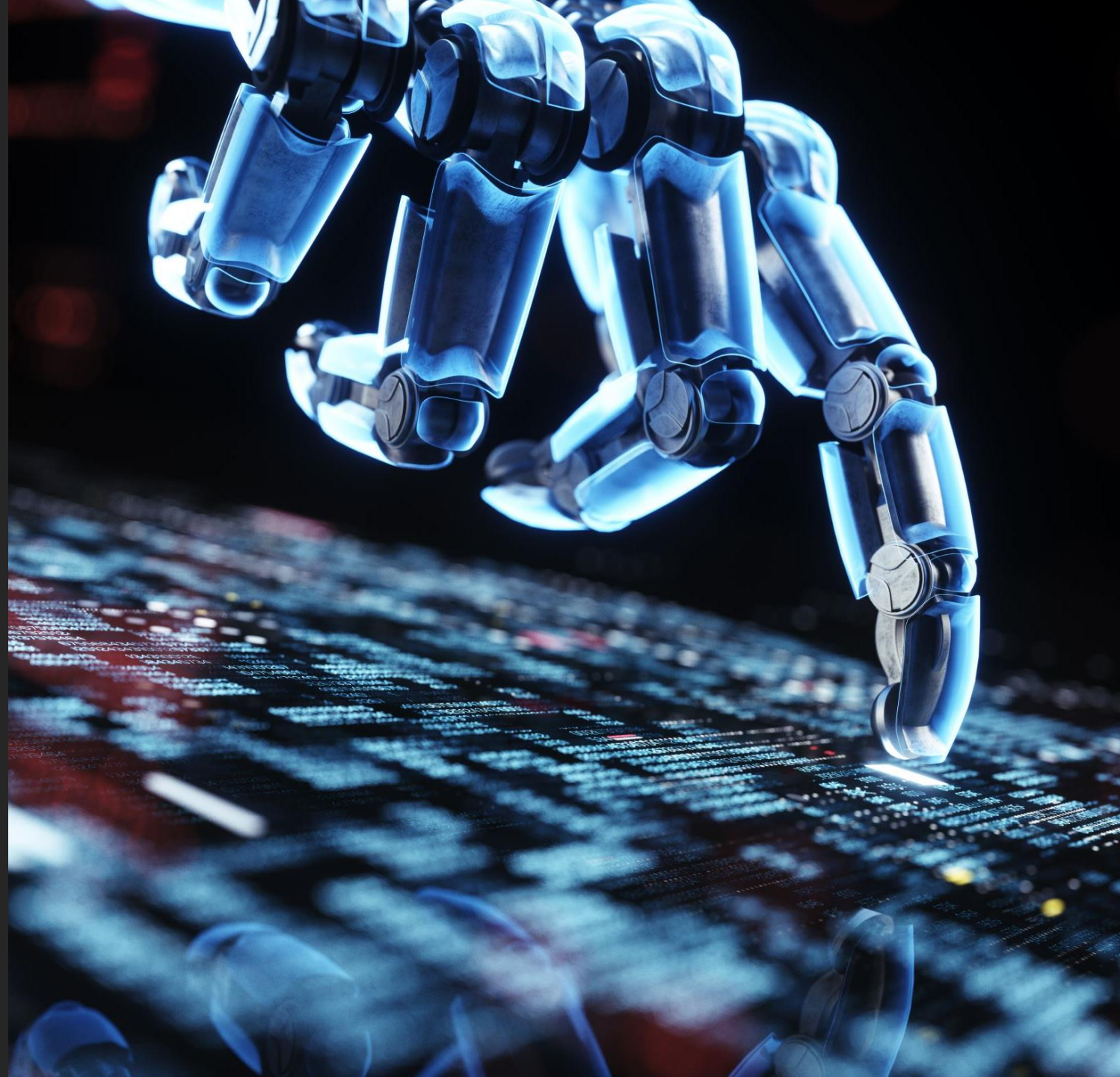
HERRAMIENTAS DE IA Y VIOLENCIA DE GÉNERO

Carlota Cuatrecasas Monforte
Magistrada de la Plaza nº17 de la Sección Penal del TI de Barcelona



HERRAMIENTAS DE IA

Para cometer delitos

→ Facilita la ejecución de delitos ya existentes

→ Provoca la creación de nuevos tipos delictivos

Para investigar delitos y proteger a las víctimas

→ Permite aumentar la eficacia de las herramientas tradicionales

→ Posibilita la creación de nuevas formas de protección

HERRAMIENTAS DE IA

PARA INVESTIGAR DELITOS Y PROTEGER A LAS VÍCTIMAS

1- HERRAMIENTAS DE PREDICCIÓN Y EVALUACIÓN DE RIESGOS

2- HERRAMIENTAS PARA INVESTIGAR DELITOS Y PROTEGER A LAS VÍCTIMAS

3- OTRAS

1. Herramientas de predicción y evaluación de riesgos

A) ¿Qué son?

Sistemas que emplean IA para analizar datos históricos y pronosticar eventos y comportamientos futuros

B) Ámbitos de aplicación

Policial (usos -ej.VioGén-), penitenciario (RisCanvi) y judicial

C) Regulación

Reglamento Europeo de IA : artículos 5 y 6 (y Anexo III)

LO 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (supletoriamente: RGPD)

2. Herramientas de investigación de delitos y/o generadoras de contenido probatorio

A) Qué son?

Sistemas que, a través de la IA, pueden llevar a cabo labores con utilidad para la averiguación y la constatación de la perpetración de delitos.

B) Regulación

Reglamento Europeo de IA: artículos 5 y 6 (y Anexo III)

LO 7/2021, de 26 de mayo (supletoriamente RGPD)

C) Clases

a) Herramientas que emplean datos biométricos

b) Herramientas que emplean técnicas de Procesamiento del Lenguaje Natural (PLN)

c) Herramientas que emplean técnicas de análisis de imágenes

d) Sistemas que permiten detectar *Deep Fakes*

ARTÍCULO 6-> ANEXO III. SISTEMAS DE IA DE ALTO RIESGO

8. **Administración de justicia y procesos democráticos:**

Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial:

-en la investigación e interpretación de hechos y de la ley,

-así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos.

a) Herramientas que emplean datos biométricos

✓*Datos biométricos:* únicos, singulares e intransferibles de cada individuo (3.34)

✓Principal utilidad: identificar y verificar la identidad de las personas

-muestra dubitada vs muestra indubitada-

✓Clases

a.1) Reconocimiento facial
a.2) Reconocimiento de voz
a.3) Reconocimiento de emociones
a.4) Reconocimiento de huellas dactilares y ADN
a.5) Reconocimiento de firma y de escritura

Especial mención a los sistemas de identificación biométrica remota a tiempo real (autorización judicial)

ARTICULO 5: PROHIBICIONES

h) **el uso de sistemas de identificación biométrica remota «en tiempo real» (3.42) en espacios de acceso público con fines de garantía del cumplimiento del Derecho**, **SALVO** y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,

iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

b) Herramientas que emplean técnicas de Procesamiento del Lenguaje Natural (PLN)

- ✓ PLN: técnica de traducción del lenguaje humano (tanto hablado como escrito) a un lenguaje que “la máquina” (o, de modo más específico, el algoritmo) pueda entender

- ✓ Clases

a.1) *Chatbots*

a.2) Sistemas de análisis de textos/documentos

a.3) Sistemas de detección de contenido ilícito *on line* y de *malware*

a.1) *Chatbots*

-Contacto directo con policía o con servicios sociales (asistencia a víctimas/testigos. Caso Alexa)

-Análisis de conversaciones con sujetos sospechosos/investigados (agente encubierto)

REGULACIÓN

Artículo 6.2-Anexo III: sistemas de IA de alto riesgo

5.c) Sistemas de IA destinados a evaluar y clasificar llamadas de emergencia de personas físicas o utilizarse para despachar o establecer prioridades en el servicio de despachos de primera respuesta de emergencia, incluidos los de policía
8.a) Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios;

a.2) Sistemas de análisis de textos/documentos

-Examen de documentos
-Detección de denuncias falsas (VeriPol)

a.3) Sistemas de detección de contenido ilícito *on line* y de *malware*

-Detección de contenido ilícito escrito en la red

-Filtrado del correo electrónico/mensajes digitales para detectar *malware*

c) Herramientas que emplean técnicas de análisis de imágenes

- ✓Análisis de imágenes: técnica que permite examinar ciertos símbolos y/o figuras estáticos o dinámicos y reconocer la información que estos representan

- ✓Clases

c.1) Sistemas de detección de contenido ilícito *on line*

c.2) Sistemas de detección de contenido ilícito *off line*

c.3) Sistemas de lectura automática de placas de matrícula

c.1) Sistemas de detección de contenido ilícito *on line*

-detección de contenido audiovisual ilícito en la red
-análisis y comparativas de imágenes

c.2) Sistemas de detección de contenido ilícito *off line*

Análisis y comparativas de imágenes

c.3) Sistemas de lectura automática de placas de matrícula

d) Herramientas que permiten detectar *Deep Fakes*

- ✓*Deep Fake*: creación falsa pero hiperrealista generada a través de la IA con el fin de suplantar la identidad de uno o varios individuos, imitando principalmente su apariencia y/o su voz

- ✓Riesgo: su introducción en el proceso penal como pruebas falsas

- ✓Posible solución: uso de sistemas de IA para detectar la falsedad o autenticidad de las imágenes y/o los audios presentados.

OTRAS

a) Sistemas para facilitar el cumplimiento de la obligación de comparecencias *apud acta*

b) Herramientas de textualización/transcripción

c) Herramientas de traducción e interpretación

d) Herramientas de verificación de requisitos y de tramitación y gestión procesal

OTRAS

a) Sistemas para facilitar el cumplimiento de la obligación de comparecencias *apud acta*

b) Herramientas de textualización/transcripción

c) Herramientas de traducción e interpretación

d) Herramientas de verificación de requisitos y de tramitación y gestión procesal

MUCHAS GRACIAS

c.cuatrecasas@poderjudicial.es