GRADO EN DERECHO

AÑO 2023/2024

Inteligencia artificial aplicada a la resolución de controversias:

EL PAPEL CRUCIAL DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL.

Especial mención a los sistemas de predicción y valoración del riesgo, así como a los sistemas que utilizan datos biométricos; en específico, los de reconocimiento facial.

TRABAJO REALIZADO POR:

MARTA MONTALBÁN AGUINACO

DIRIGIDO POR:

ALBERTO SAIZ GARITAONANDIA

EL PAPEL CRUCIAL DE LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL

ÍNDICE

1. INTRODUCCIÓN

1.1. CONTEXTUALIZACIÓN DEL TEMA

Indudablemente, en la actualidad, la incorporación de la tecnología se erige como una necesidad imperante tanto en nuestra esfera cotidiana como en el ámbito profesional. En este sentido, el campo del derecho no escapa a esta realidad, ya que la tecnología emerge como una herramienta esencial para facilitar y agilizar las labores de todos los juristas. Si bien es cierto que gran parte de las funciones requeridas en este campo demandan un enfoque personalizado y se vinculan estrechamente con la facultad de razonamiento humano, existen numerosas tareas que podrían ser eficazmente gestionadas con el apoyo de sistemas automatizados. La incorporación de tecnología en estas áreas podría significativamente aliviar la carga laboral de los profesionales, permitiéndoles enfocarse en actividades de mayor relevancia.

En el contexto de un mundo en constante desarrollo tecnológico, hemos sido testigos de un asombroso y continuo avance en la adopción de nuevas tecnologías, destacándose especialmente la inteligencia artificial, en adelante IA. Esta última ha ido ganando progresivamente terreno en nuestras vidas y se vislumbra como una herramienta inevitable en el largo plazo. De hecho, su presencia ya es palpable en numerosos aspectos de nuestra rutina diaria, desde el desbloqueo facial de nuestros dispositivos móviles hasta la utilización de sistemas de navegación GPS para llegar a destinos específicos, entre otros ejemplos. Y es que esa inteligencia artificial, que antes sólo concebíamos como una fantasía de películas de ciencia ficción, ha dejado de ser una ilusión para transformarse en una realidad tangible. Si bien es cierto que estos sistemas no están exentos de desafíos, es innegable que también poseen numerosas virtudes que podemos aprovechar en nuestro beneficio.

En la actualidad, observamos un creciente uso de tecnologías en el ámbito de la justicia, donde cada día se incorporan nuevas técnicas tecnológicas al quehacer cotidiano de los juristas. La digitalización se ha vuelto omnipresente, con un aumento significativo en la

automatización de procesos. Un ejemplo paradigmático de esta tendencia se evidenció durante la pandemia, cuando las restricciones de movilidad y contacto social obligaron a recurrir exclusivamente a las tecnologías para llevar a cabo las gestiones jurídicas en la Administración de Justicia. El uso de videoconferencias en los tribunales, una práctica que anteriormente habría parecido inverosímil, se convirtió en la norma. A pesar de la eventual relajación de estas medidas, muchas de las prácticas adoptadas durante este período persisten, como lo evidencian los numerosos juicios penales en los que se han presentado testimonios y pericias realizadas a través de medios informáticos, transmitidos mediante videoconferencia durante las audiencias orales.

En consideración de lo anteriormente expuesto, resulta imperativo llevar a cabo un análisis detallado de las diversas alternativas que la inteligencia artificial podría brindar en el ámbito de la justicia, especialmente durante el proceso penal, específicamente en la fase de instrucción de un caso. Con este propósito, procederemos a examinar el tipo de herramientas que esta tecnología podría proveer para asistir en la investigación de un delito, al mismo tiempo que evaluaremos los desafíos más prominentes que podríamos enfrentar al emplearla en este contexto.

Dada la limitación de espacio para este trabajo, nos enfocaremos en las herramientas de predicción y evaluación de riesgos, así como en aquellas que emplean datos biométricos, particularmente aquellas basadas en el reconocimiento facial, con el objetivo de prevenir e investigar posibles delitos e identificar a los responsables. A continuación, examinaremos la legislación europea relevante sobre el uso de estos sistemas, teniendo en cuenta que se trata de un campo emergente que aún carece de una regulación tan completa como la que podría tener una materia más establecida.

Hemos optado por focalizarnos en este aspecto debido a la relevancia que tiene en la era actual explorar las potenciales utilidades de los sistemas de inteligencia artificial. Nos encontramos continuamente rodeados de cámaras, y, queramos o no, estamos bajo constante vigilancia, ya sea por las cámaras de seguridad en los establecimientos que visitamos, por las cámaras ubicadas en espacios públicos o, incluso, por las cámaras de nuestros propios dispositivos móviles, con las que a menudo capturamos imágenes de nuestro entorno.

Es cierto que en muchas ocasiones estos sistemas pueden suponer una amenaza para ciertos derechos como puede ser el derecho a la privacidad. No obstante, en el contexto de este trabajo, examinaremos cómo, en realidad, estos sistemas pueden contribuir en numerosas ocasiones a la resolución de delitos penales.

Además, hemos optado por centrarnos en el proceso de instrucción penal debido a nuestra experiencia en este ámbito, donde hemos podido constatar la importancia de mejorar dicho proceso. En nuestra humilde opinión, el sistema de justicia penal (y probablemente otros ámbitos) adolece de numerosas carencias, especialmente en España, donde se caracteriza por su lentitud y la escasez de recursos humanos y materiales necesarios para llevar a cabo las tareas requeridas. No es raro que un acusado deba esperar hasta cuatro años para ser juzgado, lo cual ilustra la gran problemática que enfrentamos en el país en relación con el proceso penal. Por tanto, cualquier método o sistema que pueda contribuir a mejorar el funcionamiento de este proceso es siempre bienvenido. No obstante, es imperativo salvaguardar los derechos de los ciudadanos, lo que implica buscar un equilibrio entre la implementación de sistemas inteligentes y la protección de los derechos individuales.

1.2. OBJETIVOS DEL TRABAJO

El propósito de este trabajo es examinar los beneficios e inconvenientes que podrían surgir al implementar la inteligencia artificial en la investigación de procesos penales. Se busca determinar si el uso de estas herramientas tecnológicas sería útil para investigar un crimen o si, por el contrario, los inconvenientes asociados con esta tecnología podrían generar más problemas que soluciones.

Para ello, examinaremos no sólo qué es la inteligencia artificial y su crecimiento constante en nuestra sociedad, sino también qué tipos de tecnologías podrían ser utilizadas en un proceso penal y qué tipo de ayuda podrían proporcionarnos en nuestra labor diaria. Si bien es cierto que no es factible analizar todas las posibles herramientas de inteligencia artificial, nos centraremos en aquellas utilizadas para evaluar el riesgo de un ciudadano, así como en aquellas que emplean datos biométricos, específicamente el reconocimiento facial, con el fin de prevenir o investigar delitos.

Además, analizaremos la nueva legislación europea sobre IA y la relacionaremos directamente con el uso de estos sistemas que explicaremos más adelante. Debemos tener en cuenta en todo momento que es una materia muy novedosa y que, por lo tanto, carece de una regulación tan concreta, por ello hay que recurrir a este Reglamento aprobado recientemente, y el cual es el primero que regula la IA en una Ley concreta para ello.

Examinaremos también los importantes riesgos asociados, cómo los sesgos inherentes a este tipo de máquinas o la falta de transparencia o explicabilidad. Esto es crucial, ya que no es lo mismo ser juzgado o investigado por un ser humano que por una máquina. Además, analizaremos los derechos fundamentales que están en riesgo al utilizar estos métodos inteligentes.

La metodología de este trabajo ha consistido en una revisión bibliográfica de libros y artículos relacionados con la inteligencia artificial, así como su utilización en los diferentes trámites del proceso penal.

2. FUNDAMENTOS TEÓRICOS

2.1. CONCEPTO DE IA

La inteligencia artificial es un concepto de difícil descripción, pues no existe una definición universal y aceptada por todo el mundo de esta. Dar una única respuesta a qué es la inteligencia artificial es algo imposible hoy día, pues esta misma evoluciona muy deprisa.

La Comisión Europea define la IA como *"sistemas de software (y posiblemente también de hardware) diseñador por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital: percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado. Los sistemas de IA pueden usar reglas*

simbólicas o aprender un modelo numérico. También pueden adaptar su comportamiento al analizar cómo el medio ambiente se ve afectado por sus acciones previas"[1]

Al mismo tiempo la Propuesta del 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, publicada en 21 de abril de 2021, define los sistemas de inteligencia artificial (sistema de IA) en su artículo 3.1 de la siguiente manera: *"el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I - esto es, estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo; estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico); estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización*[2] *- y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa"*[3].

En nuestra opinión, la IA es aquella que se dedica a intentar que las máquinas sean inteligentes, su finalidad es obtener en una máquina la inteligencia que tiene un ser humano, es decir, conseguir que una máquina sea capaz de responder y reflexionar como lo haría un ser humano, para ello se alimenta a este sistema de una base de datos, llamados algoritmos, mediante los cuales se entrena a la misma para dotarlo de los medios

[1] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 24.

[2] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021. Anexos. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

[3] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

suficientes para ser capaz de cómo hemos dicho, tener la inteligencia de una persona, o al menos acercarse a ella.
En cuanto a su relación con la investigación criminal, la IA se entrelaza estrechamente con esta, y a medida que el tiempo avanza, se perfila como una herramienta inevitable que se empleará en diversos grados dentro del ámbito judicial, particularmente en el proceso penal.

En efecto, observamos actualmente la aplicación de tales sistemas en una variedad de funciones y capacidades. Las Fuerzas y Cuerpos de Seguridad del Estado emplean estos recursos para anticipar áreas con mayor riesgo de actividad delictiva, asignando recursos de manera más estratégica en consecuencia[4]. A título de ejemplo, destacan dos herramientas empleadas por las fuerzas policiales: los mapas criminales y las tecnologías de reconocimiento facial[5], esta última explorada con mayor detalle posteriormente.

La integración de la IA en el ámbito legal tiene como principal objetivo aumentar la eficacia y celeridad de los procedimientos judiciales, aliviando así la carga de trabajo del personal administrativo de justicia.

Además de lo mencionado, la inteligencia artificial también ofrece herramientas para analizar grandes volúmenes de datos de manera rápida y precisa, lo que puede ser fundamental en la detección de tendencias delictivas y la identificación de posibles vínculos entre casos aparentemente no relacionados. En resumen, la incorporación de la inteligencia artificial en la investigación criminal no solo promete agilizar los procedimientos, sino también mejorar la calidad y precisión de las investigaciones.

2.2. PRINCIPALES RIESGOS

La irrupción de la IA en el ámbito jurídico ha impulsado indudablemente la creación de un nuevo sistema en el que tenemos que ser capaces de combinar la tecnología con los

[4] AGUINAGA BARTOLOMÉ, A., "La Inteligencia Artificial en el proceso penal. Especial referencia al reconocimiento facial". 2022, p. 7.
[5] ALONSO SALGADO, C, "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", IUS ET SCIENTIA, vol. 7 (2021), pp 25-36

derechos y garantías procesales que son necesarios en el proceso judicial. Y es que, aunque parezca sencillo, el equilibrio de estos dos elementos no es más que problemático si buscamos un proceso justo y garantista.

Al respecto, tendremos que poner de manifiesto los problemas que suscita este tipo de tecnologías, que son, por un lado, la falta de transparencia y explicabilidad de los mismos, así como los sesgos inherentes a estos que conllevan una posible vulneración de los derechos fundamentales de los ciudadanos.

2.2.1. SESGOS

Uno de los principales riesgos de la inteligencia artificial en el ámbito del proceso penal es su propensión para cometer errores, lo que impide que sea una herramienta perfecta y libre de fallos, al menos por el momento y posiblemente de manera indefinida. Sin embargo, este mismo problema se presenta en el ser humano.

Hay que partir de la base de que estas máquinas, si bien son objetivas, parten de un algoritmo que funciona dependiendo de cómo hayan sido entrenados. Pues bien, estos algoritmos son entrenados de acuerdo con unas bases de datos que son creadas por seres humanos[6]. Y es que como bien indica MURILLO FUENTES el algoritmo será el encargado de ajustar el modelo del sistema inteligente con los datos de entrenamiento que disponga, encontrándonos, en este momento, con un obstáculo significativo en relación con la representatividad de la muestra y, desde una perspectiva más técnica, con los eventuales errores que se pueden producir en el etiquetado de estos[7].

Es esencial que los datos que alimentan el sistema sean, en primer lugar, representativos. No podemos pasar por alto que la Inteligencia Artificial se distingue por almacenar y procesar una gran cantidad de datos. Esto quiere decir que estos sistemas tienen la capacidad de procesar y analizar grandes volúmenes de información de manera eficiente. Por ello, es crucial asegurarse de que estos datos mantienen su representatividad con el

[6] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. pp. 4-5. https://doi.org/10.15304/epc.44.8859

[7] MURILLO FUENTES, J.J., ¿"Qué es lo que no funciona en los algoritmos de inteligencia artificial?" en COLOMER HERNÁNDEZ, I. (Dir.), Uso de la información y de los datos personales en los procesos: los cambios en la era digital, Cizur Menor, 2022, pp. 154 y ss.

tiempo. Si esta representatividad se pierde, estaremos perpetuando la falta de representación cada vez que utilicemos este sistema.

Además, es crucial que los datos introducidos en el algoritmo estén correctamente ingresados. Si los datos no son verídicos, el sistema perderá su fiabilidad y, por consiguiente, los resultados obtenidos serán inexactos. La intervención humana es necesaria para la introducción de estos datos, ya que el ser humano debe verificar la exactitud de la información proporcionada a la Inteligencia Artificial. De esta manera, se dota a esta tecnología de una cierta independencia que puede conducir a resultados fiables de manera directa.

Para lograrlo, es evidente que el propio sistema debe poseer capacidades de aprendizaje autónomo. Es imprescindible que esta tarea se realice de manera objetiva, ya que, de lo contrario, si no se siguen parámetros objetivos y específicos al crear la base de datos con la que operará el algoritmo, nos enfrentamos al principal obstáculo de la Inteligencia Artificial: los sesgos[8].

Entendemos el sesgo como "aquella inclinación que favorece o perjudica a una persona, objeto o posición"[9], este representa el mayor de los impedimentos que tienen estos sistemas inteligentes y el mismo compromete gravemente la eficacia y salvaguarda de la tutela judicial efectiva.

Para eludir este problema, tenemos que identificar el origen de este. Sin embargo, coincidimos con BORGES BLAZQUEZ cuando afirma que "los datos van a tener los mismos sesgos y prejuicios que tiene el ser humano que programa la máquina. En otras palabras, las máquinas van a ser racistas, sexistas y clasistas si lo son sus programadores"[10], esto implicaría que el sesgo se reproduzca continuamente cada vez que se aplique este sistema, ya que el sesgo estaría integrado en su funcionamiento intrínseco. Por lo tanto, consideramos que este problema no tiene una solución sencilla, dado que los

[8] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 5. https://doi.org/10.15304/epc.44.8859

[9] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 6. https://doi.org/10.15304/epc.44.8859

[10] BORGES BLÁZQUEZ, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", Revista Ius et Scientia, núm. 2, vol. 6, 2020, pág. 54.

resultados generados por los seres humanos ya incorporan subjetivamente el sesgo de cada juez que ha tomado decisiones en el pasado. Evitar este problema no es algo trivial y requiere precauciones exhaustivas para asegurar que se pueda aplicar sin infringir el derecho al debido proceso de cualquier ciudadano.

Si bien es cierto, que los sesgos no sólo se producen por culpa del programador, estos sesgos también pueden aparecer en diferentes momentos. Por ello, vamos a diferenciar distintos tipos[11] de sesgos algorítmicos.

- Sesgos inteligentes: a través del aprendizaje autónomo del que goza el sistema de inteligencia artificial se crean por la propia herramienta.
- Sesgos humanos: son aquellos que se crean por consecuencia de la intervención humana en la introducción de datos en el sistema, estos son de difícil solución pues la intervención humana es necesaria.
- Sesgos cognoscibles o porcentuales: estos son los que surgen a raíz de no introducir los datos suficientes o que los datos introducidos no tienen la suficiente representatividad necesaria.

Exactamente, los sesgos pueden manifestarse en diversas formas y contextos. Por lo tanto, para mitigar este problema, sería necesario examinar todas las etapas de funcionamiento del sistema de Inteligencia Artificial, ya que en cualquiera de ellas podríamos encontrarnos con este desafío significativo.

En conclusión, los sesgos son un dificultoso asunto de complicada solución, por ello tenemos que prestar una especial atención a cómo entrenamos a los algoritmos que pretendemos utilizar, debido a que el juicio de la IA no es imparcial ni es absolutamente fiable[12]. Por ello coincidimos con MIRÓ LLINARES que la IA que pretendemos aplicar en un futuro tiene que ser creada por equipos de "científicos sociales y juristas capaces

[11] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 7. https://doi.org/10.15304/epc.44.8859

[12] BORGES BLÁZQUEZ, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", Revista Ius et Scientia, núm. 2, vol. 6, 2020, pág. 17.

de establecer tanto los criterios jurídicos y criminológicos de clasificación como de interpretación de resultados"[13].

De esta manera, al menos nos aproximaremos a un sistema inteligente creado por diversos profesionales, lo que contribuiría a que este proceso sea lo más equitativo posible. Aun así, estamos muy lejos de conseguir que una máquina no tenga este gran fallo en su funcionamiento, pero eso no quiere decir que con los avances tecnológicos y la intervención de diferentes profesionales que no solo entrenen al algoritmo, sino que lo revisen cada cierto periodo de tiempo no sea una opción más que viable en un futuro.

2.2.2. TRANSPARENCIA Y EXPLICABILIDAD

Como se ha puesto de manifiesto para que un proceso penal sea garantista con la utilización de sistemas inteligentes, es necesario que los algoritmos que lo componen sean explicables y transparentes, de lo contrario, como ya hemos explicado, pondremos en juego derechos fundamentales de los ciudadanos.

Aunque a primera vista pueda parecer que estos dos conceptos son idénticos y que si tenemos un proceso transparente será consecuentemente explicable, en realidad nos podemos encontrar con un sistema inteligente que sea transparente pero inexplicable. Esto se debe a la imposibilidad de conocer con precisión cómo se ha llegado al resultado al que ha llegado la máquina, a pesar de que este sea transparente y abierto al público.[14] Esto es, como bien dice SÁNCHEZ SÁEZ hay que obligar a los diseñadores y empresas de IA no sólo a enseñar los algoritmos (código fuente) sino explicar cómo se llega a los resultados o información de salida (trazabilidad o cognoscibilidad)[15].

Respecto de cómo debe de ser esta transparencia y explicabilidad, estamos totalmente de acuerdo con CORVALÁN cuando dice que "la IA debe poder explicar en un lenguaje

[13] BORGES BLÁZQUEZ, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", Revista Ius et Scientia, núm. 2, vol. 6, 2020, pág. 17.
[14] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 14. https://doi.org/10.15304/epc.44.8859
[15] SÁNCHEZ SÁEZ, A.J. El posible uso de la inteligencia artificial en el ámbito judicial: el contexto jurídico español y europeo. Especial referencia al contencioso-administrativo. *Rivista Italiana de Informativa e Diritto: periodico internazionale del CNR-IGSG, 2,* 2023, pág. 15.

comprensible para los seres humanos en qué factores se basa y cómo pondera los elementos que la sustenta"[16], si no lo hiciésemos de esta manera estaríamos priorizando la eficiencia del proceso ante las garantías de las partes. Por ello, consideramos necesario que cualquier persona con un nivel medio de inteligencia sea capaz de comprender lo que explica este sistema inteligente.

Por un lado, tendríamos el principio de transparencia, que es aquel que refuerza el principio de publicidad procesal, mediante el cual tenemos la posibilidad de saber cómo funciona el algoritmo, y, por otro lado, el principio de explicabilidad, que es aquel que favorece al conocimiento de la fundamentación jurídica que se ha llevado a cabo para llegar a la sentencia, proporcionando así seguridad jurídica a las partes.[17] Y es que, estamos ante el problema de la caja negra o *black box*, definido como "la incapacidad de comprender completamente el proceso de toma de decisiones de un sistema de IA y la incapacidad de predecir las decisiones o resultados de estos"[18]. De hecho, en la Unión Europea, los sistemas de *deep learning* con cajas negras están prohibidos debido a que obstaculizan la motivación y la transparencia de las resoluciones judiciales. Por ello, cada vez más empresas optan por utilizar algoritmos con "cajas blancas", que, aunque menos potentes, explican todos los pasos seguidos por la máquina para llegar a la solución. Sin duda, en el sistema judicial, estos últimos deberían ser los únicos permitidos[19].

Si se cumpliesen dichos principios podríamos resolver grandes problemas relacionados con la aplicación de estos sistemas inteligentes, como bien menciona CRISTINA SAN MIGUEL CASO "si conocemos cómo funciona el sistema, el derecho a obtener una resolución motivada y el derecho al recurso, no encontrarían mayores problemas"[20] , y coincidimos totalmente con esa afirmación, ya que el fundamento del derecho al debido

---

[16] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 15. https://doi.org/10.15304/epc.44.8859

[17] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 14. https://doi.org/10.15304/epc.44.8859

[18] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 69.

[19] SÁNCHEZ SÁEZ, A.J. El posible uso de la inteligencia artificial en el ámbito judicial: el contexto jurídico español y europeo. Especial referencia al contencioso-administrativo. *Rivista Italiana de Informativa e Diritto: periodico internazionale del CNR-IGSG, 2,* 2023, pág. 16.

[20] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 14. https://doi.org/10.15304/epc.44.8859

proceso, que es inherente a todos los ciudadanos, radica en comprender las razones detrás de las decisiones que nos afectan, incluso si no estamos de acuerdo con ellas.

No obstante, encontramos aquí otro gran problema, como en la mayoría de los casos los algoritmos son propiedad de una empresa privada, y por lo tanto están protegidos por el secreto de empresa, esto nos impide conocer cómo este algoritmo ha obtenido la respuesta en cuestión. Es decir, aquí nos enfrentamos al problema de las "cajas negras" que mencionamos anteriormente. Entonces, nos estamos ante un conflicto de intereses entre el derecho de la empresa (en específico, el secreto de empresa y en materia de propiedad intelectual e industrial) y el derecho de defensa y al debido proceso, y es que el encausado tiene derecho a conocer la fundamentación jurídica detrás de la sentencia, lo que implica estar informado de todos los pasos que condujeron a esa conclusión. Si esto no se cumple, nos enfrentamos a una falta de transparencia y explicabilidad que podría generar indefensión en las partes involucradas[21]. Si bien es cierto que en algunos casos la protección de la propiedad intelectual puede ser compatible con el acceso a los algoritmos, si se da prioridad al interés público de garantizar una justicia objetiva y de calidad. Todo esto debe ser explicado de manera comprensible tanto para los jueces como para los usuarios[22].

Entonces, ¿cómo solucionamos este problema? En nuestra opinión, para abordar este problema, consideramos que a pesar de que en ciertos casos pueda ser compatible el uso de una empresa privada en la que se tenga acceso al algoritmo, en este caso, no deberíamos permitir que empresas privadas gestionen un asunto de carácter público como el derecho penal. El derecho penal concierne a toda la sociedad y, por lo tanto, es de naturaleza eminentemente pública. No podemos permitir que la búsqueda de beneficios empresariales ponga en riesgo derechos fundamentales que pertenecen a todos los seres humanos, ya que esto sería contrario a la ley. Por lo tanto, es crucial que, al utilizar sistemas de inteligencia artificial, se respeten los principios de transparencia y explicabilidad, y, en consecuencia, no se debe permitir que empresas privadas sean

[21] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. pp. 14 y ss. https://doi.org/10.15304/epc.44.8859

[22] SÁNCHEZ SÁEZ, A.J. El posible uso de la inteligencia artificial en el ámbito judicial: el contexto jurídico español y europeo. Especial referencia al contencioso-administrativo. *Rivista Italiana de Informativa e Diritto: periodico internazionale del CNR-IGSG, 2,* 2023, pág. 18.

propietarias de estos algoritmos, al menos en el ámbito penal. Ciertamente, es innegable que en la actualidad el Estado carece de la capacidad para alcanzar los niveles de especialización que caracterizan a una empresa privada dedicada a este ámbito. Sin embargo, sería prudente considerar una colaboración entre ambas entidades, permitiendo que la empresa privada asista al Estado en la implementación de sistemas públicos.

2.2.3. DERECHOS EN JUEGO

La integración de la inteligencia artificial (IA) en el proceso penal plantea desafíos significativos en relación con los derechos fundamentales. Existe un riesgo de que la opacidad y el sesgo algorítmico comprometan derechos fundamentales como la privacidad, la presunción de inocencia y el derecho a un juicio justo, entre otros.

Tal y como hemos mencionado ya, es innegable que la IA está poco a poco perpetrando en nuestra vida diaria, lo cual aporta numerosas ventajas a la sociedad. No obstante, si la empleamos sin restricciones conlleva varios riesgos que pueden impactar directamente en los derechos fundamentales de los ciudadanos. Es por ello por lo que examinaremos qué principios y qué derechos son los que hay que proteger a la hora de aplicar este tipo de inteligencia.

Cuando empleamos máquinas inteligentes, surgen implicaciones directas para varios derechos fundamentales. Por un lado, IA podría ofrecer soluciones a numerosos problemas en el ámbito del proceso penal, especialmente en lo concerniente a su agilidad y eficiencia, aspectos en los que el sistema judicial suele mostrar deficiencias. Sin embargo, es crucial garantizar que los ciudadanos sean sometidos a un proceso legal que respete plenamente sus derechos, y es por ello por lo que estamos totalmente de acuerdo con lo que dice CRISTINA SAN MIGUEL[23] de que debemos primar las garantías y

[23] SAN MIGUEL CASO, C., “Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal”. *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 8. https://doi.org/10.15304/epc.44.8859

derechos de las partes a la luz de todos los obstáculos intrínsecos a los sistemas inteligentes.

Ante esta nueva realidad tecnológica encontramos dos escenarios procesales diferentes: por un lado, que se utilice esta inteligencia como una herramienta asistencial en la labor del juez - es el caso que nos concierne en este trabajo- y, por otro lado, la plena sustitución del juez insertando un juez robot que toma la decisión judicial. Nos vamos a centrar en la aplicación de estos sistemas como meros ayudantes en el proceso penal ya que es hoy en día una realidad que se utilizan sistemas de este tipo.[24]

Por lo tanto, al utilizar estos sistemas de manera instrumental, no debemos olvidar que la justicia tiene que ser debidamente aplicada en el ordenamiento jurídico. Lo que queremos decir con esto es que el carácter complementario de estas herramientas tiene una gran incidencia en la manera en que se va a motivar o la forma que va a tener la resolución judicial. Por tanto, es esencial recordar el artículo 120.3 de la Constitución Española, que resalta la importancia de la motivación de las sentencias. Desde nuestra perspectiva, sería beneficioso utilizar esta tecnología como un complemento al trabajo del juez, siempre y cuando las decisiones se fundamenten y expliquen de manera clara y detallada. No sería suficiente justificar una resolución basándose únicamente en los resultados de un sistema de IA; más bien, el juez debería emplear dichos resultados como una herramienta auxiliar en el proceso de toma de decisiones, explicando de manera transparente el razonamiento detrás de la sentencia final. Y es que, de no ser así, se vulneraría ciertos derechos fundamentales y como afirma BARONA VILAR hay que "equilibrar las tecnologías con los derechos fundamentales de los ciudadanos[25]".

Los derechos en juego al aplicar inteligencia artificial en el proceso penal son diversos y abarcan una amplia gama. Desde el derecho a la tutela judicial efectiva, que podría verse comprometido si una persona no puede alegar su derecho de defensa debido a la falta de transparencia en el proceso de toma de decisiones, hasta el principio de libertad religiosa,

[24] SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. p. 10. https://doi.org/10.15304/epc.44.8859

[25] BARONA VILAR, S.: "Inteligencia artificial o a la algoritmización de la vida y de la justicia: ¿solución o problema?". Revista Boliviana de Derecho, Núm. 28 (2019), pp. 18-49.

que podría verse afectado por la instalación de cámaras de videovigilancia fuera de un lugar de culto. Incluso si la finalidad no es vigilar la asistencia a dicho lugar de culto, la grabación continua podría implicar una intrusión en la privacidad de quienes acuden allí.

Efectivamente, el amplio espectro de aplicaciones de las tecnologías biométricas, especialmente el reconocimiento facial, en el que luego nos centraremos, tiene el potencial de influir en prácticamente todos los derechos fundamentales de los individuos. Entre otros, el FRA menciona los siguientes: "la dignidad humana, al respeto de la vida privada, la protección de datos personales, la no discriminación, los derechos del niño y de los mayores, los derechos de las personas con discapacidad, la libertad de reunión y asociación, la libertad de expresión, el derecho a una buena administración, y el derecho a un recurso efectivo ante la ley y a un juicio justo"[26].

El uso de sistemas biométricos, como el reconocimiento facial, impacta en los derechos fundamentales y la dignidad humana al cosificar a las personas y debilitar su anonimato. Esto genera un efecto amedrentador al ser usado para recoger datos en espacios públicos y compararlos con bases de datos policiales, tratando a todas las personas como sospechosas potenciales y afectando su comportamiento y confort en la sociedad.

Bajo esta perspectiva colectiva, es esencial considerar el impacto en principios fundamentales como el democrático y la seguridad jurídica. La mera existencia de estos sistemas puede coartar la participación en la vida social y cultural, afectando el ejercicio de libertades como la de expresión, reunión, asociación y circulación. Esto podría inducir una sensación de vigilancia constante y disuadir el ejercicio de estos derechos fundamentales[27].

En resumen, emplear estos sistemas inteligentes en el proceso penal radica en el riesgo de vulnerar derechos todo tipo de derechos. Esto es porque estos sistemas pueden estar sesgados además de tener otros riesgos ya explicados, normalmente serán

[26] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 13.
[27] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, págs 13 y 14.

discriminaciones indirectas, no voluntarias, producida por manejar datos no representativos, asimismo, en lo que respecta al reconocimiento facial, implica una vigilancia constante que restringe nuestras actividades cotidianas. Por tanto, su implementación requiere un cuidadoso equilibrio entre la eficiencia y la protección de los derechos individuales.

3. LA INTELIGENCIA ARTIFICIAL EN EL PROCESO PENAL

3.1. HERRAMIENTAS DE IA PARA INVESTIGAR DELITOS

Por consiguiente, nos adentramos en el núcleo de la investigación, explorando las diversas herramientas disponibles para abordar delitos. Aunque existen numerosas aplicaciones de inteligencia artificial (IA) potencialmente útiles en el proceso penal, nuestro enfoque se dirigirá específicamente hacia aquellas que tienen el potencial de predecir y analizar delitos. Comenzaremos exponiendo las herramientas destinadas a la predicción y evaluación de riesgos, para luego adentrarnos en los sistemas que emplean datos biométricos con el mismo propósito. En esta última sección, nos centraremos particularmente en los sistemas de reconocimiento facial.

3.1.1. HERRAMIENTAS DE PREDICCIÓN Y EVALUACIÓN DE RIESGOS

Este tipo de herramientas se podrían definir como “aquellos sistemas que emplean tal tecnología con la finalidad de predecir eventos futuros y, por ende, valorar la existencia de posibles y potenciales peligros o riesgos venideros, a saber: dónde es más probable que vaya a producirse un crimen, si un detenido tiene riesgo de fuga o de reiteración delictiva, si un investigado por violencia de género es probable que vaya a atentar de nuevo contra la víctima, si es previsible que un preso reingrese en prisión tras la concesión de un permiso penitenciario, o si una empresa va a deshacerse de sus activos tras la

notificación del inicio de su investigación, entre otros"[28]. Si bien es verdad que los algoritmos no poseen la facultad de predecir el futuro de manera precisa, sí pueden calcular la probabilidad de que ciertos eventos ocurran basándose en datos históricos[29]. Para lograr esta tarea con éxito, es imperativo que los algoritmos sean entrenados adecuadamente.

Este tipo de herramientas que analizaremos enseguida, pueden ser de gran ayuda para los distintos Cuerpos y Fuerzas de Seguridad como para los que nos concierne más a nosotros, para los juristas. Los juristas, en diversas ocasiones, se ven en la tarea de tomar decisiones de gran calado en los derechos fundamentales de los ciudadanos. Estas decisiones suelen basarse en la anticipación de comportamientos futuros, una tarea inherentemente compleja. Ejemplos de estas decisiones incluyen la imposición de medidas cautelares como la prisión provisional, la determinación de la necesidad de órdenes de protección que puedan limitar la libertad individual, o la asignación de recursos de vigilancia a áreas específicas, entre otras[30].

Hasta el momento, jueces, policías y fiscales han debido basarse en la experiencia y en el análisis de las circunstancias específicas de cada caso para tomar decisiones. Estas decisiones se fundamentan en la interpretación de la ley y la jurisprudencia vigente. Es cierto que, a pesar de su formación, los profesionales del sistema judicial pueden enfrentarse a situaciones de incertidumbre y sobrecarga de trabajo. Además, la interpretación de la ley puede variar según el juez que esté a cargo del caso, lo que aumenta el riesgo de decisiones inconsistentes y potencialmente infractoras de los derechos fundamentales. Si bien es cierto que en España gozamos de una segunda

[28] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 125.
[29] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 125.
[30] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 126.

instancia lo que nos permite acudir a órganos superiores para que vuelvan a revisar el caso concreto[31].

Pues bien, la IA podría ser de gran ayuda en la toma de estas decisiones, gracias a esta tecnología los resultados se podrían obtener de manera más eficiente y rápida, lo que podría aligerar la carga de trabajo de los juristas involucrados.

En el presente trabajo nos centraremos en las herramientas empleadas para la toma de decisiones en la fase de instrucción judicial, dejando de lado las que podría haber en el ámbito policial.

Las herramientas de evaluación de riesgos se pueden describir como sistemas que, utilizando inteligencia artificial, detectan posibles peligros y evalúan la probabilidad de su ocurrencia. Su principal propósito es proporcionar información y apoyo a los seres humanos en la toma de decisiones, es decir, por ahora no buscan sustituir al ser humano, simplemente asistirlo para facilitar su labor.

Pues bien, en el ámbito penal son dos las razones por las cuales se han implementado tales sistemas, de acuerdo con CUATRECASAS MONFORTE, y estos son los siguientes: por un lado, la idea de que su uso puede reducir los sesgos humanos al utilizar (aparentemente) datos objetivos; y, por otro lado, la idea de que con su uso habrá una gran reforma en el sistema penal y, también se reducirá la carga de trabajo de los juristas, así como los costes de la Administración de Justicia. Sin embargo, por muy claros y estimulantes que parezcan estos objetivos, en la práctica veremos que no solucionan los problemas como se espera.[32]

Las herramientas de valoración del riesgo juegan un papel primordial al estructurar el proceso de estimación de riesgos. Hay que saber que, en el procedimiento penal, la evaluación de riesgos se suele llevar a cabo mediante el denominado "modelo actuarial

[31] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 127.
[32] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p.164.

de evaluación de riesgos", este consiste en asignar unos valores numéricos a cada factor de riesgo y tras esto se combinan y ponderan cada uno de estos factores a través del algoritmo del sistema para así asignar una puntuación de riesgo[33].

Es decir, estas consideran la probabilidad de que ocurra un evento futuro como resultado de la combinación de diversos factores que previamente contribuyeron a su manifestación. Para ello, se seleccionan muestras de los sujetos y se observan sus circunstancias y comportamientos para determinar qué factores se pueden asociar a la ocurrencia de ciertas acciones. Se utiliza sobre características personales, antecedentes delictivos, y factores contextuales para calcular una puntuación de riesgo. No obstante, debemos tener en cuenta que no se realizan predicciones individuales para personas específicas, sino que las herramientas interpretan valores obtenidos en relación con grupos de individuos que comparten ciertas características. Sin embargo, al considerar la variabilidad inherente entre individuos dentro de un mismo grupo, se hacen evidentes las limitaciones de estas predicciones, especialmente cuando solo se tienen en cuenta factores estáticos.[34]

Como mencionamos anteriormente, los riesgos principales de la IA incluyen sesgos inherentes y falta de transparencia, lo que puede llevar a la violación de derechos fundamentales. Estos problemas también afectan a las herramientas de predicción y evaluación de riesgos, poniendo en peligro su eficacia y potencial. Por lo tanto, es crucial enumerar de manera concisa los principales riesgos asociados con su uso.

Por un lado, encontramos la calidad de datos que se emplean, el hecho de que introduzcamos datos de "mala calidad" en estos sistemas conllevan a unos resultados nefastos y muy perjudiciales para el individuo en el que se empleen[35], y es que como bien

[33] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 165.
[34] SÁNCHEZ VILANOVA, M. "El uso de algoritmos predictivos en el derecho penal. A propósito de la sentencia de la corte de justicia del distrito de la Haya (Países Bajos) sobre RyRI, de 5 de febrero de 2020. *Teoría & Derecho. Revista de Pensamiento jurídico, (33),* 2022, p.11. https://doi.org/10.36151/TD.2022.059
[35] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 165.

menciona SÁNCHEZ VILANOVA "la precisión de estas predicciones varía según el tipo de predicción, el entorno en el que se recopilan los datos del predictor, el mismo tipo de fórmula estadística utilizada o la cantidad de información disponible"[36]. Como hemos destacado anteriormente en la sección sobre los riesgos, es fundamental realizar un entrenamiento adecuado del algoritmo que utilizaremos. De lo contrario, la introducción de datos inexactos podría llevar a respuestas erróneas, dado que incluso un cambio mínimo puede provocar combinaciones sustancialmente distintas de las esperadas.

Además, como hemos señalado anteriormente, la falta de transparencia es un aspecto crítico. En este contexto, es crucial que tanto fiscales como jueces comprendan la información proporcionada por estos sistemas. En muchas ocasiones, estos actores no tienen un conocimiento profundo sobre el funcionamiento de los sistemas de IA, lo que resulta en la toma de decisiones sin una comprensión adecuada del origen de los resultados. De igual manera, los ciudadanos deben estar informados sobre los criterios utilizados por estos sistemas para tomar decisiones y sobre qué bases se sustentan esas decisiones[37].

Por último, todo esto conlleva una posible vulneración de ciertos derechos fundamentales especialmente sensibles, como lo son los derechos a la: libertad[38], la privacidad[39], la igualdad y la no discriminación[40], y, especialmente, la presunción de inocencia, entre otros[41].

Dicho lo expuesto, en la UE y por lo tanto en España no se utilizan estos métodos tanto como en los EE. UU. donde está mucho más extendido su uso. De hecho, lo cierto es que, en EE. UU. cada vez más autores apuestan por su introducción. Especial mención

[36] SÁNCHEZ VILANOVA, M. "El uso de algoritmos predictivos en el derecho penal. A propósito de la sentencia de la corte de justicia del distrito de la Haya (Países Bajos) sobre RyRI, de 5 de febrero de 2020. *Teoría & Derecho. Revista de Pensamiento jurídico, (33),* 2022, p.12. https://doi.org/10.36151/TD.2022.059

[37] CUATRECASAS MONFORTE, C. "La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional". La Ley, Madrid, España, 2022, p. 167.

[38] Art. 6 CDFUE Y 17 CE

[39] Art 7 y 8 CDFUE 18 CE

[40] Art 20-23 CDFUE Y 14 CE

[41] Art 48 CDFUE Y 24 CE

haremos más tarde a COMPAS, que es la herramienta de evaluación de riesgos empleada, por excelencia, en los procesos penales estadounidenses.

3.1.2. HERRAMIENTAS QUE EMPLEAN DATOS BIOMÉTRICOS

En esta sección, nos enfocaremos en las herramientas destinadas específicamente a determinar si se ha cometido un delito o a identificar al culpable, en lugar de evaluar el riesgo de reincidencia del individuo. Estas herramientas son de particular relevancia en la fase de instrucción de un proceso penal, donde se busca determinar si existen suficientes indicios de la comisión del delito para preparar el juicio, tal como lo establece el artículo 299 de la Ley de Enjuiciamiento Criminal (LECrim).[42]

En este estudio, nos enfocaremos en las herramientas que utilizan datos biométricos, especialmente en el reconocimiento facial. No obstante, cabe destacar que existen otras herramientas, como el reconocimiento de ADN, el reconocimiento de emociones, entre otras.

3.1.2.1. Datos biométricos. Reconocimiento facial.

¿Qué son los datos biométricos? Pues bien, los datos biométricos son definidos en el artículo 4.14 del Reglamento General de Protección de Datos (RGDP)[43] ; en el artículo 3, punto 18, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo[44]; y en

[42] Ley de Enjuiciamiento Criminal (LECrim). 14 de septiembre de 1882.BOE-A-1882-6036 Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

[43] 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) Diario Oficial de la Unión Europea, p.34. 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) (boe.es)

[44] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE BOE.es - DOUE-L-2018-81849 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las

el artículo 3, punto 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[45], de la siguiente manera: "*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".* Es decir, son datos que se obtienen a raíz de las diferencias que tenemos los humanos que nos hace únicos, tales como la huella dactilar, la voz, el ADN y otras muchas características que nos hacen diferenciarnos del resto de seres humanos.

Entre estas podemos diferenciar aquellos datos que provienen de la fisiología del ser humano y las que provienen del comportamiento de este. Estas últimas son más difíciles de analizar, pues mientras que el ADN de una persona va a ser el mismo siempre, la voz por ejemplo puede variar a lo largo de nuestra vida[46]. Por ello, a pesar de agrupar todas estas en la misma categoría de datos biométricos, no todas son iguales.

Es cierto que, en la actualidad, la inteligencia artificial (IA) tiene la capacidad de procesar millones de datos biométricos y compararlos con la información previamente entrenada en sus algoritmos para identificar a un individuo en cuestión de segundos, una tarea que un ser humano podría llevar horas o incluso más tiempo realizar. Sin embargo, es importante tener en cuenta que esta tecnología no es infalible. No obstante, cada vez más IA están combinando múltiples rasgos biométricos para aumentar la fiabilidad de los resultados obtenidos. Por ejemplo, los sistemas automatizados de control fronterizo o

instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE.

[45] Directiva (UE) 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 parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DIRECTIVA (UE) 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 parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/ 977/ JAI del Consejo (boe.es)

[46] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 225.

eGates que analizan tanto la huella dactilar como el reconocimiento facial para verificar la identidad del pasajero[47].

En efecto, existen diversos tipos de datos biométricos, entre los cuales se incluyen el reconocimiento facial, el reconocimiento de voz, el reconocimiento de emociones, el reconocimiento de huellas dactilares, el reconocimiento de ADN y el reconocimiento de firma y escritura. De hecho, se llegan a distinguir entre identificados "fuertes" (huellas dactilares, ADN…) y "débiles" (formas de andar, pulsaciones de teclas…)[48]. En el ámbito de este trabajo, nos centraremos específicamente en el reconocimiento facial.

Mediante el reconocimiento facial se busca obtener este tipo de datos de las imágenes del individuo involucrado en un acto delictivo, las cuales han sido previamente captadas mediante sistemas de videovigilancia, ya sea con fines preventivos o de investigación. Posteriormente, se someten estos datos a procesos de análisis específicos con el objetivo de determinar, con un alto grado de certeza, la identidad de dicha persona[49].

El ámbito de interés de este estudio no abarca el simple análisis de vídeos y fotografías sin el uso de sistemas automatizados para extraer datos biométricos y sin cotejo con una base de datos adicional. Lo que resulta de mayor interés en este contexto es la aplicación de componentes de inteligencia artificial o aprendizaje automático, una tendencia cada vez más predominante que marca un avance cualitativo significativo. Este tipo de sistemas automatizados son proclives a la vigilancia masiva, muy difíciles de restringir, los datos que manejan son sensibles, la duración del tratamiento puede ser muy duradera, las conclusiones a las que puede llegar pueden tener un enorme impacto y es posible que se utilicen para finalidades no conocidas. Por eso mismo, es importante destacar que la regulación actual sobre tratamientos "simples" de videovigilancia no proporciona una

[47] List of E-gate Vendors | Automated Border Control | Features & Benefits (dcs.aero)
[48] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 7.
[49] FREIRE MONTERO, A. F. El reconocimiento facial como instrumento de investigación y prevención del delito. *Anuario Da Facultade de Dereito Da Universidade Da Coruña/Anuario Da Facultade de Dereito Da Universidade Da Coruña*, 2022, p. 7. https://doi.org/10.17979/afdudc.2022.26.0.9145

base legal suficiente para habilitar tratamientos con sistemas biométricos que involucren inteligencia artificial y reconocimiento facial[50].

Para empezar, es imprescindible diferenciar entre la identificación biométrica (uno a varios) y la autenticación o verificación biométrica (uno a uno). Y es que la piedra angular para que un dato biométrico se considere un dato sensible o categoría especial de datos es que se trate para "identificar de manera unívoca a una persona física". Por ello, el Grupo del Artículo 29[51] define:

- Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).
- Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

La cuestión es que los segundos no son considerados como tratamiento de datos sensibles y por lo tanto no se encuentran bajo la regulación del artículo 9 RGPD, ya que como bien dice la AEPD a pesar de que se realice un tratamiento de los datos personales, no se llega a procesar la información contra una base de datos previa que permita o confirme la identificación de uno a varios[52]. Sin embargo, en mayo de 2022 el CEPD ha afirmado que ambos casos "constituyen un tratamiento de datos personales, y más concretamente un tratamiento de categorías especiales de datos personales". No obstante, es necesario su posible ratificación judicial o regulatoria[53].

[50] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 8.
[51] Grupo de trabajo del artículo 29. Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, pág. 6 Draft outline for WP29 opinion on "consent" (europa.eu)
[52] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 10.
[53] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, págs. 10 y 11.

La finalidad del uso de estas técnicas puede ser muy amplia y variada. Desde la verificación con datos faciales para acceder al celular o a servicios personales del individuo, hasta el reconocimiento de ciudadanos en la vía pública o en eventos como manifestaciones, con el fin de analizar si están registrados en una base de datos específica y recopilar información sobre su comportamiento, entre otras posibles aplicaciones. Es crucial tener en cuenta que cuando se implementan sistemas de control como estos en espacios públicos, no solo se ven afectadas las personas específicamente buscadas, sino también todas aquellas que transitan por el área en cuestión, por ello hay que diferenciar entre la vigilancia selectiva y la masiva. También es importante saber que hay lugares públicos más sensibles que otros, por ejemplo, un espacio de afluencia habitual religiosa o un espacio destinado a la actividad sindical, es decir, cualquier espacio público que pueda afectar a sujetos especialmente caracterizados[54].

Un factor determinante diferenciado en la Ley de IA es si el tratamiento se lleva a cabo en tiempo real o no, ya que la duración y el mantenimiento de los datos es un elemento muy relevante.

En cuanto a sus posibles utilidades respecto del proceso de instrucción penal, encontramos entre otras, las siguientes:

En principio, estas herramientas podrían facilitar la realización de una rueda de reconocimiento. Aunque pueda parecer una tarea sencilla, encontrar personas con características físicas similares a las descritas por una víctima en algunos casos no es tarea fácil. De hecho, constituye un trabajo arduo para todos los profesionales de la Administración de Justicia involucrados en la instrucción del caso penal correspondiente.

La rueda de reconocimiento se realiza bajo la decisión del juez de instrucción cuando se considera necesaria para avanzar en el procedimiento. En este contexto, los abogados defensores suelen aprovechar la situación para invocar el derecho de defensa de sus

[54] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, págs. 17 y 18.

representados, cuestionando la validez de la rueda realizada. Dada la dificultad de encontrar personas con rasgos físicos similares y la laboriosa tarea que implica, en ocasiones pueden transcurrir largos períodos de tiempo hasta que se lleva a cabo. Esta demora no solo dilata el proceso, sino que también brinda al presunto culpable la oportunidad de haber modificado su apariencia física, lo que dificulta su reconocimiento[55].

Por lo tanto, si contáramos con bases de datos que almacenan fotografías o que tengan la capacidad de encontrar fotografías similares en cuestión de segundos, como lo haría la IA, estas podrían facilitar la identificación y verificación de la persona buscada en cuestión. Siempre que se respetarán los límites legales que habría que imponerles ya que tendrían que respetar los derechos fundamentales que están en juego. Y es que, si no se aplicase la IA de esta manera segura, resultaría "mucho peor el remedio que la enfermedad"[56].

Asimismo, los sistemas de reconocimiento facial de inteligencia artificial pueden ser útiles para identificar a los sospechosos en casos donde no hay testigos disponibles para contrastar la información obtenida mediante este método. Debido a que hay casos en los que no hay una víctima directa que pueda identificar al culpable del delito.

Un ejemplo ilustrativo de esta aplicación se manifiesta en los casos de conducción temeraria. Imagínese que un individuo es sorprendido circulando a una velocidad de 200 km/h en una vía cuya velocidad máxima permitida es de 100 km/h. En tales circunstancias, al verificar las imágenes obtenidas por cámaras de vigilancia para determinar la identidad del titular del vehículo registrado en la matrícula, se observa una discrepancia: la titularidad corresponde a una mujer que niega haber conducido el vehículo, y las imágenes evidencian claramente la presencia de un hombre al volante. Ante esta discrepancia, la mujer alega la posibilidad de que su hermano o su esposo hayan utilizado el vehículo en cuestión. Podría darse el caso de que un observador humano no

[55] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, pp 244-260.
[56] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 253.

lograra distinguir, mediante las imágenes captadas por las cámaras, cuál de los dos individuos ha conducido el vehículo, debido a la similitud en sus rasgos faciales. No obstante, un sistema de inteligencia artificial podría realizar esta identificación basándose en datos biométricos en cuestión de segundos.

Ciertamente, existen numerosos escenarios en los cuales la aplicación de sistemas de inteligencia artificial resultaría de gran utilidad. A través de estas herramientas, sería factible comparar e identificar al responsable de un delito con notable celeridad, lo que permitiría avanzar en el proceso legal. Ya que, en muchos de estos casos, la imposibilidad de identificar al culpable conlleva el archivo del caso, en virtud del principio "in dubio pro reo"[57].

Otras de las situaciones en las que podríamos utilizar este método de reconocimiento facial serían: la localización de personas desaparecidas, la identificación de individuos que han violado medidas cautelares o condenas, la ubicación de aquellos que deben comparecer ante los tribunales en momentos específicos, así como la detección e identificación de posibles delincuentes que crucen las fronteras, entre otros escenarios.

Por ejemplo, en el caso de los quebrantamientos de medidas cautelares, estos pueden presentar desafíos significativos en términos de recopilación de pruebas. Puede ocurrir que una víctima informe a la policía sobre la presencia de su agresor en una zona donde tiene prohibido acercarse, pero, la falta de evidencia tangible puede dificultar la verificación de la denuncia. La presencia de cámaras de vigilancia en áreas específicas podría proporcionar un medio efectivo para corroborar rápidamente la veracidad de la afirmación de la víctima, ofreciendo así un respaldo objetivo a su testimonio y facilitando la recolección de pruebas para proceder con acciones legales[58].

También, en el caso de los ciudadanos que tienen que acudir a los juzgados conllevan mucha labor tanto material como personal, si tuviésemos unas cámaras de reconocimiento

[57] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p. 263.

[58] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, pp. 270 y ss.

facial en las puertas de los juzgados capaces de detectar que ese sujeto ha llegado solo con que ese sujeto se personase delante de esas cámaras, entonces ahorraría mucho trabajo a los trabajadores de la Administración de Justicia que hoy día son encargados de asegurarse que ese individuo se ha personado en los juzgados[59].

Por último, los sistemas inteligentes de reconocimiento facial pueden ser útiles en una variedad de situaciones además de las mencionadas. Lo importante es entender cómo funciona, ya que, resumidamente, el reconocimiento facial con inteligencia artificial en el proceso penal implica capturar imágenes faciales, extraer características únicas, compararlas con una base de datos y tomar decisiones sobre la identidad de individuos. Esta ayuda gratamente en la identificación de sospechosos, pero no reemplaza la evaluación humana en el proceso legal.

4. MARCO LEGAL

4.1. REGLAMENTO DE LA UE Y SU REGULACIÓN ACERCA DEL USO DE ESTOS SISTEMAS DE IA

En el ámbito del uso de tecnologías y datos biométricos, se observa una significativa confluencia y superposición de regímenes jurídicos. Hay que tener muy presente que toda la materia relacionada con la IA es algo en constante evolución y que queda todavía mucho camino por recorrer, por lo tanto, no es una materia sobre la que encontremos una gran variedad de normativa, más bien, nos encontramos ante una normativa muy reciente.

Analizaremos entonces qué incidencia tiene el Reglamento del Parlamento Europeo y el Consejo para establecer reglas armonizadas de IA (de ahora en adelante: Ley de IA) en relación con la IA y en específico en relación con el uso de este tipo de sistemas utilizando herramientas relacionadas con datos biométricos ya que es el tema que nos concierne en el presente trabajo.

[59] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, pp. 277-278.

Antes de todo, es cierto que las instituciones de la Unión Europea han intentado llevar a cabo una serie de estudios y han publicado diversos trabajos que pretendían aclarar en cierto modo esta materia, como por ejemplo el *Libro Blanco sobre IA* de febrero de 2020[60]. Sin embargo, no es hasta el 13 de marzo de 2024 que encontramos la Ley de la IA, ya que hasta este momento no teníamos regulado el uso de este tipo de sistemas inteligentes. Este Reglamento es de vital importancia ya que regula diversos aspectos y problemáticas.

Podríamos dedicar un trabajo entero solo a analizar esta Ley, sin embargo, nos centraremos en su relación con el uso de datos biométricos, explicaremos qué condiciones se imponen en el uso de este tipo de sistemas y en qué situaciones está permitida su utilización.

Es apropiado comenzar el análisis considerando el futuro Reglamento sobre IA de la UE. Este parte de una teórica prohibición general al uso de sistema de IA de identificación biométrica, con la excepción de algunos casos que luego explicaremos, que son calificados de alto riesgo y que por lo tanto quedan abajo la intensa regulación de esta Ley. Además, su posible aplicación tendrá que respetar las normativas pertinentes de protección de datos y otras normas.

Ya en la exposición de motivos se menciona que la presente propuesta contiene determinadas normas específicas para la protección de las personas en relación con el tratamiento de los datos personales, específicamente las restricciones que se le van a imponer a estos sistemas de IA para la identificación biométrica remota "en tiempo real" (más adelante explicaremos lo que es) y explica que a la hora de analizar este aspecto tenemos que atender al artículo 16 del TFUE que dice: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen".[61]

[60] LIBRO BLANCO sobre la inteligencia artificial -un enfoque europeo orientado a la excelencia y la confianza. Bruselas, 19 de febrero de 2020. EUR-Lex - 52020DC0065 - EN - EUR-Lex (europa.eu)
[61] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Exposición de motivos, p. 3 y ss. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

Así mismo, en los considerandos se define tanto la noción de "datos biométricos" como la noción de "sistema de identificación biométrica remota". Mientras que la primera definición coincide con la mencionada anteriormente en el trabajo, la segunda debe definirse de la siguiente manera: "como un sistema de IA destinado a identificar a distancia a personas físicas comparando sus datos biométricos con los que figuren en una base de datos de referencia, sin saber de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen. Es preciso distinguir entre los sistemas de identificación biométrica remota "en tiempo real" y "en diferido", dado que tienen características distintas, se utilizan de manera diferente y entrañan riesgos distintos." Seguidamente refiere que mientras que en los de "tiempo real" la recogida de los datos biométricos, su comparación e identificación ocurren de manera instantánea o casi instantánea, en los sistemas "en diferido" los datos ya se han recabado y su comparación e identificación se producen en un momento posterior.[62]

La cuestión es que esos sistemas de identificación biométrica remota "en tiempo real" invaden especialmente los derechos y las libertades de las personas, ya que pueden provocar la sensación de estar en constante vigilancia y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales, cuestión ya mencionada anteriormente respecto de los derechos fundamentales que están en juego al aplicar estos sistemas[63]. Por ello, como hemos explicado, el Reglamento parte de que se prohíbe el uso de estos sistemas, salvo en tres situaciones que han enumeraremos de manera concreta y precisa, y son casos en los que su utilización es estrictamente necesaria para lograr un interés público esencial y en donde los riesgos son inferiores a la importancia de su uso.

[62] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Considerando 7 y 8, p. 22. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

[63] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Considerando 18, p. 25. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

Todo uso de estos sistemas de identificación biométrica remota en "tiempo real" en espacios de acceso público con fines de aplicación de la ley debe estar permitido de una manera expresa y específica por una autoridad judicial o bien una autoridad administrativa de un Estado miembro. Esta autorización habrá que obtenerla con anterioridad de su uso a menos que sea una situación de urgencia y se justifique. Con todo esto no podemos olvidar que con este Reglamento los Estados miembros siguen teniendo la oportunidad de no ofrecer el uso de estos sistemas, ya que es el Estado miembro es el que puede decidir si autorizar expresamente su utilización.[64]

Los requisitos y presupuestos para esta autorización están predeterminados en el Reglamento y se precisa que el sistema que se vaya a utilizar sea "estrictamente necesario". Además, se deben cumplir otros requisitos como: la necesidad y proporcionalidad, tener en cuenta en lugar en el que se están colocadas las cámaras, las consecuencias de no usar el sistema, y el impacto en los derechos de los afectados[65].

Asimismo, todo aquel tratamiento de datos biométricos y datos personales que sea distinto al de identificación biométrica remota en "tiempo real" de este Reglamento debe seguir cumpliendo todos los requisitos del artículo 9, apartado 1, del Reglamento (UE) 2016/679; el artículo 10, apartado 1, del Reglamento (UE) 2018/1725 y el artículo 10 de la Directiva (UE) 2016/80[66].

No se olvida tampoco el reglamento de mencionar la gran problemática de los sesgos, cuando en su considerando 33 expresa que los sistemas de IA destinados a la identificación biométrica remota pueden dar lugar a resultados sesgados y por lo tanto a

[64] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Considerando 21 y 22, p. 26. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

[65] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 23.

[66] Estos artículos vienen a decir que todos aquellos tratamientos de datos personales que revelen el origen étnico o racial, las opiniones política, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física sólo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardas adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

tener ciertas consecuencias discriminatorias. Por ello, los sistemas de identificación biométrica remota tanto en "tiempo real" como "en diferido" conllevan un alto riesgo -razón por la que son calificados de este modo-.

En cuanto al control de dichos sistemas, como norma general es el proveedor del producto quien debe llevar a cabo a la evaluación de este bajo su propia responsabilidad, sin embargo, debido a las graves consecuencias que puede conllevar la identificación biométrica de personas, en este caso debe preverse que un organismo notificado participe en la evaluación de la conformidad. Serán las autoridades nacionales competentes las que designen a los organismos notificados que realizarán esa evaluación externa[67]. Es fundamental informar a las personas involucradas sobre la interacción con sistemas de inteligencia artificial, salvo que la situación sea evidente por sí misma.

Demos paso ahora a examinar la normativa específica que regula este tipo de sistemas inteligentes. Como bien menciona el artículo 1. d), uno de los objetos del presente Reglamento es: "las normas armonizadas de transparencia aplicables a los sistemas de IA destinados a interactuar con personas físicas, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica, así como a los sistemas de IA usados para generar o manipular imágenes, archivos de audio o vídeos". Encontramos en el artículo 3, las definiciones relativas a todos los conceptos que nos interesan, como bien son: datos biométricos, sistema de categorización biométrica, entre otros.

Si bien hemos explicado que este Reglamento en principio parte de la prohibición del tratamiento de datos biométricos. Pero el uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de aplicación de la ley estarán prohibidos, de acuerdo con el artículo 5.1 d) de esta Ley, salvo que su uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

- La búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos

[67] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Considerando 64 y 65, p. 38. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

- La prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista
- La detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido algunos de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo[68], para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro (En el artículo 2.2 de la Decisión mencionada se enumeran esos delitos, entre los cuales se incluyen el delito de terrorismo y el delito de corrupción, entre otros. Es importante destacar que, dentro de los 32 delitos mencionados, algunos poseen una relevancia superior a otros. Por consiguiente, la aplicación de sistemas específicos variará dependiendo del tipo de delito en consideración. Esta variación se justifica en la necesidad de evaluar la proporcionalidad y la pertinencia de su empleo, así como en la consideración de la gravedad del delito y los potenciales perjuicios que puedan derivarse del mismo[69].)

Es decir, en los casos que nos concierne en principio de acuerdo con este Reglamento estará autorizado el uso de este tipo de sistemas, ya que sirven para una finalidad concreta que es la de buscar víctimas de un delito, así como conocer al culpable de uno.

Evidentemente, siempre bajo unas cautelas y requisitos que explicaremos más adelante. Debido a que para su utilización se deberán tener en cuenta diferentes aspectos como la naturaleza de la situación para que se dé lugar a este tipo de herramientas, igualmente habrá que atenerse a las consecuencias que podría tener su uso para los derechos y las libertades de las personas implicadas. Además, el uso de estos sistemas para las causas

[68] Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros. BOE.es - DOUE-L-2002-81377 Decisión Marco del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (2002/584/JAI).

[69] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Considerando 19, p. 25. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

que hemos mencionado anteriormente tendrá que ser proporcionadas en relación con su uso[70].

Para poder utilizar estos sistemas, como bien expresa el artículo 5.3 del Reglamento, se tendrá que obtener "una autorización previa por parte de una autoridad judicial o de una autoridad administrativa independiente del Estado miembro donde se vaya a utilizar este sistema". No obstante, sí es una situación de urgencia que está debidamente justificada sí que se podrán utilizar estas herramientas sin la autorización pertinente, siempre que se solicite lo más inmediatamente posible y se conceda con posterioridad[71].

Por último, en el Título IV, artículo 52 del Reglamento[72] encontramos ciertas obligaciones de transparencia que deben de cumplir determinados sistemas de IA. Recalca que los proveedores deben garantizar que estos sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de una manera que las personas que estén interactuando con dichas máquinas estén informadas de ello, excepto que sea evidente que se están utilizando debido al contexto. Sin embargo, no se aplicará esta obligación a aquellos sistemas que estén autorizados para fines de detección, prevención, investigación o enjuiciamiento de infracciones penales, salvo que estén a disposición del público para denunciar una infracción penal. Añade que los usuarios de un sistema de categorización biométrica y de un sistema de reconocimiento de emociones deben informar del funcionamiento de dichos sistemas a las personas físicas que estén expuestas a él, siempre exceptuando a los que con autorizados por la ley para fines de detección, prevención e investigación de infracciones penales. Por lo tanto, podemos ver que estas obligaciones no son vinculantes en aquellos casos que nos conciernen, ya que

[70] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Art. 5.1, p 49. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

[71]Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Art. 5.3, p 50 y 51. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

[72] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021.Art. 52, p.77 y 78.EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

los casos de los que hemos hablado tienen como finalidad prevenir e investigar delitos penales.

4.2. NORMATIVA CONCURRENTE

Los sistemas de identificación biométrica involucran el tratamiento de datos personales, por lo tanto, además de estar sujetos a la Ley de Inteligencia Artificial y tener que cumplir con los requisitos exigidos a los sistemas de alto riesgo, también están sujetos al régimen de protección de datos. Esta concurrencia no es sencilla pues son normas con lógicas diferentes. Mientras que la Ley de IA va dirigida a imponer obligaciones a los proveedores de los sistemas de IA y a las empresas o entidades que los utilicen, la de protección de datos va más enfocada a establecer garantías para las personas adecuadas[73].

El uso de sistemas biométricos en el ámbito policial y penal quedará bajo la regulación de la Directiva (UE) 2016/680 y, por ende, la transposición española de la Ley Orgánica 7/2021, de 26 de mayo. Asimismo, todo aquel tratamiento de datos biométricos y otros datos especialmente protegidos estarían sometidos al régimen general de protección de datos (RGPD).

Pues bien, desde la perspectiva de protección de datos el punto de partida es la prohibición del tratamiento de datos, que sólo se puede levantar si se dan los requisitos excepcionales que se regulan. Por consiguiente, deberá cumplir con lo estipulado tanto en la Directiva como en el RGPD, donde los artículos 10 y 11 de la primera guardan similitud con los artículos 9 y 22 de la segunda, si bien estos últimos son más estrictos[74].

En términos generales, la implementación de sistemas de identificación biométrica implica una significativa limitación de varios derechos fundamentales, lo que demanda una legislación exhaustiva, de alta calidad y altamente protectora.

[73] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 25.

[74] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 26.

La legislación debe establecer normativas claras y precisas que definan el alcance y la aplicación de la medida en cuestión, y debe imponer salvaguardias para garantizar que las personas cuyos datos son tratados tengan suficientes garantías para proteger eficazmente sus datos personales contra el riesgo de abuso y cualquier acceso o uso indebido de los mismos. La ley también debe establecer condiciones sustantivas y procedimentales, así como criterios objetivos para determinar los límites del acceso de las autoridades competentes a los datos y su uso posterior.

En efecto, el Tribunal Constitucional español ha sido riguroso en cuanto a los principios de calidad legislativa, también en lo que respecta al derecho de protección de datos personales. Cabe destacar la STC 76/2019, de 22 de mayo, donde se enfatizó la importancia de establecer de manera clara y completa las disposiciones legales que regulan el tratamiento de datos personales, sin dejar lagunas que deban ser llenadas posteriormente por desarrollos legales adicionales o dejando decisiones críticas en manos de los particulares. Y estas exigencias legales se dan de manera precisa respecto de datos especialmente protegidos del artículo 9 RGPD y el artículo 10 de la Directiva (UE) 2016/680, entre los que se incluyen los datos biométricos[75].

En síntesis, corresponde a la legislación incorporar las garantías efectivas que equilibren el régimen restrictivo de derechos, especialmente en el caso de tratamientos biométricos. De este modo, la normativa legal deberá especificar los objetivos concretos, la fiabilidad y precisión mínimas del algoritmo utilizado, el período de retención de los datos, la capacidad de auditar estos criterios, la trazabilidad del proceso y otras salvaguardias pertinentes.

Es importante tener en cuenta que para levantar la presunta prohibición establecida en el artículo 5 de la Ley de Inteligencia Artificial, se requiere una acción expresa por parte del legislador, particularmente en lo que concierne al uso de sistemas para la detección, localización, identificación o enjuiciamiento de personas (artículo 5.1 d) iii). Deben

[75] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 29.

establecerse normativas detalladas en relación con las autorizaciones específicas necesarias para el uso de estos sistemas y para su supervisión (artículos 5.3 y 5.4).

Por consiguiente, la Ley de Inteligencia Artificial por sí sola no constituye una regulación legal adecuada para supervisar el uso de sistemas de identificación biométrica. La falta de prohibición de ciertos casos de reconocimiento facial u otros tratamientos biométricos no implica su autorización y legalización en términos de protección de datos, en el considerando 24 lo podemos ver reflejado. Efectivamente, existe una incertidumbre al respecto, por lo que se ha sugerido aclararlo explícitamente en el texto. Sería recomendable que la regulación de sistemas biométricos en la Ley de Inteligencia Artificial se alinee con el Reglamento General de Protección de Datos (RGPD) y la Directiva (UE) 2016/680. Asimismo, sería conveniente que la Ley de IA enumere los propósitos para los cuales se permite la identificación biométrica a distancia en tiempo real[76].

5. CASOS DE ESTUDIO REALES

5.1. ESTADOS UNIDOS: sistema de valoración de riesgos

En España, el uso de sistemas de valoración de riesgos y reconocimiento facial no es común. Sin embargo, en países como Estados Unidos, estas técnicas son más habituales. Nos centraremos en un caso particular que destaca uno de los principales riesgos que hemos discutido: los sesgos. En este país, se emplea un sistema llamado COMPAS, uno de los más conocidos, cuyo uso ha resultado en una sentencia que ilustra claramente esta problemática

COMPAS (*Correctional Offender Management Profiling Alternativa Sanctions*), propiedad de *Northpoint*, es una de las varias herramientas que usa el sistema de justicia

[76] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 31.

penal de EE. UU. de "evaluación de riesgo"[77]. Es un sistema mediante el cual se ayuda al juez a decidir si un acusado, que todavía no es culpable, debe esperar al juicio en prisión o si por el contrario debe ser liberado hasta el juicio oral.

El algoritmo de este sistema de IA realiza un cálculo para determinar la probabilidad de reincidencia de un acusado, y en base a este análisis decide si se le concede la libertad condicional o si debe permanecer en prisión mientras espera el juicio. Este proceso implica la consideración de diversos datos, como la edad del individuo, su historial criminal, los detalles del delito actual y respuestas a preguntas sobre su comportamiento, entre otros factores relevantes, los cuales son evaluados en conjunto para determinar las probabilidades de reincidencia.

No obstante, los algoritmos que utiliza el sistema COMPAS siguen siendo privados y están protegidos por el secreto de empresa. Sin extendernos mucho, uno de los mayores problemas que se plantean en torno al uso de estos sistemas es que colisionan derechos como el del secreto de la empresa y el derecho a la defensa de los acusados y a un proceso con todas las garantías, en los casos en los que la IA pertenece a una empresa privada, como en este caso[78].

El Tribunal Supremo de Wisconsin (EE. UU.) analizó y resolvió en el caso *"State vs Loomis"*, y se convirtió en referente sobre el uso de este tipo de sistemas en el proceso penal. Por ende, procederemos a examinar de manera sucinta este caso, dado que guarda una estrecha relación con el sistema COMPAS, el cual fue empleado para determinar el destino del denunciante Eric Loomis.

Eris Loomis fue acusado de cinco cargos por intervenir presuntamente en un tiroteo efectuado desde un vehículo. Este negó haber participado en este tiroteo si bien admitió haber conducido ese mismo vehículo ese mismo día, para poder quedar en libertad

[77] HAO, K. "Caso práctico: probamos por qué un algoritmo judicial justo es imposible". Noviembre de 2021. Caso práctico: probamos por qué un algoritmo judicial justo es imposible | MIT Technology Review en español

[78] CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*". La Ley, Madrid, España, 2022, p.173.

admitió los cargos relacionados con conducir un vehículo ajeno sin autorización e intentar huir de la policía.

El magistrado, al determinar la pena, consideró diversos elementos, entre los cuales figuraba el dictamen arrojado por el sistema COMPAS. Este evaluó al individuo y concluyó que presentaba un alto riesgo de reincidencia.

En tal sentido, Loomis solicitó que se revisara la sentencia, argumentando, entre otros aspectos, que la fundamentación de la decisión en el resultado emanado del sistema COMPAS vulneraba su derecho a un debido proceso. Sin embargo, el tribunal rechazó modificar la condena, explicando que el resultado derivado de dicho sistema únicamente había servido para respaldar las conclusiones alcanzadas con el resto de la información disponible, y que, incluso en ausencia de dicho sistema, el desenlace habría sido idéntico.

Tras esto, Loomis recurrió entonces ante el Tribunal Supremo de Wisconsin (TSW) alegando que la utilización de tal sistema (COMPAS) vulneraba su derecho a un proceso con todas las garantías por tres razones y cito textualmente: "(1) se había violado su derecho a ser condenado sobre la base de información fiable y precisa, ya que la naturaleza de secreto comercial del algoritmo con el que funciona COMPAS le había impedido conocer cómo se habían calculado las estimaciones de riesgo y por tanto refutar la validez científica del nivel de riesgo que dicha herramienta le había asignado; (2) se había vulnerado su derecho a obtener una sentencia individualizada, y (3) se había tenido en cuenta indebidamente su género para determinar la pena[79].

El Tribunal Supremo de Wisconsin rechazó el recurso al considerar que el secreto empresarial es esencial para el funcionamiento de COMPAS, y que la falta de acceso a esta información no infringió el derecho de los acusados a ser juzgados sobre una base fiable. Argumentó que Loomis tuvo acceso a los resultados basados en sus propias respuestas al cuestionario previo. Además, el Tribunal destacó que la sentencia fue individualizada, ya que los resultados de COMPAS fueron solo un componente adicional para el juez al tomar su decisión. Finalmente, explicó que el uso del género como un

[79] MARTÍNEZ GARAY, L. "Peligrosidad, algoritmos y *due process*: el caso *state vs loomis*". *Universidad de Valencia. Revista de Derecho Penal y Criminología,* núm 20 (julio de 2018), p. 491.

factor en la evaluación del riesgo no es discriminatorio, sino que mejora la precisión del sistema y beneficia tanto a los acusados como a la administración de justicia[80].

La sentencia resalta el dilema de integrar datos considerados rigurosos por el tribunal, pero que plantean riesgos para los derechos del acusado. ¿Deberíamos descartar los beneficios potenciales de los sistemas de evaluación de riesgos si existe la posibilidad de comprometer los derechos fundamentales al aplicarlos? Como bien dice la fórmula de Blackstone (ratio de Blackstone) "es mejor que diez personas culpables escapen a que un inocente sufra"[81].

A continuación, ofreceremos una síntesis de los riesgos asociados a la inteligencia artificial en el contexto de este caso específico. En primer lugar, se argumenta que la información obtenida en los sistemas de valoración de riesgos es objetiva y, por lo tanto, preferible a la evaluación de un juez que podría estar influenciada por prejuicios subconscientes. Sin embargo, se pasa por alto que los algoritmos de estos sistemas se basan en datos históricos de casos anteriores, los cuales han sido juzgados por jueces que ya tenían estos sesgos subconscientes. Esto significa que, aunque las respuestas de los sistemas puedan parecer objetivas, todavía pueden reflejar un sesgo sistémico integrado en su funcionamiento, que podría perpetuarse y multiplicarse con el tiempo[82].

En este caso específico, se observa una tendencia a desfavorecer a las minorías, particularmente a la comunidad afroamericana en Estados Unidos. Aunque la raza no se considere directamente en la evaluación del riesgo, otros factores como los antecedentes penales están estrechamente ligados a la raza, dado el conocimiento general de que las minorías étnicas enfrentan más condenas y sentencias más severas. Por lo tanto, si los algoritmos se entrenan con casos predominantemente desfavorables para estas minorías, como los afroamericanos, el sistema perpetúa este sesgo.

Se plantea otro dilema de igual o mayor importancia: ¿es ético emplear sistemas de evaluación de riesgos basados en herramientas protegidas por el secreto comercial, cuyo

[80] MARTÍNEZ GARAY, L. "Peligrosidad, algoritmos y *due process*: el caso *state vs loomis*". *Universidad de Valencia. Revista de Derecho Penal y Criminología,* núm 20 (julio de 2018), p. 492.
[81] MARTÍN, L "La fórmula de Blackstone. Grietas de miseria moral e insolidaridad resquebrajan hoy la sociedad española". Abril de 2013. La fórmula de Blackstone | Opinión | EL PAÍS (elpais.com)
[82] MARTÍNEZ GARAY, L. "Peligrosidad, algoritmos y *due process*: el caso *state vs loomis*". *Universidad de Valencia. Revista de Derecho Penal y Criminología,* núm 20 (julio de 2018), pp. 496 y ss.

funcionamiento no se divulga al público? Según los principios legales, los acusados tienen derecho a conocer con precisión y fiabilidad sobre qué información se les acusa y a verificar su veracidad, como hemos explicado anteriormente en el trabajo. Por lo tanto, no sería apropiado considerar suficiente que los resultados de la evaluación de riesgos se proporcionen al acusado, junto con los datos que él mismo proporcionó en el cuestionario, como afirmó el Tribunal Supremo de Wisconsin (TSW). En este caso, el acusado carecía de información sobre el valor atribuido a cada respuesta que ofreció en el cuestionario de evaluación de riesgos[83].

Desde nuestra perspectiva, resulta inmoral e ilegítimo recurrir a sistemas privados que impactan significativamente en los derechos fundamentales de los ciudadanos. Resulta inconcebible que se empleen este tipo de sistemas, especialmente considerando que podrían ser desarrollados por el gobierno o administraciones públicas, lo que garantizaría una mayor transparencia en el uso de la información y en el proceso de evaluación del riesgo, o en el caso de que lo desarrollen empresas privadas, que sus algoritmos no lo sean. Los derechos consagrados en el artículo 24.2 de nuestra Constitución, que protegen los intereses individuales, deben prevalecer sobre los beneficios que una empresa pueda obtener a expensas de dichos derechos.

5.2. ESPAÑA: reconocimiento facial.

En España, el uso de sistemas como COMPAS, comunes en Estados Unidos, aún no está extendido. Sin embargo, un caso relevante fue la sanción impuesta a la cadena de supermercados MERCADONA por el uso de tecnologías de reconocimiento facial en sus establecimientos. Esta situación, estrechamente relacionada con el tema tratado, evidenció la vulneración de derechos que implicaba el uso de dichos sistemas, siendo una de las razones principales para la condena a MERCADONA.

[83] MARTÍNEZ GARAY, L. "Peligrosidad, algoritmos y *due process*: el caso *state vs loomis*". *Universidad de Valencia. Revista de Derecho Penal y Criminología,* núm 20 (julio de 2018), pp. 497 y ss.

En estos supermercados se pusieron unas cámaras de vigilancia de reconocimiento facial mediante las cuales se podía comprobar si entraba al establecimiento alguna persona que había tenido alguna prohibición de entrar en el supermercado[84].

Es decir, implantó un sistema inteligente biométrico que controlaba si quienes accedían a algunos establecimientos estaban en sus listas de búsqueda por motivos judiciales previos, por lo que fue sancionada en 2021 por la AEPD.

La AEPD inició actuaciones de investigación al conocer acerca de la implantación de estos sistemas en Mercadona, los cuales como he resumido detectaban a aquellas personas que tenían sentencias firmes y órdenes de alejamiento en vigor contra Mercadona o contra alguno de sus trabajadores. Después de todo resolvió que debía sancionar a MERCADONA por infracción de los siguientes artículos: art. 6 y 9 del RGDP[85], tipificadas en el art. 83.5. a), de dicha norma; art. 12 y 13 del RGDP, tipificadas en el art. 83.5.b), de dicha norma; art. 5.1c), del RGDP, tipificada en el art. 83.5.a), de dicha norma; art. 25.1 del RGDP, tipificada en el art. 83.4.a), de dicha norma; art. 35 del RDGP, tipificada en el art. 83.4.a), de dicha norma; y por último, prohibir todo el tratamiento de datos personales relativo al reconocimiento facial en sus establecimientos, de acuerdo al art. 58.2.f). Por lo tanto, se le condenó con una sanción de dos millones de euros[86].

La empresa intentó apelar argumentando que se aplicaban estos sistemas debido a la protección del "interés público", en lugar de admitir que el único propósito era proteger exclusivamente los intereses de la empresa. No obstante, quedó claro que el uso de estos sistemas no era proporcional, ya que existen medios menos intrusivos en la privacidad del usuario[87].

---

[84] El reconocimiento facial de Mercadona acaba en multa de 2,5 millones de euros: qué dice la Agencia de Protección de Datos y qué lecciones se pueden extraer (xataka.com)

[85] 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) Diario Oficial de la Unión Europea. 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) (boe.es)

[86] PS-00120-2021 Resolución de fecha 23-07-2021 Artículo 12 13 15 25 35 5.1.c) 6 9 RGPD (aepd.es)

[87] PÉREZ, E." El reconocimiento facial de Mercadona acaba en multa de 2,5 millones de euros: qué dice la Agencia de Protección de Datos y qué lecciones se pueden extraer". 2021. El reconocimiento facial de

Es crucial tener en cuenta el impacto al implementar sistemas de reconocimiento facial en espacios públicos de acceso, ya que no solo afecta a las personas buscadas, sino a todas las personas analizadas. Aunque el procesamiento de datos sea rápido, implica grandes cantidades de información, que incluyen a colectivos vulnerables como menores o discapacitados. Esto se tuvo en cuenta al evaluar la situación del supermercado en cuestión[88].

6. CONCLUSIONES

En conclusión, la inserción de la inteligencia artificial (IA) en el panorama jurídico marca un punto de inflexión en la evolución del sistema legal contemporáneo. Si bien la IA presenta un horizonte prometedor de avances, su actual estado de desarrollo y su constante evolución plantean incógnitas sobre sus límites y potencialidades futuras. Resulta innegable que, incluso hace pocos años, la magnitud de las capacidades actuales de la IA habría parecido imposibles, lo que subraya la necesidad de reconocer que todavía queda mucho camino por recorrer en este ámbito.

La incorporación de la IA en el proceso penal supone, sin duda, un progreso significativo en términos de eficiencia, comodidad y precisión. No obstante, como hemos destacado en el presente análisis, este avance no está exento de desafíos y riesgos que hay que tener en consideración. Y es que, los sistemas inteligentes, si bien prometen mejorar la toma de decisiones, se enfrentan a sesgos algorítmicos, opacidad en su funcionamiento y falta de explicabilidad, lo cual plantea interrogantes sobre la equidad y la justicia en la aplicación del derecho.

En lo que respecta a la predicción y valoración de riesgos, los sistemas de IA como hemos analizado suelen ser susceptibles a sesgos y errores, esto puede desembocar en resultados

Mercadona acaba en multa de 2,5 millones de euros: qué dice la Agencia de Protección de Datos y qué lecciones se pueden extraer (xataka.com)

[88] COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023, pág. 17.

discriminatorios o injustos, como ha quedado patente en casos de notoriedad, como el *“State vs Loomis”.*

Desde nuestra perspectiva, los sistemas de predicción y evaluación de riesgos aún no han alcanzado el nivel de desarrollo necesario para su plena aplicación, especialmente evidenciado en el caso *"State vs Loomis"*, donde se recurrió a una empresa privada para evaluar la probabilidad de reincidencia de un individuo. Como hemos argumentado a lo largo de este estudio, si bien estos sistemas podrían ofrecer valiosa ayuda al canalizar las probabilidades de reincidencia, su utilización plena requiere un examen meticuloso.

Es crucial subrayar que cualquier sistema de este tipo debe ser gestionado por una entidad pública, garantizando la transparencia en su funcionamiento y asegurando que tanto el individuo evaluado como el magistrado tengan acceso a la información utilizada en el proceso. O, si, por el contrario, no puede ser así y debe ser una empresa privada la que lleve a cabo este sistema inteligente, su algoritmo deberá ser público. En este contexto, considero que un sistema de este tipo podría complementar eficazmente la labor del juez, quien, en última instancia, debe tener la autoridad para tomar decisiones. Incluso si el magistrado opta por no seguir las recomendaciones del sistema inteligente, esa prerrogativa debe ser respetada, pues estos sistemas deben ser considerados como herramientas complementarias, no como dictámenes inflexibles.

Asimismo, la utilización de datos biométricos, en particular el reconocimiento facial, suscita inquietudes adicionales sobre la protección de la privacidad, en términos generales, y la preservación de los derechos fundamentales.

Es evidente que la implementación de sistemas de reconocimiento facial conlleva implicaciones profundas, particularmente en relación con la instalación de cámaras de videovigilancia en espacios públicos. Estos entornos, en teoría, deberían garantizar un cierto grado de libertad individual, sin embargo, la presencia de cámaras de vigilancia plantea cuestiones sobre la privacidad y la autodeterminación.

El simple conocimiento de ser observado, aunque no se tenga la intención de vigilancia directa sobre uno mismo, puede generar una sensación de vigilancia constante y coartar

la libertad de acción en espacios que deberían ser de libre acceso. Un ejemplo ilustrativo de esta situación es cuando las cámaras se ubican cerca de lugares de culto o de reuniones sindicales, lo que puede disuadir a las personas de participar en estas actividades, menoscabando así indirectamente derechos fundamentales como la libertad de reunión y la libertad religiosa.

Por otro lado, es indudable que estos sistemas ofrecen ventajas significativas en términos de seguridad pública. La capacidad de detectar rápidamente a delincuentes o individuos desaparecidos es innegablemente valiosa y puede salvar vidas. En este sentido, puede considerarse que el beneficio de la seguridad pública compensa la intrusión en la privacidad que implica la vigilancia continua.

Sin embargo, es imperativo que el uso de estos sistemas se adhiera estrictamente a los límites legales y éticos. La retención de datos personales capturados por las cámaras de reconocimiento facial debe ser limitada en el tiempo y su eliminación debe ser rápida y efectiva, garantizando así la protección de la privacidad de los individuos involucrados.

En resumen, si bien el uso de sistemas de reconocimiento facial puede ofrecer beneficios en términos de seguridad pública, es esencial que se implementen salvaguardas adecuadas para proteger los derechos individuales y mantener un equilibrio entre seguridad y privacidad en el espacio público.

Para afrontar estas preocupaciones, el Reglamento del Parlamento Europeo y el Consejo para establecer reglas armonizadas de IA establece ciertas directrices para regular el uso de sistemas de datos biométricos, como bien hemos explicado. En este caso, los prohíbe en términos generales, exceptuando la prohibición en situaciones específicas en las que se considera necesario el uso de estos sistemas siempre que garanticen la protección de los derechos individuales y la privacidad. Es decir, aunque se permita su uso en determinados contextos, ello no exime de la necesidad de cumplir con los rigurosos requisitos para salvaguardar estos derechos fundamentales.

Considero que, a pesar de los esfuerzos regulatorios existentes, aún persisten lagunas significativas en el marco normativo aplicable a los sistemas de reconocimiento facial.

En primer lugar, es importante señalar que la regulación actual es de naturaleza europea, lo que implica que cada estado miembro debe adaptarla y autorizarla según su propio criterio, lo cual genera incertidumbre sobre su implementación efectiva y sus implicaciones prácticas.

De hecho, dado que esta regulación acaba de ser aprobada y aún no es aplicable, carecemos de casos concretos que nos permitan evaluar su efectividad y conformidad con los principios fundamentales de derechos humanos y protección de datos. Este período de transición nos brinda la oportunidad de examinar detenidamente si dicho marco normativo proporciona las salvaguardias necesarias para garantizar el funcionamiento adecuado de los sistemas de reconocimiento facial sin menoscabar los derechos individuales.

Asimismo, es fundamental tener en cuenta que, en el caso específico de España, la regulación nacional deberá armonizarse con otras normativas relevantes, como la legislación sobre protección de datos. Por lo tanto, aún no podemos evaluar plenamente el alcance y la eficacia de estos sistemas inteligentes ni de su marco regulatorio asociado. Aunque las directrices normativas parecen claras en teoría, su implementación y autorización por parte de cada estado requerirán una comprobación detallada en el futuro cercano para determinar si su uso en espacios públicos es verdaderamente justificado y beneficioso.

En última instancia, si bien las tecnologías emergentes pueden ser de gran ayuda para la Administración de Justicia y los profesionales del derecho, queda patente que aún queda un largo trecho por recorrer en su perfeccionamiento. Es imperativo reconocer que la intervención humana sigue siendo fundamental en el proceso penal. La IA, por tanto, debería concebirse como un complemento al juicio humano, no como su sustituto. A través de un enfoque equilibrado y una supervisión constante, podremos aprovechar el potencial transformador de la IA en el ámbito legal, sin comprometer los principios esenciales de justicia y equidad. Además, creo que debemos someter estos sistemas a revisiones, ya sean semanales, mensuales, anuales dependiendo de la importancia de los casos que lleven.

En definitiva, resulta patente que, al igual que la sociedad progresa con el devenir tecnológico, el ámbito penal no puede ser diferente y debe adaptarse para no quedar rezagado. De lo contrario, correremos el riesgo de quedar obsoletos frente al dinamismo inherente al desarrollo de la sociedad contemporánea.

Por consiguiente, en el contexto del proceso penal, la Inteligencia Artificial (IA) podría erigirse como un aliado de suma importancia para los profesionales del derecho y los funcionarios de la Administración de Justicia, al ofrecer una respuesta más eficiente, reducir los tiempos de procesamiento y elevar el nivel de objetividad jurídica, lo cual redundaría en una mejora sustancial de la calidad de las decisiones judiciales. Es crucial recalcar que esta integración debe ser concebida desde una óptica de complementariedad, no de sustitución, del juicio humano. Con base en la información proporcionada por estos sistemas, una vez perfeccionados y normalizados en su uso, el magistrado estará en condiciones de fundamentar y motivar su fallo con mayor solidez, respetando siempre sus propias convicciones, conocimientos y valores, y manteniendo una vigilancia constante sobre los posibles sesgos inherentes a estas tecnologías.

7. BIBLIOGRAFÍA

- CUATRECASAS MONFORTE, C. *"La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional"*. La Ley, Madrid, España, 2022
- AGUINAGA BARTOLOMÉ, A., "La Inteligencia Artificial en el proceso penal. Especial referencia al reconocimiento facial". 2022
- ALONSO SALGADO, C, "Acerca de la inteligencia artificial en el ámbito penal: especial referencia a la actividad de las fuerzas y cuerpos de seguridad", *IUS ET SCIENTIA*, vol. 7 (2021).
- SAN MIGUEL CASO, C., "Inteligencia Artificial y algoritmos: la controvertida evolución de la tutela judicial efectiva en el proceso penal". *Estudios Penales y Criminológicos.* Vol. 44 Núm. Ext 2023. https://doi.org/10.15304/epc.44.8859
- MURILLO FUENTES, J.J., ¿"Qué es lo que no funciona en los algoritmos de inteligencia artificial?" en COLOMER HERNÁNDEZ, I. (Dir.), Uso de la información y de los datos personales en los procesos: los cambios en la era digital, Cizur Menor, 2022.

- COTINO HUESO, L. Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos, 2023.
- SÁNCHEZ SÁEZ, A.J. El posible uso de la inteligencia artificial en el ámbito judicial: el contexto jurídico español y europeo. Especial referencia al contencioso-administrativo. *Rivista Italiana de Informativa e Diritto: periodico internazionale del CNR-IGSG, 2,* 2023.

- BORGES BLÁZQUEZ, R., "El sesgo de la máquina en la toma de decisiones en el proceso penal", Revista Ius et Scientia, núm. 2, vol. 6, 2020

- BARONA VILAR, S.: "Inteligencia artificial o a la algoritmización de la vida y de la justicia: ¿solución o problema?". Revista Boliviana de Derecho, Núm. 28 (2019),

- SÁNCHEZ VILANOVA, M. "El uso de algoritmos predictivos en el derecho penal. A propósito de la sentencia de la corte de justicia del distrito de la Haya (Países Bajos) sobre RyRI, de 5 de febrero de 2020. *Teoría & Derecho. Revista de Pensamiento jurídico, (33),* 2022. https://doi.org/10.36151/TD.2022.059

- PÉREZ, E." El reconocimiento facial de Mercadona acaba en multa de 2,5 millones de euros: qué dice la Agencia de Protección de Datos y qué lecciones se pueden extraer". 2021. El reconocimiento facial de Mercadona acaba en multa de 2,5 millones de euros: qué dice la Agencia de Protección de Datos y qué lecciones se pueden extraer (xataka.com)

- FREIRE MONTERO, A. F. El reconocimiento facial como instrumento de investigación y prevención del delito. *Anuario Da Facultade de Dereito Da Universidade Da Coruña/Anuario Da Facultade de Dereito Da Universidade Da Coruña,* 2022. https://doi.org/10.17979/afdudc.2022.26.0.9145

- HAO, K. "Caso práctico: probamos por qué un algoritmo judicial justo es imposible". Noviembre de 2021. Caso práctico: probamos por qué un algoritmo judicial justo es imposible | MIT Technology Review en español

- MARTÍN, L "La fórmula de Blackstone. Grietas de miseria moral e insolidaridad resquebrajan hoy la sociedad española". Abril de 2013. La fórmula de Blackstone | Opinión | EL PAÍS (elpais.com)

- MARTÍNEZ GARAY, L. "Peligrosidad, algoritmos y *due process*: el caso *state vs loomis*". *Universidad de Valencia. Revista de Derecho Penal y Criminología,* núm 20 (julio de 2018

NORMATIVA

- Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 21 de abril de 2021. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)
- Constitución Española. BOE 311. 29 de diciembre de 1978. Constitución Española. (boe.es)
- Ley de Enjuiciamiento Criminal (LECrim). 14 de septiembre de 1882.BOE-A-1882-6036 Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.
- Grupo de trabajo del artículo 29. Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, pág. 6 Draft outline for WP29 opinion on "consent" (europa.eu)
- 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) Diario Oficial de la Unión Europea, p.34. 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) (boe.es)
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE BOE.es - DOUE-L-2018-81849 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE

- Directiva (UE) 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 parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DIRECTIVA (UE) 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 parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/ 977/ JAI del Consejo (boe.es)

- LIBRO BLANCO sobre la inteligencia artificial -un enfoque europeo orientado a la excelencia y la confianza. Bruselas, 19 de febrero de 2020. EUR-Lex - 52020DC0065 - EN - EUR-Lex (europa.eu)
- Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros.BOE.es - DOUE-L-2002-81377 Decisión Marco del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (2002/584/JAI).