, además, una alta calidad de los conjuntos de datos que alimentan el sistema con el objetivo de minimizar los riesgos de sesgo y de evitar resultados discriminatorios. El sistema, pues, requiere de un nivel alto de robustez, seguridad y precisión en el análisis. Finalmente, se exige que se adopten medidas adecuadas de supervisión humana con la finalidad de minimizar los riesgos.

3. El derecho español y las limitaciones sobre el uso de la IA en la investigación de delitos de OCSG

A nivel español, hasta el día en que se han escrito estas líneas solo está vigente la LO 7/2021 que transpone y reproduce lo indicado en la Directiva 2016/680. Al margen de ello, no existe ninguna otra normativa específica sobre el uso de herramientas basadas en IA; menos aún, en el ámbito del sistema de justicia penal, que limite el uso de la IA, más allá de lo que establece el RIA.

Así pues, teniendo en cuenta que el RIA habilita la posibilidad del uso de herramientas basadas en IA –siempre, evidentemente, que se respeten las limitaciones, los requisitos y las garantías que la ley europea establece– es necesario analizar brevemente si existen otro tipo de limitaciones en su uso. Para ello, teniendo en cuenta las implicaciones a los derechos fundamentales de los investigados, se analizará, primero, las posibles limitaciones del uso de la IA en el ámbito de la investigación de delitos de OCSG por parte de la policía y, posteriormente, en el seno del proceso penal.

Empezando por la primera de las posibilidades, la legislación permite que la policía judicial realice diligencias de investigación de delitos con carácter previo al inicio del proceso penal (art. 20 RD 769/1987). Estas diligencias, además, pueden ir dirigidas a perseguir delitos en general, siempre que ello no suponga realizar investigaciones prospectivas de una concreta persona con la finalidad de buscar potenciales actividades delictivas que haya podido cometer (STS 314/2015, de 4 de mayo).

Entre las posibilidades, la policía judicial se encuentra plenamente facultada para rastrear las fuentes digitales abiertas, incluidas las redes sociales, con el objetivo de encontrar indicios que puedan ser relevantes para el curso, si es el caso, de una investigación judicial posterior (Circular 2/2022, de 20 de diciembre, de la Fiscalía General del Estado, sobre la actividad extraprocesal del Ministerio Fiscal en el ámbito de la investigación penal). Igualmente, es posible incorporar en las diligencias de investigación las fuentes de prueba obtenidas por particulares, como puede ser el registro de chats que posibles víctimas de *grooming* puedan aportar a la policía. Así, es posible el rastreo de fuentes digitales abiertas (como pueden ser webs, foros en internet, redes sociales, etc.) mediante herramientas como la Child Safe AI o el PrevBot. Incluso, nada impide que se usen herramientas basadas en IA para filtrar y priorizar el gran volumen de casos que llega a manos de la policía española, al estilo de la herramienta Chat Analysis Triage Tool mencionada anteriormente con el objetivo de mejorar la capacidad de trabajo de esta y con ello poder llegar a un mayor número de casos. De hecho, en tanto que no se limiten derechos fundamentales de terceros es posible realizar cualquier tipo de investigación. La única limitación se establece en el momento en que se hayan recopilado indicios suficientes de la comisión de alguno de los tipos penales en los que se concreta el OCSG, pues entonces será necesario iniciar el proceso penal y, con ello, seguir las reglas allí establecidas. En este sentido, la STS 980/2016,

de 11 de enero, establece que estas investigaciones «agotan su funcionalidad cuando sirven de respaldo a la decisión del fiscal de archivar la denuncia o promover el ejercicio de las acciones penales que estime pertinentes».

Lo que en ningún caso estaría permitido en una fase prejudicial es el uso de otros métodos como el agente encubierto informático[1] para encontrar potenciales delincuentes en la red, pues está expresamente prohibido por ley. Esta posibilidad, que podría ser muy útil en el ámbito del OCSG, está expresamente reservada para los casos en que existe una investigación judicial, tal como se infiere del articulado del artículo 282 bis.2 LECrim al indicar que «El *juez de instrucción* podrá autorizar...».[2] En este punto, es clave determinar si herramientas de IA como son los *chatbots* –por ejemplo, Sweetie–, que se hiciesen pasar por menores de edad a modo de potenciales víctimas de OCSG debe ser considerado un «agente» encubierto informático. Aunque realmente en este caso el agente es una aplicación informática basada en IA, lo que es seguro es que detrás existe un agente de policía, encargado de supervisar y de validar los resultados de la máquina, así que su uso fuera del ámbito de una investigación judicial se plantea muy complicado (Agustina y Vargas, 2019). Si su uso queda reservado a la fase judicial pierde gran parte de su utilidad: la de poder «cazar» a potenciales *groomers*, puesto que ello resultaría en una investigación judicial prospectiva, prohibida en el derecho procesal penal español, tal como establece, por ejemplo, la STC 197/ 2009, de 28 de septiembre. A ello se suma otros problemas, como el hecho de que estaríamos ante un delito imposible (Cuatrecasas Monforte, 2022; Agustina y Vargas, 2019).

Posteriormente, una vez iniciada la fase judicial, la legislación española no limita la posibilidad de utilizar tecnología basada en IA para conseguir fuentes de prueba, siempre que posteriormente ello se presente a través de alguno de los medios de prueba admitidos en derecho. En esta fase, sin embargo, es importante respetar todas las garantías constitucionales ligadas al proceso penal. El posible uso de herramientas basadas en IA en este punto, de hecho, no puede alterar el alcance de los distintos derechos, garantías y límites relacionados con las fuentes de prueba. A ello debe sumarse la necesidad de que, tal como indica el RIA, es necesario tener en cuenta que su uso respete los distintos principios que han sido establecidos por la legislación europea y sobre todo que el resultado de la investigación sea consecuencia de la intervención humana y no del algoritmo (de Luis García, 2023).

4. A modo de conclusiones: el uso de la IA en la investigación policial y judicial en los casos de OCSG

De los estudios sobre OCSG realizados por la doctrina, se puede concluir que éste es un fenómeno lo suficientemente grave –tanto por afectar a un porcentaje elevado de menores, como por los bienes jurídicos afectados– para merecer la pena buscar nuevas vías para perseguir de forma eficaz por parte de los agentes del sistema de justicia. Justamente se ha visto que la legislación aplicable relativa a la prevención y persecución de estos delitos obliga a los estados parte a que tomen medidas de política criminal tales como la introducción de mecanismos de persecución eficaces. En este sentido, las herramientas basadas en IA se presentan como claves para gestionar el volumen de trabajo que implica la recopilación de evidencias en casos complejos de OCSG. A ello se suma el reciente avance legislativo a nivel europeo mediante el cual se regula su uso. Así, si bien con anterioridad a 2024 la legislación era parca, lo que podía generar problemas de seguridad jurídica, así como el riesgo de que la prueba fuera declarada ilegal, desde que el RIA regula el uso de la IA de forma específica en el ámbito del sistema de justicia penal, debe concluirse que a partir de ahora sí que es posible legalmente usar este tipo de herramientas en la investigación policial de delitos de OCSG e incluso, en el ámbito judicial.

Dicho lo anterior, cabe tener presente que la implementación de la IA en la lucha contra el OCSG presenta beneficios, sobre todo en la fase policial de investigación de estos hechos delictivos. A su vez, también presenta serios desafíos, en particular, en relación con su implementación y el respecto a las garantías del proceso penal.

Por lo que se refiere a los beneficios, las distintas herramientas de IA que actualmente existen podrían ser útiles

1. Término que se utiliza para designar a los funcionarios de policía que actúan en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito. Su principal regulación jurídica se encuentra en el artículo 282 bis LECrim.
2. Cursiva añadida por el autor.

para su aplicación en una fase prejudicial en la persecución de estos delitos dada su capacidad para filtrar y priorizar casos, lo que facilitaría una gestión más eficiente, permitiendo a los cuerpos policiales enfocarse en los supuestos de mayor relevancia y en los que existen más indicios de que estamos ante un posible caso de OCSG. Como consecuencia de los límites en los derechos fundamentales que impone la legislación procesal penal española, la herramienta que menos útil se presenta es la implementación de *chatbots* como Sweetie 2.0, pues el uso de agentes encubiertos informáticos solo se permite una vez que existe una investigación judicial. Teniendo en cuenta el principal objetivo que se persigue con su uso; agilizar el proceso de investigación judicial e incrementar el número de casos que la policía es capaz de perseguir, más difícil es ver los beneficios del uso de herramientas basadas en IA una vez en la fase de instrucción, si bien su uso es legal y, por ejemplo, podría servir para facilitar la búsqueda de los hechos clave en un *chat log*. A pesar de ello, su uso difícilmente podría superar el *test* de proporcionalidad.

No obstante, debe también tenerse en cuenta que la doctrina ha puesto de manifiesto que existen multitud de riesgos asociados con el uso de herramientas basadas en algoritmos o en IA. Algunos de los más denunciados son, por ejemplo, el sesgo o su baja capacidad para predecir los casos más graves (Martínez Garay *et al*., 2024). Lo cierto es que para evitar estos y otros problemas propios de las herramientas basadas en algoritmos o en IA, es muy importante que previamente haya un análisis del fenómeno de OCSG integral, que tenga en cuenta los distintos perfiles de los distintos ofensores y de las víctimas, y que los datos con que se alimenten los sistemas sean lo suficientemente completos para evitar que los resultados no sean mejores que los que podría ofrecer un humano. En este sentido, creo que la implementación de IA, en lugar de agravar la situación, puede ofrecer una oportunidad para identificar y mitigar estos sesgos, mejorando potencialmente la equidad del sistema (Zavrsnik, 2020). De hecho, los riesgos sobre sesgo que puedan imputarse a una herramienta de IA son los mismos que han podido generar los humanos, pues provienen de los datos –generados por humanos– con los que el sistema se alimenta (Miró Llinares, 2020). Igualmente, es necesario que el algoritmo sea transparente, explicable y que sea robusto. Otra cuestión relacionada con las garantías es la necesidad de motivar las decisiones, en el sentido de que la IA sea considerada solo como una herramienta de apoyo a los agentes policiales y judiciales, y no como un sustituto de sus funciones. La IA debe complementar el trabajo humano, proporcionando análisis y datos que permitan una toma de decisiones más informada y precisa (de Luis García, 2023). Estas herramientas deberán asimismo cumplir con el resto de los requisitos exigidos por el RIA, por lo que deben ser transparentes, robustas, trazables, etc. También con las garantías y derechos de los investigados en el seno del proceso penal (de Miguel Beriain y Pérez Estrada, 2019; de Luis García, 2023). De hecho, se considera clave que la creación e implementación de estas medidas se lidere desde el sector público, pues de lo contrario difícilmente podrá cumplirse con las exigencias europeas.

En resumen, la IA tiene el potencial de transformar significativamente la gestión de los casos policiales de OCSG, aportando herramientas que mejoren la eficiencia operativa y las capacidades predictivas de las fuerzas de seguridad, pero que en ningún caso sustituyan a estas. No obstante, es crucial que se utilice de manera complementaria, con una comprensión clara de sus limitaciones y riesgos, para asegurar que el papel fundamental de los agentes del sistema de justicia se mantenga y fortalezca.

Reconocimientos

Este artículo ha sido elaborado en el marco de los Proyectos de investigación Derecho penal y comportamiento humano (MICINN-RTI2018-097838-B-100) y Ciberacoso sexual a menores: perfiles linguísticos para el desarrollo de herramientas digitales forenses para prevención, detección y priorización en España (PID2020-117964RB-I00).

Referencias bibliográficas

AGUSTINA, J. R.; VARGAS, A. (2019). «¿Es necesaria una dogmática de los ciberdelitos? A propósito de la utilización de agentes encubiertos en la lucha contra la explotación sexual de menores en el ciberespacio». En: García Cavero, P. y Chinguel Rivera, A. I. (coords). *Derecho y Persona*, págs. 609-644. Perú: Ideas Solución Editorial.

BERGEN, E. (2014). *Comparing adult-youth and adult-adult online sexual solicitation: Manipulative behaviors, situational factors, and outcomes*. Tesis doctoral. Abo: Abo Akademy University.

BRAGADO, A. (2020). «Visión criminológica del delito online grooming». *Behavior & Law Journal*, vol. 6, n.º 1, págs. 42-50. DOI: https://doi.org/10.47442/blj.v6.i1.73

CAMACHO COLLADOS, M. (2016). *Statistical analysis of spatio-temporal crime patterns: Optimization of patrolling strategies*. Tesis doctoral [en línea]. Disponible en: http://hdl.handle.net/10481/44557. Granada: Universidad de Granada. [Fecha de consulta: 22 de julio de 2024].

CHIU, M.; SEIGFRIED-SPELLAR, K.; RINGENBERG, T. (2018). «Exploring detection of contact vs. fantasy online sexual offenders in chats with minors: Statistical discourse analysis of self-disclosure and emotion words». *Child Abuse & Neglect*, vol. 81, págs. 128-138. DOI: https://doi.org/10.1016/j.chiabu.2018.04.004

CUATRECASAS MONFORTE, C. (2022). *La Inteligencia Artificial en el proceso penal de instrucción español: posibles beneficios y potenciales riesgos*. Tesis doctoral. Universitat Ramon Llull.

DE LUIS GARCÍA, E. (2023). «Justicia, inteligencia artificial y derecho de defensa». *IDP. Revista de Internet, Derecho y Política*, n.º 39, págs. 1-12. DOI: https://doi.org/10.7238/idp.v0i39.417164

De MIGUEL BERIAIN, I.; PÉREZ ESTRADA, M. (2019). «La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados». *Revista de Derecho UNED*, n.º 25, págs. 531-561. DOI: https://doi.org/10.5944/rduned.25.2019.27013

DE SANTISTEBAN, P.; GÁMEZ-GUADIX, M. (2017). «Prevalence and risk factors among minors for online sexual solicitations and interactions with adults». *Journal of Sex Research*, vol. 55, pág. 1 y ss. DOI: https://doi.org/10.1080/00224499.2017.1386763

DEHART, D.; DWYER, G.; SETO, M. C.; MORON, R.; LETOURNEAU.; E.; SCHWARZ-WATTS, D. (2017). «Internet sexual solicitation of children: A proposed typology of offenders based on their chats, e-mails, and social network posts». *Journal of Sexual Aggression*, vol. 23, n.º 1, págs. 77-89. DOI: https://doi.org/10.1080/13552600.2016.1241309

Europa Press (2024, 5 de septiembre). «Igualdad iniciará "en breve" un proyecto piloto que incorporará la IA al Sistema VioGén para detectar víctimas». *Europa Press* [en línea]. Disponible en: https://www.europapress.es/epsocial/igualdad/noticia-igualdad-iniciara-breve-proyecto-piloto-incorporara-ia-sistema-viogen-detectar-victimas-20240905142913.html. [Fecha de consulta: 1 de enero de 2025].

GÁMEZ-GUADIX, M.; MATEOS-PÉREZ, E. (2019). «Longitudinal and reciprocal relationships between sexting, online sexual solicitations, and cyberbullying among minors». *Computers in Human Behavior*, vol. 94, págs. 70-76. DOI: https://doi.org/10.1016/j.chb.2019.01.004

GONZÁLEZ-ÁLVAREZ, J. L.; SANTOS-HERMOSO, J.; CAMACHO-COLLADOS (2020). «Policía predictiva en España. Aplicación y retos de futuro». *Behavior & Law Journal*, vol. 6, n.º 1, págs. 26-41. DOI: https://doi.org/10.47442/blj.v6.i1.75

INNERARITY, D. (2023). «Prediciendo el pasado: una crítica filosófica del análisis predictivo». *IDP. Revista de Internet, Derecho y Política*, n.º 39, págs. 1-12. DOI: https://doi.org/10.7238/idp.v0i39.409672

MARTÍNEZ GARAY, L. (2016). «Errores conceptuales en la estimación de riesgo de reincidencia. La importancia de diferenciar sensibilidad y valor predictivo, y estimaciones de riesgo absolutas y relativas». *Revista Española de Investigación Criminológica*, vol. 14, págs. 1-31. DOI: https://doi.org/10.46381/reic.v14i0.97

MARTÍNEZ GARAY, L. (coord.). (2024). *Three predictive policing approaches in Spain: Viogén, RisCanvi and Veripol Assessment from a human rights perspective*. Universitat de València [en línea]. Disponible en: https://regulation.blogs.uv.es/files/2024/05/Three-predictive-policing-perspectives-web-17.06.24.pdf. [Fecha de consulta: 22 de julio de 2024].

MIRÓ LLINARES, F. (2018). «Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots». *Revista de Derecho Penal y Criminología*, n.º 20, págs. 87-130. DOI: https://doi.org/10.5944/rdpc.20.2018.26446

MIRÓ LLINARES, F. (2020). «Policía predictiva: ¿utopía o distopía? Sobre las actitudes hacia el uso de algoritmos de big data para la aplicación de la ley». *IDP. Revista de Internet, Derecho y Política*, n.º 30, págs. 1-18. DOI: https://doi.org/10.7238/idp.v0i30.3223

MONTIEL, I.; CARBONELL, E.; PEREDA, N. (2015). «Multiple online victimization of Spanish adolescents: Results from a community sample». *Child Abuse & Neglect*, vol. 52, pág. 123 y ss. DOI: https://doi.org/10.1016/j.chiabu.2015.12.005

NATIONAL SOCIETY FOR THE PREVENTION OF CRUELTY TO CHILDREN (2024). «Online grooming crimes against children increase by 89% in six years». *NSPCC* [en línea]. Disponible en: https://www.nspcc.org.uk/about-us/news-opinion/2024/online-grooming-crimes-increase/. [Fecha de consulta: 30 de diciembre de 2024].

PASHA, S. A.; ALI, S.; JELJELI, R. (2022). «Artificial Intelligence Implementation to Counteract Cybercrimes Against Children in Pakistan». *Arena of Technologies*. DOI: https://doi.org/10.1007/s42087-022-00312-8

PRESNO LINERA, M. A. (2023). «Policía predictiva y prevención de la violencia de género: el sistema VioGén». *IDP. Revista de Internet, Derecho y Política*, n.º 39, págs. 1-13. DOI: https://doi.org/10.7238/idp.v0i39.416473

QUIJANO-SÁNCHEZ, L.; LIBERATORE, F.; CAMACHO-COLLADOS, J.; CAMACHO-COLLADOS, M. (2018). «Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police». *Knowledge-Based Systems*, vol. 149, págs. 155-168. DOI: https://doi.org/10.1016/j.knosys.2018.03.010

RAPONI, S.; OLIGERI, G.; ALI, I.M. (2022). «Sound of guns: digital forensics of gun audio samples meets artificial intelligence». *Multimed Tools Appl*, vol. 81, págs. 30387-30412. DOI: https://doi.org/10.1007/s11042-022-12612-w

RIBERAS-GUTIÉRREZ, M.; RENESES, M.; GÓMEZ-DORADO, A.; SERRANOS-MINGUELA, L.; BUENO-GUERRA, N. (2024). «Online Grooming: Factores de Riesgo y Modus Operandi a Partir de un Análisis de Sentencias Españolas». *Anuario de Psicología Jurídica*, vol. 34, págs. 119-131. DOI: https://doi.org/10.5093/apj2023a9

RODGER, H.; LENSEN, A.; BETKIER, M. (2022). «Explainable artificial intelligence for assault sentence prediction in New Zealand». *Journal of the Royal Society of New Zealand*, vol. 53, n.º 1, págs. 133-147. DOI: https://doi.org/10.1080/03036758.2022.2114506

SAVE THE CHILDREN (2023). *Online grooming. Análisis de sentencias sobre abusos sexuales en internet a niños y niñas en España*. Save the Children [en línea]. Disponible en: https://www.savethechildren.es/sites/default/files/2023-11/OnlineGrooming_ESP.pdf. [Fecha de consulta: 30 de enero de 2025].

SCHULZ, A.; BERGEN, E.; SCHUHMANN, P.; HOYER, J.; SANTTILA, P. (2016). «Online Sexual Solicitation of Minors How Often and between Whom Does It Occur?». *Journal of Research in Crime and Delinquency*, vol. 53, pág. 165 y ss. DOI: https://doi.org/10.1177/0022427815599426

SEIGFRIED-SPELLAR, K C.; ROGERS, M. K.; RAYZ, J. T.; YANG, S.; MISRA, K.; RINGENBERG, T. (2019). «Chat analysis triage tool: Differentiating chats between minors and contact-driven vs. noncontact driven child sex offenders». *Forensic Science International*, vol. 297, págs. e8-e10. DOI: https://doi.org/10.1016/j.forsciint.2019.02.028

SKIDMORE, M.; AITKENHEAD, B.; MUIR, R. (2022). «Turning the tide against online child sexual abuse». *Police Found* [en línea]. Disponible en: https://www.police-foundation.org.uk/wp-content/uploads/2022/07/turning_the_tide_FINAL-.pdf. [Fecha de consulta: 22 de julio de 2024].

SMITH, M.; MILLER, S. (2022). «The ethical application of biometric facial recognition technology». *AI & Soc*, vol. 37, págs. 167-175. DOI: https://doi.org/10.1007/s00146-021-01199-9

SOLDINO, V.; SEIGFRIED-SPELLAR, K. C. (2024). «Criminological differences between contact-driven and online-focused suspects in online child sexual grooming police reports». *Child Abuse & Neglect*, vol. 149. DOI: https://doi.org/10.1016/j.chiabu.2024.106696

VAN GIJN-GROSVENOR, E. L.; LAMB, M. E. (2021). «Online groomer typology scheme». Psychology, *Crime & Law*, vol. 27, n.º 10, págs. 973-987. DOI: https://doi.org/10.1080/1068316X.2021.1876048

VILLACAMPA, C.; GÓMEZ, M. J. (2017). «Online child sexual grooming: Empirical findings on victimisation and perspectives on legal requirements». *International Review of Victimology*, vol. 23, n.º 2, págs. 105-121. DOI: https://doi.org/10.1177/0269758016682585

WACHS, S.; WOLF, K.; PAN, C. (2012). «Cybergrooming: Risk factors, coping strategies and associations with cyberbullying». *Psicothema*, vol. 24, pág. 628 y ss.

WINTERS, G. M., KAYLOR, L. E. y JEGLIC, E. L. (2021). «Toward a Universal Definition of Child Sexual Grooming». *Deviant Behavior*, vol. 43, pág. 926 y ss. DOI: https://doi.org/10.1080/01639625.2021.1941427

ZAVRŠNIK, A. (2020). «Criminal justice, artificial intelligence systems, and human rights». *ERA Forum*, vol. 20, pág. 567 y ss. DOI: https://doi.org/10.1007/s12027-020-00602-0

Cita recomendada

SALAT PAISAL, Marc (2025). «El uso de la inteligencia artificial en la investigación policial y judicial de delitos de *online child sex grooming* en España». *IDP. Revista de Internet, Derecho y Política*, núm. 42. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i42.430914

Sobre la autoría

Marc Salat Paisal
Universitat de Lleida
marc.salat@udl.cat

Profesor agregado Serra Húnter de derecho penal en la Universitat de Lleida. Su investigación se ha centrado en el análisis de determinados procesos de victimización y desvictimización, especialmente en relación con determinadas formas de violencia de género y con el tráfico de seres humanos, así como con cuestiones relacionadas con las sanciones penales ante la delincuencia sexual y las alternativas al proceso penal. Actualmente es co-IP de un proyecto de investigación sobre delitos por razón de honor y miembro de otro proyecto sobre el uso de la IA en delitos de *sex grooming*, en los que estudia los riesgos, los retos normativos y las posibles estrategias de prevención y detección de este fenómeno.