Carlota Cuatrecasas Monforte
Doctora Derecho (Mención Internacional)
Jueza Jugado Penal 1 Tarrasa

LA INTELIGENCIA ARTIFICIAL Y LA INVESTIGACIÓN DE DELITOS

LA INTELIGENCIA ARTIFICIAL Y LA INVESTIGACIÓN DE DELITOS

1.- INTRODUCCIÓN

1.1.- El uso de la inteligencia artificial (IA) en el ámbito de la Justicia: una aproximación.

Bill Gates, tecnólogo por excelencia de nuestra era, pronunció la que sin duda es una de las frases célebres que mejor reflejan la realidad de la eclosión tecnológica que hoy en día estamos viviendo y que, por supuesto, cuenta con sus luces y con sus sombras: "*La primera regla de cualquier tecnología utilizada en una empresa es que la automatización aplicada a una operación eficiente magnificará la eficiencia. La segunda es que la automatización aplicada a una operación ineficiente magnificará la ineficiencia*".

Y tal aseveración, cargada de contenido y fuerza, aplicable, sin duda, al uso de la IA, tanto en el sector privado como en el sector público, debería servir de base para la toma de cualquier decisión relacionada con tal tecnología, ya que si bien muchos la ven como una posible salvación sin precedentes, lo cierto es que esta tiene un desmedido potencial para generar el efecto contrario al que se pretende conseguir con su uso, por lo que debe emplearse con muchísima cautela.

Y es que la IA, desde luego, es una herramienta tecnológica que cuenta con capacidad más que suficiente para magnificar la eficiencia de las tareas humanas, eso es un hecho indiscutible, pero asimismo tiene un enorme potencial para magnificar su ineficiencia e incluso, perpetuarla, lo cual resulta extremadamente peligroso, especialmente en el ámbito de la justicia.

Históricamente, uno de los mayores retos con los que se han topado las sociedades ha sido el de conseguir una justicia de calidad. Tal cuestión, no obstante, no ha sido ni será jamás resuelta de un modo uniforme y homogéneo, habida cuenta de la gran diversidad de culturas y civilizaciones que han convivido, conviven y convivirán en nuestro planeta, que tienen distintos valores y distintas formas de concebir y entender qué es lo justo y lo injusto y, desde luego, cómo debe gestionarse.

Así, no cabe duda de que existen tantas definiciones de justicia como personas habitan el mundo, y ello fue precisamente lo que, bajo mi punto de vista, creó en la humanidad la necesidad de alcanzar pactos sociales para convivir en paz, habida cuenta de lo inviable y salvaje que resulta para los humanos, como seres racionales que somos, vivir sin fijar unas bases comunes de convivencia que, compartidas por la mayoría, garanticen los derechos individuales y colectivos previamente establecidos, tal y como defendieron las teorías del contrato social desarrolladas por Hobbes, Locke y Rousseau.

Y en la actualidad, tales pactos sociales, existentes en mayor o menor medida y bajo diferentes formatos, en prácticamente todos los lugares del mundo, tienen un contenido distinto en cada territorio. No obstante, y a pesar de la referida gran diversidad, existe una específica premisa común: la necesidad de que la resolución de los conflictos se lleve a cabo en un lapso de tiempo y con una celeridad prudencialmente aceptable. Y es que tal y como ya advirtió el filósofo Séneca miles de años atrás, el retraso en la resolución de conflictos puede producir enormes injusticias, ya que "*nada se parece tanto a la injusticia como la justicia tardía*".

En España, Estado democrático y de Derecho, en virtud de lo dispuesto en el artículo 117 de la Constitución Española, la justicia emana del pueblo y se administra en nombre del Rey por jueces y magistrados integrantes del poder judicial, uno de los tres poderes del Estado.

Y, en concreto, todo el engranaje que hace funcionar la maquinaria judicial en nuestro país, como es sabido, se halla incorporado en la Administración de Justicia que, sin duda, está cargada de eficiencias que conviene magnificar y, por supuesto, también de ineficiencias que, por el contrario, conviene reducir al máximo o eliminar, por lo que el uso de la IA debe hacerse de forma muy controlada en tal ámbito y, sobre todo, con garantías de éxito legalmente avaladas, como se verá más adelante.

Por desgracia, no solo hoy en día, sino históricamente, el servicio que la referida Administración ha venido prestando a los ciudadanos no ha sido el esperado, y ello ha derivado en que la Administración de Justicia haya sido y continúe siendo la peor valorada por los justiciables españoles[1], lo cual se reputa inaceptable. Inaceptable principalmente porque la justicia resulta la última y la única opción que tienen miles de personas para resolver aquellos conflictos que influyen en los más importantes aspectos de sus vidas y que no les dejan vivir con la paz que todo ser humano merece.

Principalmente, la justicia española es lenta, en ocasiones extremadamente lenta, y ello es algo que, como es evidente, conviene mejorar. Y entiendo que el progreso en tal sentido pasa por buscar posibles soluciones y analizar qué opciones existen hoy en día para evolucionar y mejorar la calidad del servicio prestado por la Administración, lo cual debería ser la principal aspiración (y es, desde luego, la principal responsabilidad) de todo servidor público.

Y qué mejor manera de buscar formas de progreso que la de explorar todas aquellas posibilidades que pueden ofrecernos las nuevas tecnologías que tenemos hoy en día disponibles y, en concreto, la IA, que todavía es una tecnología poco explorada en el ámbito de la justicia, principalmente porque no suele resultar rentable invertir en investigación para su uso con fines públicos.

En concreto, además, me gustaría poner de manifiesto que si bien la calidad del servicio que ofrecen los tribunales debe ser la máxima en cualquier orden jurisdiccional y en cualquier fase procesal, entiendo que en la fase de instrucción del proceso penal los derechos de los ciudadanos requieren de especial protección, habida cuenta del momento tan inicial en que se halla la investigación de hechos presuntamente delictivos, con

[1] Véase, entre otras, la encuesta sobre Opinión pública y política fiscal elaborada por el Centro de Investigaciones Sociológicas (CIS) en julio de 2021. Última visita el 22 de marzo de 2023. https://datos.cis.es/pdf/Es3332marMT_A.pdf

información generalmente escasa y poco clara, con el riesgo que ello conlleva tanto para las víctimas (y, eventualmente, para la sociedad en general), que precisan de protección, como para las personas investigadas como presuntos autores, siendo que en todo caso debe prevalecer su derecho a la presunción de inocencia, y tal colisión de derechos, no suele resultar fácil de gestionar, máxime con recursos materiales y humanos muy limitados, tanto policiales como judiciales.

1.2.- La necesidad de regulación del uso de la IA, especialmente en el ámbito de la Justicia.

Así, los beneficios que podría aportar la IA para conseguir mejorar la calidad y la eficiencia del mencionado proceso penal de instrucción, como se verá, son evidentes, si bien no pueden analizarse de modo responsable sin ser puestos en una balanza con los posibles riesgos que esta podría implicar, ya que tienen potencial, incluso, para empañar las propias bonanzas.

La buena noticia es que los referidos riesgos pueden minimizarse e incluso llegar a eliminarse mediante la regulación, y es que el Derecho juega un rol fundamental en el ámbito de la IA, puesto que se erige como herramienta clave para poner límites y garantizar que esta se emplee para crear valor en la sociedad, en aplicación de lo dispuesto en el artículo 18.4 de la Constitución Española.

Así, corresponde, principalmente al poder legislativo, establecer unas bases regulatorias claras y completas que permitan hacer un uso adecuado y garantista de la IA con el fin de lograr mejorar la calidad de la justicia, en concreto penal, lo cual se circunscribe en el ámbito de las obligaciones que el artículo 9.2 de la referida Carta Magna impone a los poderes públicos al establecer: "*Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social.*"

Y la referida regulación, habida cuenta de que la IA es una tecnología que no entiende de fronteras y que, por ende, debe estudiarse desde una perspectiva global, bajo mi punto de vista debería hacerse desde una doble perspectiva:

-por un lado, una perspectiva transnacional, a través de una institución u organización internacional, que debería fijar unos mínimos comúnmente exigibles a todos los países del mundo (o los máximos posibles) para garantizar un uso de la IA en beneficio de la humanidad, a poder ser de forma jurídicamente vinculante, para evitar actuaciones basadas en intereses particulares con potencial lesivo para el bien común.

Y es que, por un lado, entiendo que en el ámbito internacional la institución que estaría mejor posicionada para establecer unos principios básicos o normas mínimas comunes sobre el uso de la IA a nivel mundial sería la Organización de las Naciones Unidas (ONU), puesto que esta cuenta con la membresía de la práctica totalidad de los países del mundo (un total de 193 Estados miembros), y ya en el pasado ha adoptado regulaciones de similar naturaleza con fines de bien común, a saber, la Declaración Universal de Derechos Humanos, adoptada y proclamada por la Asamblea General en su

resolución 217 A (III), de 10 de diciembre de 1948, que sin duda marcó un hito en la historia de la humanidad.

Así, entiendo que dicha normativa podría recogerse en una Declaración Universal de Principios de IA, que, en mi opinión, debería contener, al menos, los siguientes principios:

- *Principio de respeto a la dignidad del ser humano, con garantía de supervisión y control humano de los sistemas de IA y prioridad del bienestar social y ambiental;*
- *Principio de respeto a la libertad y a la privacidad del ser humano, con garantía de gestión individual de los datos personales;*
- *Principio de transparencia y explicabilidad de los sistemas;*
- *Principio de equidad, igualdad, no discriminación del ser humano e inclusión;*
- *Principio de robustez, solidez técnica y seguridad;*
- *Principio de responsabilidad.*[2]

No obstante, en el caso de la normativa básica en materia de IA, bajo mi punto de vista sería necesario dar un paso más. Y es que esta tecnología tiene capacidad para escapar del control de los seres humanos, lo cual podría resultar una gran amenaza para nuestra especie. En tal sentido, ya Brad Darrach, en 1970, parafraseando a uno de los padres de la IA, Marvin Minsky, manifestó "*Si los humanos tienen suerte, puede que* (las máquinas) *decidan conservarlos como animales de compañía. Si no tienen suerte, se les tratará como comida*".[3]

Así, aunque ello suene un tanto catastrofista y deba tomarse con ciertas cautelas, considero que resultaría absolutamente fundamental que la eventual normativa básica o de mínimos que se adoptara a nivel internacional en materia de IA tuviera carácter jurídicamente vinculante, a fin de evitar eventuales conductas de Estados miembros díscolos con intereses particulares que pudieran llevar a la humanidad a un punto de no retorno, ya que es evidente que si la IA saliera del control humano, la afectación resultaría global.

Además, para garantizar el cumplimiento de tal regulación, entiendo que deberían establecerse unos férreos mecanismos de control que previeran fuertes y disuasorias sanciones para aquellos que decidieran incumplir, ya que, como he dicho, el daño ocasionado por estos podría ser irreparable; y, por otro lado, una perspectiva nacional, a través de los poderes legislativos de cada Estado (o conjuntos de Estados, como en el caso de la Unión Europea), que deberían establecer de forma más específica y profunda los modos de uso y los límites de la IA en el ámbito de sus respectivas jurisdicciones, siempre con respeto a los principios básicos fijados a nivel internacional.

Y es que es importante, en materia de IA, que todos vayamos en la misma dirección, a pesar de los múltiples intereses (sobre todo, económicos y de poder) que existen a su

[2] Cuatrecasas Monforte, C. "*La Inteligencia Artificial como herramienta de investigación criminal*". Editorial La Ley. 2022. Pág.50.
[3] Darrach, B. (1970). "Meet Shaky, the first electronic person: The fascinating and fearsome reality of a machine with a mind of its own". *Life.* Pág.66.

alrededor, ya que su potencial lesivo, como se ha dicho, es real y elevado, y resulta extremadamente peligroso para todos.

En la actualidad, no obstante, por desgracia, no contamos ni con una regulación básica ni con una más específica, al menos en España y en el ámbito de la Unión Europea, lo cual resulta muy decepcionante.

Así, por un lado, respecto de la normativa básica, si bien se han llevado a cabo numerosas iniciativas (tanto públicas como privadas), para establecer los principios básicos que deberían regir en torno al uso de la IA, lo cierto es que ninguna de ellas ha tenido el alcance al que he hecho referencia.

No obstante, al respecto, especial mención merece, por la gran cantidad de Estados firmantes, la adoptada por la UNESCO en su 41ª Conferencia General celebrada del 9 al 24 de noviembre de 2021, consistente en la publicación de una Recomendación sobre la Ética de la IA, si bien carece de carácter jurídicamente vinculante, siendo una mera recomendación, lo cual es claramente insuficiente, por los motivos ya expuestos.

Por otro lado, respecto de la normativa específica, en este caso, sorprende que la Unión Europea, que suele resultar enormemente garantista con el respeto a los derechos y las libertades de sus ciudadanos, en este caso haya llegado "tarde y mal", a pesar de la responsabilidad que ostentaba por ser el mercado único más grande del mundo (y, de hecho, todavía no ha llegado, puesto que aún no se ha publicado el texto definitivo del Reglamento Europeo de IA). Y, como consecuencia de tal falta de regulación, en algunos de los Estados miembros de la referida Unión se han venido empleando durante los últimos años sistemas de IA con potencial para vulnerar derechos fundamentales de forma masiva, tal y como se han encargado de denunciar múltiples organizaciones *pro* derechos humanos, lo cual resulta absolutamente intolerable.

Cierto es que en fecha 21 de abril de 2021 la Comisión Europea publicó 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 y, posteriormente, el Consejo de la Unión Europea, en su sesión nº3917/1, celebrada los días 5 y 6 de diciembre de 2022, adoptó su posición ("orientación general") sobre la referida propuesta, si bien resta pendiente la publicación, en los próximos meses, como ya he avanzado, del Reglamento Europeo de Inteligencia Artificial, lo cual, sin duda, supondrá un antes y un después en el uso de la IA en todos los ámbitos, entre otros, en el de la investigación criminal y la justicia.

A la espera, pues, como he dicho, del texto definitivo de Reglamento Europeo sobre IA, no obstante, especialmente crítica me muestro con el contenido de la referida Propuesta de la Comisión Europea, puesto que, a mi juicio, los mecanismos de control de calidad de los sistemas de IA que prevé son claramente insuficientes en lo referente a herramientas de investigación criminal.

Y es que en la antedicha Propuesta únicamente se impone un control público activo en caso de tratarse de sistemas que emplean datos biométricos para la identificación de personas físicas a tiempo real o remoto y, ello, sin embargo, no se exige para el resto de herramientas de IA cuyo uso se permite para fines de investigación criminal (artículos 43

-procedimiento ordinario- y 47 -procedimiento de urgencia-), a pesar de que la gran mayoría de estas son calificadas como de alto riesgo por la propia Propuesta, lo cual no se reputa lógico.

Mi sugerencia al respecto, desde luego, es la de ir más allá, y es que considero que la clave del éxito del uso de la IA en el ámbito de la UE para fines de investigación criminal subyace en la fijación de unos férreos y completos mecanismos de control de calidad *ex ante* (con carácter previo a su puesta en circulación) y *ex post* (cada cierto tiempo, para comprobar que los estándares cualitativos siguen cumpliéndose, de forma similar a lo que se lleva a cabo con los vehículos a motor con la Inspección Técnica de Vehículos -ITV).

Y, para ello, entiendo que una buena solución sería la de la creación de una Agencia Europea de IA, que centralizara el filtro y el control de la calidad de los sistemas que pretendieran ser empleados dentro de nuestras fronteras (similar a la Agencia Europea del Medicamento), con una sede central y, a su vez, si así se requiriera, delegaciones en los distintos Estados miembros.

Y es que considero que, si bien el control de calidad de los sistemas de IA debe ser siempre escrupuloso, en el caso del sector público, este debe ser absolutamente exquisito, habida cuenta de que en el ámbito del sector privado, si una empresa emplea algoritmos que luego resultan ser poco transparentes, por ejemplo, el usuario puede decidir contratar con la competencia, pero en caso de que sea el sector público el que emplea sistemas de IA para tomar decisiones que pueden afectar a los ciudadanos, estos no pueden renunciar o escoger que no se les apliquen sus resultados, que les son impuestos, por lo que los estándares de calidad deben ser aún más altos si cabe.

Y es que esa Agencia Europea de IA a la que he hecho referencia entiendo que otorgaría mucha confianza no solo a los ciudadanos, que necesitan garantías de que los sistemas de IA empleados, en este caso por las autoridades, son transparentes, explicables, seguros y contienen datos de calidad, con el fin de evitar vulneraciones de derechos fundamentales; sino también a los titulares de las millonarias patentes que los presentan.

No obstante, en la referida Propuesta de la Comisión Europea lo más similar a lo expuesto que se prevé es la creación de un Comité Europeo de IA (en su Título VI, artículos 56 a 58), que vele por el cumplimiento de la normativa que fije el futuro Reglamento sobre IA, e impulse la adopción de nuevas medidas, lo cual es una buena solución, pero bajo mi punto de vista insuficiente.

España, en concreto, se ha avanzado a la futura publicación del mencionado Reglamento Europeo sobre IA y ya ha anunciado que contará con una Agencia Española *de Supervisión de la Inteligencia Artificial (AESIA)***,** que llevará a cabo labores de supervisión y minimización de riesgos y buscará generar un ecosistema de investigación y empresarial de IA[4], cuya sede física estará en La Coruña.

[4] Véase nota de prensa publicada el 13 de septiembre de 2022 por el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Política Territorial en fecha, en el marco del programa España Digital 2026. Última visita el 18 de marzo de 2023.
https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/20220913_ndp_sede_agencia_ia.pdf

Y ello, si bien resulta una buena noticia, habida cuenta de que implica la creación de un organismo de control del uso de la IA en nuestro país, lo cierto es que no obedece a ningún plan conjunto de actuación liderado por la UE en virtud de una legislación conjunta previamente adoptada (que todavía no está aprobada), por lo que existe el riesgo de que, tras la publicación del referido Reglamento Europeo de IA, los planes de España deban ceñirse a otro tipo de estrategia, habida cuenta de que lo realmente efectivo sería que en todo caso fuera la UE la que acogiera la sede central de una potencial Agencia Europea de IA que asumiera competencias realmente activas (muchas más y de mayor impacto que las que contempla la Propuesta de la Comisión Europea) y, en su caso, descentralizara algunas funciones.

A la vista de lo expuesto, no obstante, procede poner de manifiesto que, aun en el caso de que llegara a existir una regulación básica y otra más específica, considero importante advertir que las autoridades, a la hora de emplear sistemas de IA, deberían hacerlo con la mayor de las cautelas y con la máxima diligencia y responsabilidad posibles, habida cuenta de los peligros que ello implica (al igual que lo hacen hoy el médico al recetar un medicamento o el farmacéutico al dispensarlo, por muy aprobado que esté su uso por la Agencia Europea del Medicamento).

En cualquier caso, es importante poner de manifiesto que la legislación sobre IA siempre deberá ir de la mano con la legislación en materia de protección de datos personales. Y es que los sistemas de tal tecnología se nutren de datos, de ingentes cantidades de datos, que han sido calificados como el petróleo del S.XXI, y, en gran parte, el éxito y el fracaso de los sistemas de IA depende de la calidad de esos datos.

Así, si se introducen en el sistema datos de mala calidad (poco representativos, obtenidos de forma ilícita, tratados sin cumplir con la normativa vigente, erróneos, etc), los resultados que arroje el sistema de IA que fue entrenado con ellos, serán asimismo deficientes, lo cual es conocido como el fenómeno: "*garbage in, garbage out*" (si entra basura, sale basura) y obviamente debe tratar de evitarse.

No obstante, cada vez existe más conciencia al respecto, y los sistemas de IA no solo cuentan con *software* más sofisticados y potentes, sino que emplean datos de mejor calidad para su entrenamiento, resultando esencial la concurrencia de ambas condiciones para que estos funcionen y lo hagan de forma óptima y correcta -lo mínimo esperable, sobre todo, en caso de ser empleado por el sector público-.

Ello, no obstante, aunque pueda parecer sencillo, es tarea complicada y a los sistemas con los que contamos hoy en día (aunque van avanzando a pasos agigantados), todavía les queda mucho camino por recorrer para alcanzar niveles aceptables de calidad (que, en el caso de uso por parte del sector público, debe rozar la infalibilidad), lo cual en ocasiones sigue generando situaciones con potencial vulnerador de derechos y libertades.

2.- LA IA PARA INVESTIGAR DELITOS

Expuesto lo anterior, por un lado, me gustaría hacer especial referencia a aquellas herramientas de IA que podrían resultar de mayor utilidad para mejorar la eficiencia del proceso penal de instrucción español y, asimismo, me gustaría hacer especial mención a los potenciales riesgos más comunes que he podido detectar en ellas y que, por ende, se debería tender a evitar.

Con el fin de sistematizar y ordenar la información y facilitar el análisis de cada una de las referidas herramientas, entiendo necesario hacer una clasificación de las mismas en tres grandes bloques:

1) Herramientas de predicción y evaluación de riesgos.
2) Herramientas de investigación de delitos.
3) Herramientas de tramitación.

a) Herramientas de predicción y evaluación de riesgos

A.1. ¿Qué son?

Los algoritmos, como tales, es evidente que no pueden predecir hechos futuros, pero desde luego sí que pueden estimar la probabilidad de que algo suceda basándose en los datos previos ya existentes.[5]

Así, las herramientas de predicción y evaluación de riesgos son aquellos sistemas que emplean IA para analizar datos históricos y pronosticar comportamientos y eventos futuros, como por ejemplo: dónde, cuándo y por quién es más probable que vaya a cometerse un delito, si un investigado tiene o no riesgo de fuga o de reiteración delictiva, si un interno va a reingresar o no en prisión tras la concesión de un permiso, o si una empresa va a deshacerse o no de sus activos tras la interposición de una querella contra ella.

Y tales sistemas, sin duda, pueden aportar un valor inmenso para auxiliar a las autoridades policiales y judiciales en la toma de decisiones de suma importancia, tales como: destinar más o menos efectivos policiales a una zona y/o en un horario concreto, someter a una persona a programas destinados a la reinserción social, acordar una medida cautelar de prisión provisional, conceder o denegar un permiso penitenciario o, en su caso, imponer una fianza o acordar un embargo.

A.2. Ámbitos de aplicación

Hoy en día, la aplicación de las antedichas herramientas resulta ampliamente extendida en el ámbito policial, existiendo más reticencias al respecto en el ámbito judicial, a pesar de que, como se verá, estas ya se emplean en diversos sistemas judiciales del mundo, como por ejemplo en Estados Unidos (EEUU).

No obstante, lo cierto es que en muchas ocasiones los jueces y magistrados tienen en cuenta la información relativa al riesgo proporcionada por la policía como un elemento más para fundamentar sus decisiones y, en caso de que tales valoraciones hayan sido efectuadas empleando sistemas de IA de predicción y evaluación de riesgos, estos estarían resultando aplicados, de forma indirecta, por las mencionadas autoridades judiciales.

A.2.1. Policial

Los sistemas de policía predictiva tienen como principal prioridad la de optimizar

[5] Waldman, A. (2019). «Power, Process, and Automated Decision-Making». *Fordham Law Review* (88). Pág. 5.

recursos y mejorar así la eficiencia de las tareas policiales de prevención criminal.

Y tal tarea se lleva a cabo mediante el análisis, a través de la IA, de los datos históricos que constan en las bases de datos policiales, y la posterior creación de unas escalas de riesgo que fijan las probabilidades de que un determinado comportamiento o evento se produzca, lo cual aporta una valiosísima información para poder, por ejemplo, incrementar la vigilancia en aquellas zonas geográficas y aquellas franjas horarias calificadas como "calientes" o sobre aquellos perfiles de personas calificadas con mayor riesgo de delinquir o con mayor vulnerabilidad (a saber, más predisposición para ser víctima de un delito).

En tal sentido, y a los efectos de poner de manifiesto las diferencias existentes entre la actividad policial tradicional (eminentemente reactiva) y la actividad policial predictiva, la Agencia de los Derechos Fundamentales de la Unión Europea elaboró en el año 2019 el siguiente (bajo mi punto de vista, muy ilustrativo) cuadro comparativo:

	ACTIVIDAD POLICIAL TRADICIONAL	POLICÍA PREDICTIVA
Contexto	Comisión de un delito o presentación de alerta sobre una persona en particular	Ni se ha cometido ningún delito ni se ha presentado ninguna alerta sobre una persona en particular
Aproximación	Reactiva	Proactiva
Objetivo	Detener al/los/las sospechoso/s/as	Prever dónde y cuándo pueden cometerse delitos o por/contra quién
Datos utilizados	Información específica relacionada con el caso	Información genérica relativa a varios casos
Tipo de proceso	Los procesos basados en datos y los procesos humanos se combinan	Se centra principalmente en procesos basados en grandes cantidades de datos

[6]

En concreto, los referidos sistemas de policía predictiva se centran en tres grandes bloques:

- La predicción de delitos (o mapeo delictivo), para pronosticar dónde -zonas geográficas, más o menos acotadas- y cuándo -estaciones el año, meses, días, franjas horarias u "horas punta", etc- existe un mayor riesgo de comisión de actos delictivos;

- La predicción de identidades delictivas, para identificar a los potenciales delincuentes del futuro, mediante la elaboración de perfiles criminales, normalmente con base en circunstancias y comportamientos de su pasado; y

- La predicción de identidades vulnerables, para identificar a los potenciales individuos o grupos de individuos que es más probable que resulten víctimas de un

[6] Cuatrecasas Monforte, C. "*La Inteligencia Artificial como herramienta de investigación criminal*". Editorial La Ley. 2022. Pág.130

delito en el futuro.

Y todo ello, sin duda, puede aportar un valor enorme para, en efecto, aumentar la eficiencia de las tareas policiales y, por ende, mejorar la calidad de las mismas, lo cual sin duda debería traducirse en una disminución de los actos delictivos -y a eso es a lo que se debe aspirar-.

Así, es evidente que si se invierten recursos en optimizar las labores preventivas de la policía con empleo de IA (capaz de analizar y cruzar ingentes cantidades de datos), y ello se lleva a cabo en estrecha colaboración con otros organismos -a saber, servicios sociales, instituciones penitenciarias, fiscalía, juzgados y tribunales, etc- con capacidad para promover y adoptar las medidas complementarias necesarias y oportunas en caso de detectar ciertos riesgos, los resultados obtenidos podrían suponer un gran avance hacia la paz social, en relación con las tareas policiales reactivas (o incluso con las tareas tradicionales preventivas pero basadas únicamente en comparativas de datos -limitados- efectuadas por efectivos humanos).

Como he avanzado con anterioridad, diversos cuerpos policiales de múltiples países del mundo a día de hoy ya emplean sistemas de policía predictiva, a saber: en Europa (entre otros, Alemania, Italia y Reino Unido), en América del Norte (Canadá y Estados Unidos -entre otros, los estados de California, Illinois y Nueva York-), en América Latina (entre otros, Chile), o en Asia (entre otros, Singapur).

En España, en la actualidad, de modo oficial no consta que se empleen herramientas de IA de policía predictiva, si bien procede hacer especial mención al sistema de evaluación de riesgos VioGén, de la Secretaría de Estado de Seguridad del Ministerio del Interior, en cumplimiento de lo establecido en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, que fue puesto en funcionamiento el 26 de julio de 2007[7].

Y es que tal herramienta -que parte de la doctrina entiende que no cuenta con tecnología de IA, sino que es un mero sistema actuarial-, establece una escala que determina el nivel de riesgo (no apreciado, bajo, medio, alto y extremo) que tiene una víctima de violencia de género y sus hijos menores de padecer nuevos ataques por parte de su agresor.

Al respecto, si bien el Ministerio del Interior manifiesta que desde la puesta en funcionamiento de tal herramienta la reincidencia de las agresiones machistas ha descendido un 25%,[8] lo cierto es que el hecho de que tal sistema no conste públicamente auditado y que la transparencia no sea completa llevó a la Fundación Eticas, en colaboración con la Fundación Ana Bella, a publicar el 8 de marzo de 2022 un informe de auditoría externa con diversos puntos controvertidos a examinar.[9]

[7] http://www.interior.gob.es/web/servicios-al-ciudadano/violencia-contra-la-mujer/sistema-viogen

[8] Véase noticia publicada en La Vanguardia el 19 de mayo de 2019. *Algoritmos contra la violencia machista.* Última visita el 24 de marzo de 2023. https://www.lavanguardia.com/tecnologia/20190519/462147339117/algoritmos-violencia-machista.html

[9] Véase el contenido íntegro en https://eticasfoundation.org/wp-content/uploads/2022/03/ETICAS-FND-The-External-Audit-of-the-VioGen-System.pdf. Última visita el 28 de marzo de 2022.

A.2.2. Judicial

Los sistemas de justicia predictiva tienen como principal prioridad la de optimizar recursos y mejorar así la eficiencia de las actuaciones judiciales tendentes a valorar riesgos futuros, lo cual siempre resulta tarea delicada.

Y tal tarea se lleva a cabo mediante el análisis, a través de la IA, de los datos históricos que constan en las bases de datos judiciales, y la posterior creación de unas escalas de riesgo que fijan las probabilidades de que un determinado comportamiento o evento se produzca, lo cual aporta una valiosísima información para poder, por ejemplo, acordar medidas cautelares.

En el ámbito judicial, el uso del referido tipo de herramientas se lleva a cabo tanto en la fase *pre* juicio (para asistir al juez en la adopción de medidas cautelares), como *per* y *post* juicio (para asistir al juez en la determinación de la peligrosidad de los individuos acusados/procesados, y en el análisis de riesgo de reincidencia de los ya condenados, a los efectos de eventual suspensión de ejecución de penas, concesión de permisos penitenciarios, etc).

A diferencia de lo expuesto respecto del uso de las herramientas de predicción y evaluación de riesgos en el ámbito policial, donde están muy extendidas, como ya se ha dicho, ello no transcurre del mismo modo en el ámbito judicial.

No obstante, sin duda existen ya jurisdicciones donde el uso de tal tipo de herramientas sí se lleva a cabo de forma extensa, como sucede, por ejemplo, en EEUU, ya que estas se usan en diversos de sus estados y condados, tal y como concretaron las organizaciones Media Mobilizing Project de Filadelfia (Pensilvania, EEUU) y MediaJustice de Oakland (California, EEUU), que elaboraron una base de datos nacional[10] que determina en qué jurisdicciones de tal país se emplean herramientas de IA de evaluación de riesgos y, en su caso, cuáles (entre otras, COMPAS y PSA).

En relación con ello, resulta interesante hacer especial mención al referido sistema COMPAS, una herramienta de IA que emplea tecnología de *Machine Learning* o aprendizaje automático en su funcionamiento, utilizada por los jueces de determinados estados de EEUU (entre otros, Nueva York, Wisconsin y California), que pronostica el riesgo de que un individuo cometa nuevos delitos en el futuro.

No obstante, una investigación de la agencia ProPublica efectuada ya en el año 2016 determinó que el algoritmo empleado por tal herramienta (que, por cierto, no es público y permanece oculto) contenía sesgos contra ciertos grupos (entre otros, las personas de raza negra)[11], lo cual, desde luego, es absolutamente inadmisible.

En cualquier caso, el uso de herramientas de este tipo, con capacidad para analizar y cruzar ingentes cantidades de datos, tal y como se ha puesto de manifiesto con anterioridad, podrían resultar de gran utilidad para auxiliar (nunca sustituir) a los jueces

[10] Véase en https://pretrialrisk.com/national-landscape/where-are-prai-being-used/ Última visita el 12 de marzo de 2023.

[11] Véase Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine Bias*. ProPublica. Última visita el 17 de marzo de 2023.
https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

en su tarea de valorar riesgos futuros, si bien, como se verá más adelante, ello únicamente podría resultar jurídicamente viable en caso de que se hiciera con las máximas garantías de respeto de los derechos fundamentales de las personas afectadas.

b) Herramientas de investigación de delitos

B.1. ¿Qué son?

Las herramientas de IA de investigación de delitos son aquellos sistemas que funcionan con IA y pueden ser empleadas por las autoridades policiales, fiscales y judiciales para averiguar y hacer constar la perpetración de delitos, con todas las circunstancias que puedan influir en su calificación, así como la culpabilidad de los delincuentes, conforme a lo dispuesto en el artículo 299 de la Ley de Enjuiciamiento Criminal.

No obstante, no existe una categoría o clasificación científica tan específica en el ámbito de la IA que aglutine todas las referidas herramientas, si bien he entendido procedente llevar a cabo su estudio conjunto para agrupar todos aquellos sistemas que cuentan con unas características y unas utilidades prácticas similares e idóneas para la investigación criminal, en aras de facilitar su análisis.

B.2. Clases

B.2.1. Herramientas que emplean datos biométricos

Los datos biométricos se definen, entre otros, en el ámbito europeo, en el artículo 4.14 del Reglamento General de Protección de Datos (RGPD) que establece que son "*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*"; y en el ámbito nacional, en el artículo 5.l) de la Ley Orgánica 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, que dispone que son "*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*".

Así, los datos biométricos, por definición singulares, únicos e intransferibles de cada individuo, tienen un enorme valor a efectos identificativos, en especial en el ámbito de la investigación criminal.

Y hoy en día ya existen sistemas de IA que emplean tal clase de datos para llevar a cabo las siguientes funciones:

- Por un lado, identificar, dar respuesta a la pregunta de: ¿quién es este individuo?; y

- Por otro lado, comprobar o verificar la identidad, es decir, dar respuesta a la pregunta de: ¿es este individuo realmente quien dice ser o quien se sospecha que es?

Con el fin de llevar a cabo tales tareas, los sistemas de IA efectúan la comparación de imágenes dubitadas, que son introducidas por las autoridades, e indubitadas, que se hallan en vastas bases de datos policiales o judiciales, y en caso de existir coincidencia o "*match*" entre ellas, hacen saltar una alerta que arroja resultados positivos y muy útiles.

B.2.1.1. Reconocimiento facial

A modo de concepto, puede decirse que el reconocimiento facial es aquella tecnología que permite, a través de la IA, identificar a personas o comprobar/verificar su identidad a través de las formas, proporciones y rasgos de su rostro.

En relación con sus potenciales utilidades, el uso de un buen sistema de IA de reconocimiento facial podría ayudar, por un lado, a identificar o verificar la presencia de ciertos delincuentes en determinados lugares, pudiendo incluso llegar a sustituir (o complementar), por ejemplo, la actual diligencia de rueda de reconocimiento.

Además, existen ya aplicaciones que permiten elaborar, a partir de una mera fotografía, el perfil de un sospechoso en cuestión de minutos (como sucede por ejemplo con Clearview, si bien existen múltiples polémicas sobre su uso[12]); y, asimismo, en China, por ejemplo, ya está extendido el uso, por parte de los agentes de policía, de las denominadas "gafas inteligentes", que cuentan con sistemas de reconocimiento facial incorporados capaces de identificar a tiempo real, mientras sus portadores patrullan, a aquellos ciudadanos con cuentas pendientes con la Administración[13], lo cual podría resultar altamente efectivo para localizar a las personas sobre las que pesan órdenes de busca y captura, entre otras.

Por otro lado, a partir de la incorporación de sistemas de reconocimiento facial en cámaras de videovigilancia podría detectarse la entrada en ciertos lugares públicos (a saber, el metro, una determinada pobación, etc) de aquellas personas sobre las que pesaran medidas cautelares o condenas de prohibición de aproximación/entrada los mismos -e incluso podría activarse un aviso directo a las fuerzas de seguridad- y ello, desde luego, no solo ayudaría en la prevención de delitos de quebrantamiento de medida cautelar o de condena (y otros aparejados a ellos), sino que además facilitaría muchísimo la instrucción de los mismos en caso de cometerse.

Finalmente, asimismo, y entre otras muchas utilidades, la tecnología de reconocimiento facial podría ser empleada por los médicos forenses para llevar a cabo la identificación de cadáveres mediante técnicas de superposición craneofacial, lo cual podría resultar de gran ayuda para identificar víctimas, por ejemplo, en aquellos casos

[12] Entre otras, véase la noticia publicada en La Vanguardia el 25 de mayo de 2022. "*Freno a Clearview AI: no podrá vender retratos de ciudadanos británicos de su base de datos*". Última visita 25 de marzo de 2023.
https://www.lavanguardia.com/tecnologia/actualidad/20220525/8288861/golpe-realidad-clearview-ai-podra-extraer-vender-rostros-britanicos-pmv.html
Y, asimismo, la noticia publicada en The New York Times el 20 de enero de 2020. "*La compañía misteriosa que podría acabar con la privacidad que conocemos*."
https://www.nytimes.com/es/2020/01/20/espanol/negocios/clearview-reconocimiento-facial.html

[13]Véase la noticia publicada en The Wall Street Journal el 7 de febrero de 2018. "*Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal*". Última visita el 22 de marzo de 2023.
https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353

más complejos.

B.2.1.2. Reconocimiento de voz

A modo de concepto, puede decirse que el reconocimiento de voz es aquella tecnología que permite, a través de la IA, identificar a personas o comprobar/verificar su identidad a través de su habla.

En relación con sus potenciales utilidades, el uso de un buen sistema de IA de reconocimiento de voz podría ayudar, entre otras, a identificar a individuos desconocidos que mantienen conversaciones en el transcurso de una conversación telefónica judicialmente intervenida, por ejemplo; y, asimismo, a verificar si la voz de una grabación corresponde o no a una determinada persona relevante para la investigación (por ejemplo, el presunto autor de unas amenazas).

B.2.1.3. Reconocimiento de emociones

A modo de concepto, puede decirse que el reconocimiento de emociones es aquella tecnología que permite, a través de la IA, detectar ciertos sentimientos, intenciones o estados de ánimo.

Dichos sistemas, por lo general, y con el fin de obtener una mayor efectividad, combinan el análisis del rostro y de la voz de las personas y son capaces de detectar microexpresiones y giros o matices vocales prácticamente imperceptibles para los humanos.

En relación con sus potenciales utilidades, el uso de un buen sistema de IA de reconocimiento de emociones podría ayudar, entre otras, a detectar con alta precisión si una persona está diciendo la verdad o no al prestar declaración.

Asimismo, existen sistemas denominados "detectores de agresiones", que, sobre la base de que el 90% de las agresiones físicas van precedidas de un incremento de estrés facial y agresividad verbal, identifican a través de la imagen y la voz, principalmente, aquellos casos en que va a producirse un ataque físico y hacen saltar un aviso de forma inmediata con la policía. Y algunos de tales sistemas han venido siendo instalados en centros educativos estadounidenses, por ejemplo, para detectar agresiones y ataques principalmente a través de la voz[14], si bien estos, por el momento, no cuenta con buenas referencias y valoraciones, habida cuenta de que todavía les queda mucho camino por recorrer para alcanzar niveles de precisión aceptables (y, además, ponen en entredicho la privacidad, tal y como ya puso de manifiesto la agencia ProPublica en una investigación que hizo en el año 2019).[15]

[14] Véase noticia publicada en El Español el 29 de junio de 2019. "*Detectores de agresiones en las escuelas de EE.UU, ¿la solución a la violencia?*" Última visita el 15 de marzo de 2023. https://www.elespanol.com/omicrono/tecnologia/20190629/detectores-agresiones-escuelas-eeuu-solucion-violencia/409959757_0.html

[15] Véase el artículo publicado por Jack Gillum y Jeff Kao, de ProPublica, el 25 de junio de 2019. *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students* https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/ Última visita el 16 de marzo de 2023.

B.2.1.4. Reconocimiento de huellas dactilares y ADN

Hoy en día, las técnicas de análisis de huellas dactilares y ADN son, sin duda, las que arrojan mejores y más infalibles resultados a la hora de proceder a identificar a personas o verificar/comprobar su identidad. Y ello se hace ya con programas que permiten un análisis de datos automatizado, lo cual resulta de gran ayuda a los técnicos humanos, que ven reducida su tarea a un momento final, cuando ya quedan solo unos pocos candidatos para analizar, una vez ya hecho un filtro previo muy útil por "la máquina".

A modo de concepto, puede decirse, por un lado, que el reconocimiento de huellas dactilares es aquella tecnología que permite, a través de la IA, identificar a personas o comprobar/verificar su identidad a partir del análisis de las formas de las crestas papilares de sus dedos y sus proporciones; y, por otro lado, que el reconocimiento de ADN es aquella tecnología que permite, a través de la IA, identificar asimismo a personas o comprobar/verificar su identidad, en este caso, a partir del análisis de los genomas humanos.

En relación con sus potenciales utilidades, el uso de un buen sistema de IA de reconocimiento de huellas dactilares y ADN podría ayudar, principalmente, a tener acceso a ingentes cantidades de datos y automatizar su análisis, con posibilidad incluso de tomar decisiones finales (que en mi opinión, deberían siempre resultar supervisadas por un humano) y, por tanto, incrementar la eficiencia de las búsquedas e identificaciones de presuntos delincuentes, víctimas, testigos, cadáveres y personas desaparecidas en las causas penales, y facilitar las tareas periciales en los casos más complejos.

B.2.1.5. Reconocimiento de firma y de escritura

A modo de concepto, puede decirse que el reconocimiento de firma y escritura es aquella tecnología que permite, a través de la IA, identificar a personas o comprobar/verificar su identidad mediante el análisis de símbolos y/o signos manuscritos, plasmados en un soporte o bien físico o bien digital.

En relación con sus potenciales utilidades, el uso de un buen sistema de IA de reconocimiento de firma y escritura, sin duda, podría servir para automatizar y, por tanto, incrementar la eficiencia de los actuales análisis de la escritura manuscrita y las firmas que resulten de interés en las causas penales, siendo que hoy en día se depende de la práctica de pruebas periciales que suelen demorarse en el tiempo (y, sin embargo, este tipo de sistemas arrojan resultados en cuestión de minutos) y, además, pueden suponer una considerable reducción de los costes asociados.

B.2.2. Herramientas que emplean técnicas de Procesamiento del Lenguaje Natural (PLN)

Las técnicas de PLN tienen por objeto traducir el lenguaje humano (tanto hablado como escrito) a un lenguaje que "la máquina" (o, de modo más concreto, el algoritmo) pueda comprender.

B.2.2.1. Chatbots

A modo de concepto, un "*chatbot*" es una herramienta que tiene por objeto mantener una conversación "*on line*" humano-máquina de forma oral, escrita, o con combinación de ambas (dependiendo de los distintos canales de entrada y salida de información), mediante técnicas de PLN.

Dentro de esta clase de sistemas, especial interés para fines de investigación criminal revisten los denominados *chatbots* cognitivos o "*Smart chatbots*", que emplean IA (en concreto, "*Machine Learning*") para comprender el lenguaje natural mediante las referidas técnicas de PLN, con potencial incluso para ejecutar órdenes, habladas o escritas.

En relación con sus potenciales utilidades, el uso de un buen *chatbot*, sin duda, podría servir para asistir a potenciales víctimas en peligro y testigos de delitos flagrantes, por ejemplo, a entablar contacto directo e inmediato con la policía, simplemente mediante la pulsación de un botón o la pronunciación de una palabra clave que daría al *chatbot* la orden de contactar con las fuerzas de seguridad y emitir determinados mensajes (con la respectiva geolocalización), reduciendo así al máximo la posibilidad de ser descubierta/o por los eventuales autores de los hechos. E, incluso, podría ir recopilando información a tiempo real mediante un sistema de preguntas y respuestas automáticas con tales interlocutores, lo cual podría arrojar a la policía todos los datos necesarios para hacer su actuación lo más eficiente posible.

Asimismo, resulta interesante hacer referencia a Sweetie[16], un *chatbot* con apariencia de niña filipina -menor de edad-, creado por la organización Terre des Hommes en 2013, con el fin de captar posibles pedófilos que siguieran sus conversaciones *on line* de índole sexual.[17] Ello, no obstante, entiendo que no resultaría jurídicamente viable en nuestro país, siendo que se hallan prohibidas las investigaciones prospectivas.

B.2.2.2. Sistemas de análisis de textos/documentos

A modo de concepto, los sistemas de análisis textual/documental son aquellas herramientas que permiten, mediante la IA, analizar y procesar la información contenida en formatos de texto.

En tal sentido, por un lado, resulta interesante hacer referencia a la enorme utilidad que podrían tener este tipo de herramientas para filtrar, ordenar y clasificar documentos de una causa policial y/o judicial, según las necesidades de la autoridad que las empleara, permitiéndole realizar búsquedas y filtros de información concreta y/o relacionada en cuestión de segundos, lo cual aportaría gran valor, especialmente, en las denominadas macrocausas.

En relación con ello, particularmente paradigmático en el ámbito judicial es el conocido como "caso Rolls Royce", en el que se empleó por primera vez en la (entonces) Unión Europea un sistema de IA para analizar ingentes cantidades de documentos en un

[16] En la actualidad ya existe la versión Sweetie 2.0.
[17] Véase noticia publicada en el portal web de la BBC el 22 de diciembre de 2017 "*Sweetie: 'Girl' chatbot targets thousands of paedophiles*". Última visita el 24 de marzo de 2023. https://www.bbc.com/news/av/technology-42461065

caso judicializado. Y es que en tal asunto, en concreto, se empleó el sistema Axcelerate (de OpenText), que con el uso de IA -con técnicas de PLN, a través de "*Machine Learning*"- logró analizar alrededor de 30 millones de documentos, de forma 2.000 veces más rápida que un ser humano y con una reducción de coste del 80%.[18]

Como consecuencia de tal éxito, a partir de ese momento el referido sistema empezó a ser empleado por la Oficina Antifraude inglesa - Serious Fraud Office (SFO)- como apoyo para sus investigaciones.[19]

Y, por otro lado, resulta asimismo interesante hacer mención a la utilidad que podrían reportar este tipo de sistemas para el análisis de texos concretos y, por ejemplo, para la eventual detección de denuncias falsas.

En relación con ello, particularmente interesante es, entre otras, la herramienta VeriPol, creada por la Policía Nacional con el fin de determinar si una denuncia por robo con violencia o intimidación es real o falsa, habiendo llegado a alcanzar un nivel de precisión de más del 90% (frente al 75% alcanzado por los agentes humanos expertos, según el Ministerio del Interior),[20] lo cual, sin duda, puede resultar de enorme utilidad no solo para detectar la posible comisión de delitos de denuncia falsa, sino también para evitar el uso de recursos policiales y, eventualmente, judiciales, de modo innecesario.

B.2.2.3. Sistemas de detección y, en su caso, moderación de contenido on line

A modo de concepto, los sistemas de análisis de contenido *on line* son aquellas herramientas que permiten, mediante la IA, analizar y procesar la información que se halla en Internet y, en su caso, filtrar y limitar su contenido -especialmente en aquellos casos en que puede resultar delictivo-.

En relación con ello, procede poner de manifiesto que, por ejemplo, los autores de los tiroteos ocurridos en la mezquita en Christchurch (Nueva Zelanda) el 15 de marzo de 2019, y en la sinagoga de Poway (California, EEUU) el 27 de abril de 2019, realizaron publicaciones en Internet antes de cometer sus ataques terroristas, y ello ocurre en múltiples ocasiones con carácter previo a la comisión de ciertos delitos.

Así, con un sistema de PLN potente se podría, sin duda, por ejemplo, identificar el incremento de los niveles de amenaza de una determinada persona o de un concreto colectivo y tomar decisiones preventivas para intentar evitar futuras actuaciones criminales.

[18] Véase noticia publicada en el portal web de la SFO (Serious Fraud Office) del Gobierno de Reino Unido el 10 de abril de 2018. "*AI powered «Robo-Lawyer» helps step up the SFO's fight against economic crime*." https://www.sfo.gov.uk/2018/04/10/ai-powered-robo-lawyer-helps-step-up-the-sfos-fightagainst-economic-crime/

[19] Véase noticia publicada en el portal web de la BBC el 4 de septiembre de 2018 "*A digital game or a powerful weapon against boardroom crime?*". Última visita el 20 de marzo de 2023. https://www.bbc.com/news/uk-45399995

[20] Véase noticia publicada en El Mundo el 27 de octubre de 2018. "*VeriPol, así sabe la Policía si tu denuncia es falsa*". Última visita el 23 de marzo de 2023. https://www.elmundo.es/espana/2018/10/27/5bd42db7e2704e27608b466e.html

B.2.3. Análisis de imágenes

El reconocimiento de imágenes es aquella aplicación de IA que permite examinar ciertas figuras y/o símbolos estáticos o dinámicos y reconocer la información contenida en ellos.

En relación con su potencial utilidad para fines de investigación criminal, es interesante hacer referencia a la existencia de empresas que ya están desarrollando programas para la investigación crímenes de guerra a través de sistemas de IA que analizan imágenes contenidas en vídeos y fotografías, a los efectos de preconstituir prueba para presentar ante la Corte Penal Internacional.[21]

Asimismo, igualmente interesante es saber que las grandes empresas tecnológicas (Facebook, Youtube, etc…) ya cuentan con sistemas de IA capaces de detectar y reconocer imágenes sensibles que puedan albergar contenido delictivo, siendo la consecuencia inmediata la de bloquear las cuentas que las suben a la red y/o las comparten y reportar tales hechos a las fuerzas de seguridad.

Finalmente es importante hacer especial mención a los sistemas de IA que tienen por finalidad la identificación de matrículas (en inglés "*Automated Number Plate Recognition*" -ANPR-) mediante el uso de técnicas de Reconocimiento Óptico de Caracteres (ROC).

Tal tecnología, empleada por muchos cuerpos policiales de alrededor del mundo, entre otros la Guardia Urbana de Barcelona, permite, mediante el uso de cámaras instaladas en los coches patrulla, detectar aquellas matrículas que constan en sus bases de datos por pertenecer a un vehículo robado, tener alguna incidencia administrativa, haber estado implicadas en la comisión de algún delito, etc.[22]

c) Herramientas de tramitación -breve apunte-

Para conseguir lograr incrementar la eficiencia en el proceso de instrucción y, por ende, mejorar la calidad del servicio prestado a los ciudadanos por la Administración de Justicia, es evidente que no basta solo con introducir cambios en el modo de practicar las diligencias de investigación y su contenido, puesto que si tales avances no van unidos, en paralelo, con una transformación del modo de tramitar las causas que permita dar celeridad a la gestión de los expedientes, sus efectos no tendrían el impacto que se pretende (y que se espera).

En relación con ello, es interesante poner de manifiesto que hoy en día, sin duda, la IA ya cuenta con un nivel de sofisticación bastante como para permitir la creación de programas o sistemas que analicen demandas/denuncias/querellas, determinen la jurisdicción y la competencia territorial, objetiva y funcional, verifiquen si estas están o no debidamente presentadas, detecten la eventual solicitud de medidas cautelares, comprueben la existencia de otrosíes, etc y, posteriormente, si es necesario, requieran de subsanación, den cuenta al/la Letrado/a de la Administración de Justicia (LAJ) o al/la

[21] Entre otras, la ONG estadounidense Benetech y la organización Syrian Archive.

[22] Véase noticia publicada en el portal web del Ajuntament de Barcelona el 7 de febrero de 2019. "*El nuevo sistema de reconocimiento automático de placas de matrícula de la Guardia Urbana.*" Última visita el 12 de marzo de 2023.
https://ajuntament.barcelona.cat/imi/es/noticia/el-nuevo-sistema

juez, o directamente procedan a su admisión/inadmisión y ulterior tramitación, a la ejecución de órdenes habladas o escritas, etc.

Y ello, sin duda, resultaría de enorme utilidad como herramienta de auxilio en nuestros juzgados y tribunales, donde la tramitación de las causas en no pocas ocasiones resulta paralizada por problemas estructurales y coyunturales que afectan a las plantillas de funcionarios, que a pesar de su profesionalidad, a veces se ven sobrepasados por la excesiva carga de trabajo existente y la falta de personal (al igual que sucede con los/as LAJs y jueces/zas), lo cual no solo da lugar a un incremento de la angustia de los ciudadanos, que tienen que pasar por largos procesos judiciales, con la carga emocional (y muchas veces económica) que ello implica, sino que también da lugar a otras consecuencias poco deseables tales como la ulterior rebaja de las penas impuestas a los autores de hechos delictivos (en ocasiones graves), por la necesidad de apreciar la atenuante de dilaciones indebidas, y ello es absolutamente inadmisible.

En tal sentido, especialmente interesante es la herramienta PROMETEA, que fue introducida en el año 2017 en el Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires (y hoy en día ya está funcionando en otras provincias argentinas, y está en marcha su implementación en la Corte Interamericana de Derechos Humanos y en la Corte Constitucional de Colombia), y permite, a través de *Machine Learning*, tramitar y gestionar expedientes de la Fiscalía y, entre otras tareas, llevar a cabo un control de los plazos, establecer qué soluciones deben darse a según la problemática de cada caso a través del análisis del histórico de supuestos similares, automatizar datos y documentos, ordenar y sistematizar información, etc.

Potenciales riesgos

Una vez expuestos los posibles beneficios que las antedichas herramientas de IA podrían reportar en la investigación criminal, resulta necesario, en un ejercicio de responsabilidad, hacer especial referencia a algunos de los principales potenciales riesgos más comunes de todas ellas y, en concreto, a cuatro de ellos.

En primer lugar, procede hacer alusión a la posible falta de precisión y potencial discriminatorio de los sistemas de IA.

Respecto de ello, queda todavía un largo camino por recorrer, especialmente en relación con la potencia informática de los sistemas y, sobre todo, con la calidad de los datos que se emplean para entrenarlos.

En cuanto a este segundo aspecto, procede advertir que, como ya se ha dicho en páginas anteriores, los sistemas de IA principalmente se nutren de datos, de ingentes cantidades de datos, que son necesarios para poder entrenar a los algoritmos y conseguir así que vayan aprendiendo y mejorando con el tiempo.

Así, por ejemplo, en el caso de las herramientas de predicción y evaluación de riesgos empleadas por parte de la policía, existe el riesgo de un uso de información contenida en bases de datos policiales creadas durante una época en la que se empleaban los denominados métodos "sucios" o poco controlados, la conocida como la época de la "*dirty police*" y que, por ende, suele ser de mala/baja calidad, lo cual podría comportar resultados asimismo de calidad escasa y, lo peor, podría conllevar la perpetuación de

patrones poco deseables. No obstante, actualmente se está tomando conciencia al respecto y ya se están empezando a tomar medidas para evitar el referido peligro (por ejemplo, en el sistema HART, empleado por la policía de Reino Unido, se han eliminado los códigos postales del formulario de evaluación de riesgos, para evitar así potenciales discriminaciones por razón de la zona geográfica donde reside cada individuo.

En segundo lugar, procede hacer alusión a la posible vulneración del derecho a la privacidad y a la protección de datos personales.

Y es que, aunque parezca mentira, en no pocas ocasiones se dejan de lado estos derechos cuando se trata del uso de sistemas de IA, lo cual es altamente peligroso, puesto que las consecuencias de una transgresión en tal sentido podrían conllevar consecuencias absolutamente irreparables para las personas afectadas.

En relación con ello, resulta interesante traer a colación la definición de tratamiento de datos de carácter personal establecida en la legislación, que debe servir como guía, sin duda, para abordar esta cuestión. Así, el artículo 4 del RGPD, en consonancia con el artículo 5 de la 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, dispone que el tratamiento de datos de carácter personal implica cualquier operación o conjunto de operaciones realizadas sobre los mismos, ya sea por procedimientos automatizados o no, tales como "*la recogida, registro, organización, estructu- ración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*", debiendo ello ser puesto en relación, asimismo, con lo establecido en el artículo 18 de la Constitución Española y en la LO Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

En tercer lugar, procede hacer alusión a la posible existencia de brechas de seguridad en los sistemas.

Y es que la información que se maneja en la investigación criminal es altamente sensible y, asimismo, la IA es una tecnología muy vulnerable a ciberataques y otras filtraciones de información no deseadas, por lo que resulta importantísimo poner el foco en la seguridad, habida cuenta de que las fatales consecuencias que, en caso de quiebros en la misma, podrían producirse, resultarían asimismo irreversibles (especialmente en caso de emplear datos biométricos, habida cuenta de que, si se "roba" una contraseña o la numeración de una tarjeta de crédito, por ejemplo, esta puede modificarse, pero en caso de que se "roben" tales datos la solución no es tan evidente).

Y, finalmente, procede hacer alusión a la posible falta de transparencia.

Y es que en materia de IA, considero que la transparencia es el eje en torno al que todo gira, habida cuenta de que resulta absolutamente imposible verificar la calidad de los sistemas (si vulneran o no derechos fundamentales, cuál es la naturaleza de los datos empleados, qué niveles de precisión se manejan, etc.), si estos no son transparentes.

Así, resulta fundamental exigir la transparencia y la explicabilidad de los sistemas de IA, especialmente porque para que sus resultados pudieran tener eficacia probatoria en el proceso judicial, estos deberían poder ser sometidos a contradicción (real)tanto en fase de instrucción como, sobre todo, en fase de plenario, con todas las garantías, y eso únicamente podría conseguirse en caso de que estos fueran totalmente transparentes y accesibles.

En relación con ello, me gustaría realizar una breve reflexión que creo que es importante. Y es que hoy en día no hay mayor caja negra o *black box* que la del cerebro del juez, puesto que actualmente es imposible conocer cuáles han sido las verdaderas motivaciones que lo/la han llevado a tomar una determinada decisión, por muy bien jurídicamente argumentada que esté. No obstante, tal hecho, invariable y patente, no puede servir de pretexto y justificación para permitir la falta de transparencia y explicabilidad de los sistemas de IA, y la existencia de cajas negras en los mismos, principalmente porque la incidencia y la repercusión que puede tener la decisión de un juez sobre los ciudadanos es absolutamente limitada, en comparación con la que puede tener, multiplicada de forma exponencial, el resultado arrojado por un algoritmo empleado, por ejemplo, por todos los jueces de España.

3.- CONCLUSIONES

Margarethe Vestager, Vicepresidenta de la Comisión Europea (2019-2024), en febrero del año 2020, al presentar la Estrategia Europea de datos y las Opciones estratégicas destinadas a garantizar un desarrollo de la IA centrado en el ser humano, manifestó: "*La IA no es buena ni mala en sí misma, todo depende de por qué y cómo es utilizada*".

Y ello, desde luego, podría resultar el perfecto resumen de todo lo expuesto a lo largo de estas páginas, habida cuenta de que, como se ha reiterado en diversas ocasiones, la IA es una tecnología que puede reportar enormes beneficios, especialmente en el ámbito de la justicia penal, pero que a su vez puede ocasionar desmedidos peligros que conviene intentar evitar en aras de garantizar su uso en beneficio de los seres humanos, lo cual solo puede conseguirse a través de la legislación.

Desde luego, entiendo que legislar sobre un fenómeno tan complejo como la IA no es tarea fácil, y menos cuando se trata de autorizar su uso para fines de investigación criminal, y por ello considero que los poderes legislativos deberían estar asesorados en tal tarea de forma transversal por los más prestigiosos y brillantes expertos en materia de IA, de protección de datos personales, de ciberseguridad y de Derecho Penal y Procesal Penal, en este caso, puesto que hay muchísimos derechos fundamentales en juego y es evidente que no todo lo técnicamente posible es (o debería ser) jurídicamente viable.

No obstante, en todo caso, entiendo que debería ponerse el foco en evitar el que, bajo mi punto de vista, es el peor de los peligros al que nos enfrentamos al autorizar el uso de los sistemas de IA en la justicia: el de su deshumanización.

Y es que la mayoría de las personas que acuden a una comisaría de policía o a un juzgado se hallan en situaciones de enorme vulnerabilidad y acuden con historias cargadas de miedos, confidencias y matices imposibles de gestionar, con la empatía y el calor que requieren, por una máquina. Y ello aunque tengamos a nuestro alcance los más sofisticados y potentes sistemas de IA, ya que nada jamás podrá sustituir el contacto

humano, y eso es lo que entiendo que no debe perderse de vista, ya que es lo que nos define como especie y lo que nos va a permitir preservar nuestra dignidad en cualquier escenario.

Así, sin duda, los juristas tenemos un enorme reto por delante y, desde luego, una inmensa responsabilidad, ya que debemos estar a la altura de las necesidades que se plantean en este gran momento histórico, con el fin de intentar sentar las bases de nuestra evolución como especie conviviendo con un fenómeno tan extraordinario pero a la vez tan peligroso como es la IA.