IUS ET SCIENTIA
2024 • Vol. 10 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2024

La justicia y el proceso penal en clave algorítmica. Nuevos enfoques, nuevos riesgos*

JUSTICE AND THE CRIMINAL PROCESS IN ALGORITHMIC KEY. NEW APPROACHES, NEW RISKS

Sílvia Pereira Puigvert
Universidad de Girona
silvia.pereira@udg.edu 0000-0002-8142-1506

Recibido: 17 de septiembre de 2024 | Aceptado: 09 de diciembre de 2024

RESUMEN

De los múltiples aspectos con que se puede abordar la inteligencia artificial (en adelante, IA), este artículo se sustenta en una breve panorámica sobre la digitalización del proceso penal y la justicia predictiva y sus riesgos. Porque se habla de predicciones algorítmicas e IA predictiva como la gran estrella emergente. Las predicciones algorítmicas se van perfeccionando y vivimos en una era digital, inmersos en una máquina digital. La revolución informática, que comenzó a finales del siglo pasado, se ha desbocado con la creciente potencia de los ordenadores y los métodos de aprendizaje profundo que engullen el imparable aumento de datos y nutren los algoritmos predictivos. Y los retos o desafíos son múltiples. Ya hay muchas alertas: se empezó por troyanos y piratas informáticos, pero ahora existen prácticas preocupantes de adquisición de datos por reconocimiento facial, por ejemplo. En las próximas líneas, intentaremos dar cabida a todas estas cuestiones.

PALABRAS CLAVE

Inteligencia artificial
Justicia predictiva
Sistemas predictivos
Reconocimiento facial
Garantías procesales
Proporcionalidad

ABSTRACT

Of the many aspects with which artificial intelligence (hereinafter AI) can be approached, this article is based on a brief overview of the digitization of the criminal process and predictive justice and its risks. Because algorithmic predictions and predictive AI are talked about as the big rising star. Algorithmic predictions are getting better and better, and we live in a digital age, immersed in a digital machine. The computing revolution, which began at the end of the last century, has run amok with increasing computing power and deep learning methods that gobble up the unstoppable increase in data and nurture predictive algorithms. And the challenges are manifold. There are already many alerts: it started with Trojans and hackers, but now there are worrying practices of data acquisition by facial recognition, for example. In the following lines, we will try to address all these issues.

KEYWORDS

Artificial intelligence
Predictive justice
Predictive systems
Facial recognition
Procedural guarantees
Proportionality

I. Consideraciones preliminares sobre la digitalización, la inteligencia artificial y el proceso penal: «algorithmic process»

Catalogar y reconocer imágenes, traducir o escribir textos, incluso de gran complejidad, realizar diagnósticos o pronósticos médicos, pilotar drones, aviones o coches, son sólo algunas de las actividades que realizan hoy en día los «agentes artificiales». Y es precisamente la constatación de esto lo que ha llevado a afirmar que ya vivimos en «sociedades algorítmicas» (Barona Vilar, 2021), es decir, organizadas en torno a la toma de decisiones automatizada por herramientas digitales.

En este escenario, era inevitable que el mundo del derecho también se viera afectado por la revolución informática o la cuarta revolución industrial o industria 4.0 (denominación usada por el fundador del Foro Económico Mundial). Por un lado, cada vez son más los ordenamientos jurídicos nacionales y supranacionales que, igualmente para seguir siendo competitivos a nivel global, han comenzado a preparar estrategias articuladas de intervención en el crucial ámbito de la IA, dirigidas a sentar las bases de su regulación. En este sentido, no hay más que pensar en la «agenda digital», fijada por la Unión Europea a partir de 2018, culminada con la «histórica» aprobación del *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen las primeras normas armonizadas de la Unión Europea en este ámbito*.

Por otro lado, en la última década también se ha intensificado el debate más general sobre el uso de herramientas digitales para hacer más eficiente el trabajo de los profesionales de la justicia, públicos y privados. Desde una perspectiva supranacional, cabe fijarnos en el Plan de Acción 2022-2025 de la CEPEJ sobre la *Digitalisation for a better justice*, que se propone el ambicioso objetivo «*to accompany States and courts in a successful transition towards digitalisation of justice in line with European standards*».

Como es sabido, el sistema penal no escapa a este fenómeno, sino todo lo contrario. Junto al discutido campo de la justicia predictiva, hay dos ámbitos en los que la innovación tecnológica se está desarrollando de forma más tumultuosa.

El primero es el de la llamada prueba digital o prueba electrónica[1]: es notorio que hoy en día existe un uso cada vez más masivo de medios tecnológicos de obtención de pruebas (basta con pensar en la importancia que asumen diligencias como las intervenciones de comunicaciones, telefónicas o telemáticas, con o sin virus informáticos, o la captación de datos externos a las comunicaciones), basados también en la IA (y aquí cabe mencionar el uso cada vez más frecuente de algoritmos de reconocimiento biométrico), que se están convirtiendo poco a poco en la *regina probatorum* del siglo XXI.

* El presente trabajo se enmarca en el Proyecto Nacional de I+D+I (PID2020-112683GB-I00). «Nueva Ley de Enjuiciamiento Criminal ¿Nuevo modelo? Adaptaciones transformativas». Asimismo, forma parte de la investigación realizada en el marco de la financiación concedida por la Fundación Privada Manuel Serra Domínguez (VIII Convocatoria de ayudas).

1. Son numerosas las locuciones utilizadas por la doctrina española (y de otros países): «prueba telemática», «prueba cibernética», «prueba tecnológica», «prueba electrónica», o «prueba digital».

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

El otro ámbito de elección es la informatización de los procesos penales. Especialmente tras el estallido de la pandemia COVID-19, que aceleró notoriamente de forma exponencial la senda de la innovación tecnológica en todos los sectores de la justicia, además de ofrecer la posibilidad de archivar y, en ciertos casos, de consultar actos, documentos y peticiones por medios telemáticos, se han digitalizado, total o parcialmente, incluso etapas fundamentales del proceso penal, como las audiencias. En poco tiempo, hemos asistido a la aparición transversal, tanto en los países de derecho romano-germánico como en los de *common law,* del «embrión» de un rito penal totalmente nuevo, porque ya no se celebra en el mundo físico de las salas de audiencia, sino en el virtual[2].

Teniendo en cuenta lo que se acaba de observar, es fácil comprender por qué el nivel de digitalización del sector penal representa actualmente uno de los parámetros tomados en consideración por las instituciones europeas para evaluar el «estado de salud» de los sistemas jurídicos nacionales. Esto se explica por el hecho de que las nuevas tecnologías son indudablemente capaces de hacer más «virtuoso» el proceso penal (Galgani, 2022), no sólo desde el punto de vista de la lucha contra la delincuencia, permitiendo un mejor control del territorio y la obtención de evidencias que de otro modo serían inaccesibles, sino también desde otras perspectivas, entre las que se encuentran las de la salvaguarda de la duración razonable de los procesos y el acceso a la justicia. En efecto, las *Information and communications technologies (ICT)* son capaces no sólo de agilizar la realización de múltiples actividades judiciales y de reducir los tiempos muertos de la justicia (piénsese en el tiempo que se ahorran al no tener que transportar físicamente los documentos entre las distintas oficinas judiciales), sino también de permitir a las personas acudir más fácilmente al sistema judicial para hacer valer sus derechos.

El problema es que la transición digital no sólo tiene luces, sino también sombras. La pandemia COVID-19, en particular, nos lo ha enseñado: si bien es cierto que las aplicaciones digitales han sido esenciales para evitar que la emergencia sanitaria paralizara totalmente los procedimientos, también lo es que han supuesto, en varias jurisdicciones, una reducción del estándar de protección de las garantías objetivas y subjetivas.

En esta dirección, hay que dar cuenta de la injerencia que los medios tecnológicos de obtención de pruebas son capaces de tener en un gran número de derechos fundamentales de la persona, como son los de libertad y secreto de las comunicaciones, respeto a la vida privada y protección de datos de carácter personal, a los que, en lo que se refiere a los *tools* de última generación basados en IA, hay que añadir también los de no discriminación, igualdad de las partes, contradicción, presunción de inocencia, e incluso el principio primario de la dignidad humana (Armenta Deu, 2021; Gialuz-Quattrocolo, 2023).

Tampoco hay que pasar por alto que la circunstancia de que las máquinas sean potentísimos «hidratadores de datos» permite, asimismo, transformarlas en estimulantes herramientas de «vigilancia masiva» (Della Torre, 2020). En efecto, aplicando una

2. Artículo 258 bis LECrim, introducido por el Real Decreto-ley 6/2023, que regula la celebración de actos procesales mediante presencia telemática.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

herramienta de reconocimiento biométrico a la red de cámaras colocadas en todas nuestras calles y edificios, así como captando la información que cada uno de nosotros difunde en el mundo digital, es posible controlar, de manera capilar, la vida de las personas. Tampoco cabe pensar que estos peligros sólo se aplican a los Estados autoritarios: el reciente escándalo *Clearview*, que ha barrido a ambos lados del Atlántico, demuestra, por otra parte, que incluso en las democracias occidentales la posibilidad de que se hagan realidad escenarios *orwellianos* está de plena actualidad.

Aun así, la IA ha pasado a suscitar un interés desbordante. Las noticias inundan los periódicos, los artículos y libros son inagotables. Y con todo, la sensación es de tremenda ignorancia. El avance es imparable y la realidad supera la ficción (lo veíamos con el *film Minority Report*). Pero es que, además, parece no tener «techo suficiente». En Colombia ya se ha celebrado la primera audiencia en el metaverso. Algo que nos puede causar sorpresa, expectación, incertidumbre, respeto, miedo y, efectivamente, ignorancia. Podemos pensar que el derecho se ha quedado un paso atrás ante la IA, pero el derecho ha acompañado en paralelo la evolución de las nuevas tecnologías, estudiando sus efectos y promoviendo su desarrollo, lo cual nos puede generar cierto alivio o tranquilidad.

II. Sistemas o algoritmos de análisis predictivo

Al hilo de lo dicho en último lugar, la larga marcha de la IA ha «desbordado» el sector penal hasta tal punto que ha encontrado aplicaciones transversales desde la fase de prevención del delito, al procedimiento penal de cognición, e incluso al derecho penitenciario. La analítica predictiva se ha vuelto altamente rentable para la economía y ha invadido todo el tejido social (control de tráfico; trasplantes y muchos otros aspectos médicos; control por perfiles para fronteras; prevención de conductas delictivas, o penas conforme a lecturas predictivas).

Los sistemas predictivos son instrumentos que se basan en la utilización de un gran número de datos (la conocida expresión *minería de datos*), de carácter personal y de otra tipología que, convenientemente procesados a través de algoritmos *ad hoc*, proporcionan unos resultados que pueden servir para predecir el posible comportamiento de una persona en distintos contextos. Pueden ayudar a determinar un peligro de reincidencia delictiva; de revictimización; el grado de incumplimiento de obligaciones procesales; el grado de incumplimiento de las condiciones que puedan imponerse con carácter cautelar en una causa, o en la fase de ejecución de sentencias (Pereira Puigvert, 2024).

Llegados aquí, ya pueden imaginarse lo que citaré a continuación. En cualquier trabajo de justicia predictiva que se precie se habla del caso *Loomis* que ha servido, a partes iguales, para observar la aplicación práctica de este tipo de herramientas de IA (en USA) para predecir comportamientos futuros y evidenciar o demostrar los riesgos de usar los resultados de esta aplicación de algoritmos sin las garantías suficientes, en particular en el proceso penal. En el asunto *Loomis*, se utilizaron las predicciones de *COMPAS*.

El uso de instrumentos de evaluación del riesgo o prevención de delitos no es exclusivo de Estados Unidos de América. Veámoslo.

IUS ET SCIENTIA • 2024
Vol. 10 • N° 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

2.1. La IA y la prevención del delito de medio ambiente

Para empezar, seguiremos el titular de una noticia periodística: «Así trabaja el equipo de Interior (del Ministerio) que predice el perfil de los asesinos»[3], con motivo de la desaparición (y posterior muerte) en Almería del niño Gabriel Cruz. Una vez esclarecido el suceso, en la Secretaría de Estado de Seguridad decidieron probar un *software* predictivo introduciendo determinadas características relacionadas con el pequeño Gabriel: varón; menor de 10 años; perfil familiar; circunstancias de la desaparición. El programa predictivo devolvió que el sospechoso más probable era mujer y cercana a la familia. A Gabriel Cruz lo mató, recordarán, Ana Julia Quezada, pareja de su padre.

La misma noticia no solamente se refería a delitos de homicidio y asesinato, sino también al caso de los pirómanos forestales. Únicamente un 1% de los incendios provocados en España se esclarecen. Por lo tanto, quedaba claro que hay que emplear otros sistemas que mejoren estos resultados. En este sentido, el conocido Fiscal de Medio Ambiente, Antonio Vercher, firmó un acuerdo con el Departamento de Matemáticas de la UAB para avanzar en el desarrollo de un modelo predictivo del pirómano forestal. Como con los homicidios, el modelo es capaz de predecir las características más probables del autor a partir de las del incendio y aprende o se perfecciona, como siempre, según aumenta la base de datos. En el proceso de validación se hizo una estimación de la tasa de acierto que rondaba el 55%. Además, este modelo predictivo ya ha competido contra humanos. Se seleccionaron 10 casos resueltos y un grupo de humanos experto en perfilado de incendiarios. A todos se les dieron las características de los incendios y debían acertar los rasgos de los autores. La conclusión es que el porcentaje de acierto de los expertos fue del 40% y del modelo predictivo, un 60%.

Con anterioridad, en 2006, a raíz de una serie de incendios forestales ocurridos en Galicia, la Guardia Civil impulsó un estudio sobre los perfiles del incendiario forestal (en colaboración con la fiscalía). Para ello, se dispuso que los agentes de las Unidades policiales encargadas del esclarecimiento de estos delitos, a lo largo de todo el territorio nacional, cumplimentaran online un cuestionario psicosocial cada vez que detuvieran a un incendiario, complementario a las diligencias policiales. Con esta información se llegó a programar un sistema predictivo utilizando redes bayesianas que documenta de las características más probables de un incendiario desconocido a partir de los indicios hallados en el foco del incendio, para ayudar a los agentes a su localización e identificación.

Los delitos medioambientales son todos aquellos actos que intencionalmente, en forma accidental o negligente, producen como consecuencia la destrucción o menoscabo de ciertos sistemas naturales, especies animales o vida vegetal cuya protección es considerada valiosa para el hombre para mantener sus condiciones de vida, salud, actividades económicas o culturales. En España, ya desde el Código Penal de 1995, y en particular con las reformas del 2010, se protegen los componentes ambientales tipificando el delito de contaminación de aguas, e se han incorporado delitos contra el aire, el suelo, por ruidos, vertidos y manejo indebido de sustancias peligrosas, así como

3. Titular extraído del siguiente enlace: https://elpais.com/tecnologia/2019/06/26/actualidad/1561500733_085160.html (última fecha de consulta 19/11/2024).

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

sus principales formas de manifestación, como los animales y vegetales. Se incluyen, además, algunos delitos adicionales como la sanción al funcionario público que concediera una licencia incumpliendo sus deberes de revisión exhaustiva previo a la autorización de funcionamiento de una fuente emisora, o bien, sus labores de fiscalización; y una regla de imposición de pena para las personas jurídicas. La reforma al CP del 2015, por la LO 1/2015, de 30 de marzo, reforzó esta tendencia.

Existe una problemática en torno al bien jurídico protegido en cuestiones ambientales.

El bien jurídico debe protegerse cuando estemos frente a una afectación, pero que esta, por su parte, no necesariamente debe suponer la lesión de un interés personal, sino que puede bastar con que cause un peligro para estos intereses. A mayor abundamiento, cuando el daño causado al medioambiente sólo afecta a un conjunto indeterminado de personas y no existe un daño individual o colectivo, la detección de los delitos contra el medioambiente es más complicada para los órganos penales. Sin embargo, cuando la acción típica ha causado daños a un grupo determinado –o fácilmente determinable de personas– serán estas las que pongan el hecho delictivo en conocimiento de la Policía Judicial, el Ministerio Fiscal o el órgano de instrucción (Marrero Guanche, 2021).

Otras dificultades son que, en general, estos delitos ocurren en contextos abiertos, que por sus propias características van eliminando evidencias y/o ampliando el impacto ocasionado a los ecosistemas y/o sujetos (Luaces Gutiérrez-Vázquez-González, 2014). Se han llevado a cabo medidas de agilización como que, en atención a la complejidad inherente a este tipo de delitos (incendios forestales) y la necesidad de desarrollar una investigación lo más rápida posible, se ha desviado la instrucción y enjuiciamiento de los incendios a tribunales profesionales, dejando sin efecto la competencia que tenía el Tribunal del Jurado.

Una lesión al medio ambiente, lo acabamos de comprobar, puede afectar a toda una colectividad, circunstancia que hace que la detección, persecución y enjuiciamiento de este tipo de delitos resulte especialmente compleja. Con técnicas o sistemas de IA puede mejorarse esta situación o, como mínimo, predecir y prevenir posibles conductas delictivas. En suma, soslayar las dilaciones indebidas en el proceso penal medioambiental.

2.2. La IA en la lucha contra la violencia de género: VioGén

En 2004, como es conocido, se promulgaba la *Ley Orgánica de Protección Integral contra la violencia machista e indiscriminada contra las mujeres*. Con esta ley, aparecen los Juzgados especializados en violencia contra la mujer y, unos años más tarde, *el sistema de VioGén*.

VioGén es una plataforma, constantemente actualizada, que integra tecnológicamente toda la información sobre un caso o una víctima, que procede de una doble fuente: por un lado, declaraciones de la víctima y de testigos, de registros oficiales, de antecedentes policiales y registros accesibles para la policía, y por otro lado, hechos como la existencia de vejaciones, insultos, humillaciones, violencia; buscando valorar el nivel de riesgo de sufrir nuevas agresiones o una escalada en la gravedad o la frecuencia (Llorente Sánchez-Arjona, 2022).

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

Entre sus objetivos, a) aglutinar a las diferentes instituciones públicas que tienen competencias en materia de violencia de género; b) integrar toda la información de interés que se estime necesaria; c) hacer predicción del riesgo; d) atendiendo al nivel de riesgo, realizar seguimiento y protección a las víctimas en todo el territorio nacional; e) efectuar una labor preventiva, emitiendo avisos, alertas y alarmas, cuando se detecte alguna incidencia que pueda poner en peligro la integridad de la víctima.

Por otra parte, el resultado que arroja la máquina es fruto de la recopilación, por parte del funcionario policial y sobre la base de las circunstancias denunciadas por la víctima, de dos formularios, a través de los que se aprecia la estrecha correlación con el caso concreto y la ausencia de cualquier parámetro discriminatorio.

El primero de los formularios, *la valoración policial del riesgo de reincidencia de violencia* entra en juego inmediatamente después de la presentación de la denuncia y tiene la función de cuantificar el grado de probabilidad de que la persona pueda seguir siendo objeto de acoso. El formulario incluye 39 indicadores de riesgo de reincidencia, agrupados en cuatro áreas temáticas (relacionadas con la gravedad del incidente denunciado, los datos del presunto agresor, las características de la víctima y la percepción de la situación por parte del agresor), y permite clasificar *el peligro como inexistente, bajo, medio, alto o extremo.* Esta clasificación va seguida de la adopción de determinadas medidas de protección que, en los supuestos más graves, pueden llevar incluso a la elaboración de un plan de seguridad personalizado, sugerido por el propio VioGén.

El segundo, *la valoración policial de la evolución del riesgo*, consta de 34 indicadores de riesgo de reincidencia y 9 factores de protección. Está diseñado para reevaluar la peligrosidad estimada inicialmente y, por tanto, para ajustar, reforzándose o flexibilizándose, según el caso, las medidas adoptadas.

En esencia, por consiguiente, estas predicciones se llevan a cabo de forma tradicional, sin que para realizar estos juicios de probabilidad se empleen programas informáticos expresos. Las Fuerzas y Cuerpos de Seguridad han recurrido al protocolo de valoración policial del riesgo que es el núcleo de VioGén (Martín Ríos, 2024). Nuestro ordenamiento, para combatir el fenómeno de la violencia de género, ha puesto en marcha una herramienta de evaluación de riesgos cuya utilización en este ámbito concreto parece «tan prometedora» que ha sido acogida con gran satisfacción por el órgano encargado de supervisar la aplicación del Convenio de Estambul por los Estados miembros del Consejo de Europa –el GREVIO–, que, en su informe dedicado a España, sugería incluso la adopción de medidas para incrementar su potencial (Agostino, 2024).

Ahora bien, de un tiempo a esta parte, las críticas del sistema VioGén han comenzado a aflorar. Así lo constata por primera vez la Sala de lo Contencioso Administrativo de la Audiencia Nacional que condenó al Ministerio del Interior español a indemnizar a la familia de una mujer asesinada sólo un mes después de denunciar a su marido por actos violentos. En aquella ocasión, la autoridad policial no había adoptado ninguna medida de protección a favor de la víctima basándose en la indicación del dispositivo de que disponía, que había calificado de «bajo» el peligro al que estaba expuesta, sin tener en cuenta, sin embargo, toda una serie de índices fácticos –entre ellos, los antecedentes y las condiciones socioeconómicas del agresor– que podían y debían haberle llevado a asignar al caso un nivel de riesgo superior (Llorente Sánchez-Arjona, 2022). Igualmente, la Fundación Éticas realizó una auditoría externa de VioGén (en 2021) y las conclusiones

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

fueron bastante negativas, destacando la falta de transparencia o la generación de posibles sesgos[4].

III. Algoritmos de reconocimiento biométrico/facial: más y mayores problemas

Desarrollados principalmente en el contexto de Estados Unidos (y siendo de uso abusivo por muchos Estados no democráticos a nivel mundial), *las tecnologías de reconocimiento facial automatizado*, basadas en la inteligencia artificial, que permiten la identificación automática de un individuo comparando una fotografía o un vídeo de su rostro con las imágenes contenidas en una base de datos de referencia, también empiezan a ser una realidad en muchos países europeos, como España, Italia, Reino Unido o Alemania.

Para que el reconocimiento facial sea efectivo se llevará a cabo un tratamiento de datos calificados como *biométricos*. Con la intención de ir aclarando conceptos, los datos biométricos, según el Reglamento General de Protección de Datos (UE), son aquellos 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. Esta tecnología disruptiva puede emplearse para diferentes tipos de fines, incluidos los juicios o audiencias telemáticas (Pesqueira Zamora, 2021). A título indicativo, el ejército ucraniano utilizó el *software* de reconocimiento facial automatizado de la empresa estadounidense *Clearview AI* (antes mencionado) para reconocer a las múltiples víctimas del conflicto bélico que, de otra forma, no podrían haber sido identificadas o hubiese requerido de un esfuerzo titánico. O el proyecto piloto, como posible alternativa a la prisión provisional, instaurado por el Gobierno de las Islas Canarias (España), en sus juzgados de instrucción, y que parte de un sistema remoto desarrollado con éxito en otros sectores como el bancario, aeronáutico o de control de fronteras. La persona compareciente verifica su identidad mediante cualquier documento válido y genera su credencial biométrica a través de reconocimiento facial. Una vez generada, se usa para verificar su identidad a distancia acompañada de una geolocalización que permite comprobar que la persona se encuentra en el territorio que debe permanecer. Y, por supuesto, otra finalidad es la prevención de conductas delictivas y en beneficio de la investigación criminal como lo que veníamos describiendo en epígrafes anteriores.

Por lo que respecta al funcionamiento del reconocimiento facial, en general y de la misma manera que ocurre con otras tecnologías basadas en la biometría, tras una primera fase de adquisición de los datos biométricos constituidos por la imagen de un rostro humano, la herramienta extrapola determinadas características de la cara tales como la posición de los ojos, de la nariz, de las fosas nasales, de la barbilla y de las orejas, que permiten la creación de un *template* o «modelo biométrico» (Borgia, 2022). Seguidamente, este modelo se compara con los datos archivados en una base de datos de referencia (que puede ser desde una base típica de permisos de conducir

4. Pueden verse las conclusiones con mayor detalle en: https://www.elconfidencial.com/tecnologia/2024-08-10/inteligencia-artificial-violencia-de-genero_3938835/ (última fecha de consulta 19/11/2024).

IUS ET SCIENTIA • 2024
Vol. 10 • N° 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

hasta información proveniente de redes sociales y que puede resultar algo más controvertido o invasivo) y, en el supuesto de que de la operación resulte, con cierta probabilidad, que las dos imágenes se refieren a la misma persona, se produce el denominado *matching*. Con mayor precisión, según el Libro Blanco de IA, mientras que la identificación consiste en que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella; la autenticación o verificación, por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; en consecuencia, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma.

Se trata de instrumentos que inevitablemente fascinan a las autoridades de *law enforcement* y que, por tanto, están destinados a repercutir en el proceso penal. De hecho, hay que tener presente, en primer lugar, que el rostro es algo difícil de ocultar y fácil de observar en espacios públicos[5].

En comparación con otras técnicas de identificación biométrica, como las centradas en el ADN, el reconocimiento facial automatizado tiene la ventaja de no requerir la cooperación de la persona captada. Además, la aplicación de las tecnologías de reconocimiento facial automatizado está facilitada por la posibilidad de utilizar las redes de cámaras preexistentes[6]. Por último, cabe señalar que los softwares que, por así decirlo, funcionan en tiempo real, son cada vez más comunes y también pueden instalarse en dispositivos móviles, como *body cameras* o *drones* (Ortiz Pradillo, 2021). El llamado modo de funcionamiento *real time* permite saber inmediatamente si un individuo sospechoso de haber cometido o incluso de ser susceptible de cometer un delito se encuentra en el lugar bajo observación.

No obstante, existe «la otra cara de la moneda», ya que el uso de estas tecnologías no es «sin coste» para los derechos y libertades fundamentales, empezando por el derecho a la intimidad y la protección de datos personales afectados por las llamadas «tecnologías de control» (Pereira Puigvert, 2019) hasta todos aquellos derechos procesales que suelen verse comprometidos por el uso de sistemas de inteligencia artificial como la presunción de inocencia, la igualdad de armas, el derecho de contradicción y el derecho a la tutela judicial efectiva (Schumann Barragán, 2021). Surge así la necesidad, por un lado, de limitar el uso de estos instrumentos respetando el principio de proporcionalidad (Borgia, 2022) y, por otro, de permitir una contradicción efectiva también y sobre todo desde el punto de vista técnico (Galgani, 2019).

Frente a estos peligros, ningún Estado ha adoptado una normativa específica que, al regular la materia, pretende ante todo salvaguardar los mencionados derechos fundamentales. La tendencia en algunos Estados miembros de la UE, aunque con lagunas importantes, es incluir el uso de estos dispositivos de reconocimiento facial en el ámbito de las actividades de videovigilancia que, si se realizan en lugares públicos, y tal y como

5. Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (and Beyond), p. 2, de la New York City Bar Association.

6. Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (and Beyond), p. 2, de la New York City Bar Association.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

opina la doctrina constitucionalista, el derecho a la intimidad personal no se constriñe al ámbito doméstico o privado, sino que despliega su eficacia también en la esfera pública, afectando al derecho a la intimidad, pero no lo vulneran al estar prevista legalmente su utilización y su exención (Ortuño Rodríguez, 2019).

En España, en virtud de la Exposición de Motivos de la LO 13/2015, la experiencia demuestra que, en la investigación de determinados delitos, la captación y grabación de comunicaciones orales abiertas (también de imágenes), mediante el empleo de dispositivos electrónicos, puede resultar indispensable al mismo tiempo que alarmante para la tutela de los derechos fundamentales. En el artículo 588 quinquies a) de la Ley de Enjuiciamiento Criminal, se permite a través de cualquier medio técnico la captación de imágenes de la persona investigada en lugares o espacios públicos sin necesidad de que la Policía Judicial solicite autorización judicial (el derecho a la intimidad no se ve tan afectado como cuando se autoriza la grabación de las comunicaciones orales). En definitiva, la videovigilancia como diligencia de investigación independiente no necesita autorización judicial, y cuando es complemento de la grabación de comunicaciones orales directa es necesaria, entonces, la autorización judicial.

Después de todo, la idea de que toda filmación de imágenes en lugares públicos puede considerarse neutra desde el punto de vista de los derechos y libertades de las personas implicadas también se desprende de una disciplina *ad hoc* entre las más avanzadas en materia de garantías, como es la española tras las modificaciones introducidas en la LECrim por esta LO 13/2015[7].

Más allá de la LECrim y la reforma operada en 2015, el único intento de regular inte-

gralmente la materia se debe a la Unión Europea con el Reglamento sobre Inteligencia Artificial, que ciertamente merece el crédito de haber colocado estas actividades entre las de alto riesgo para los derechos y libertades de las personas involucradas. Ya, con anterioridad, la UE ha otorgado un interés, más que considerable, a las nuevas tecnologías en documentos como el «Proyecto de conclusiones del Consejo relativas al Plan coordinado sobre el desarrollo y uso de inteligencia artificial», preparado por la Presidencia de la Comisión UE en 2019 o el Libro Blanco IA (Borgia, 2024).

En concreto, *la letra h) del apartado 1 del artículo 5 del Reglamento IA* establece, en primer lugar, la prohibición general del uso con fines policiales de sistemas de identificación biométrica en tiempo real en lugares accesibles al público. El artículo reza como sigue: quedan prohibidas las siguientes prácticas de IA, "el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

7. En otros países, como Italia, hay que tener en cuenta el dictamen negativo emitido por el *Garante nazionale per la protezione dei dati personali* sobre el «*SARI-Real Time*». En la documentación ministerial, se alega que la utilización de este instrumento está permitida, entre otros, por los artículos 55 y 348 del *Codice di Procedura Penale,* relativos a las funciones y prerrogativas generales otorgadas a la Policía Judicial, así como por el artículo 234, en sede de prueba documental, al que hay que remitirse para la obtención de imágenes y vídeos en el juicio. Como ya se advertía, hay perplejidades o lagunas acerca de que las tecnologías del reconocimiento facial automatizado sean equiparables a la grabación de vídeo.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

a) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,
b) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,
c) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años".

La normativa europea continúa disponiendo que el uso de un sistema de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una *autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente* cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5 (artículo 5.3 Reglamento IA).

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le aporten, de que el uso del sistema de identificación biométrica remota en tiempo real es necesario y proporcionado para alcanzar alguno de los objetivos especificados (artículo 5.3 Reglamento IA).

IV. Reflexiones finales: aprovecharnos de la tecnología, pero con cautela... y algunos interrogantes

Por más que la analítica predictiva prometa objetividad y eficiencia y sea tentador fiarnos de algoritmos en lugar de depender de humanos falibles, cuanto más se transfiera sobre decisiones humanas a los algoritmos más poder concentrarán.

En efecto, el reto ineludible que nuestros sistemas jurídicos, pero más en general el sistema europeo, deberán afrontar en los próximos años es el de construir un «*algorithmic due process*», basado en las garantías consagradas en las numerosas cartas de derechos supranacionales. Sólo así será posible aprovechar las oportunidades que brindan las aplicaciones digitales, sin correr el riesgo de que acaben transformándose de medios útiles para aumentar la eficiencia de la justicia, en aplicaciones capaces de comprimir los derechos fundamentales más básicos de las personas.

Ante un escenario de reformas legislativas en las que hay un denominador común: eficiencia (procesal, organizativa, digital), el uso de sistemas de IA puede lograr su consecución. Hemos descrito experiencias disruptivas o predictivas con resultados significativos y óptimos. Pero, al mismo tiempo, hay fallos. Ni las máquinas están

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

exentas del error. Y hay errores que «pueden pagarse caros»: dejar en libertad un preso porque el algoritmo considera que no reincidirá y reincide o al revés. Se dice que la opacidad del algoritmo supone un riesgo para el derecho a la tutela judicial efectiva y la presunción de inocencia. Pero, según determinados autores, de un análisis de los distintos derechos subjetivos públicos que conforman el derecho a la tutela judicial efectiva o de defensa (art. 24 CE) no es evidente determinar qué concreta dimensión se vería vulnerada (Schumann Barragán, 2021).

Es evidente que delegar en una máquina conlleva un riesgo y es que el tratamiento automatizado de datos de la máquina, del algoritmo, acabe teniendo un peso relevante, determinante, dejando al margen otros factores en la toma de decisiones como el componente o control humano. Escribiendo este artículo, leía un trabajo sobre la *empatía* como motivación de las sentencias (Soba Bracesco, 2023) que ha sido utilizado en pronunciamientos de los tribunales de Uruguay (empatía como sentimiento o capacidad de ponerse en el lugar del otro, del litigante contrario). Las máquinas no tienen empatía ni sentido de la responsabilidad. Únicamente, los humanos pueden rendir cuentas y tener la libertad de asumir responsabilidades.

Aquí se abre otro debate (que ya ponía de manifiesto De la Oliva Santos, 2019), ¿de las decisiones erróneas de los algoritmos quién rinde cuentas?

Los riesgos de la IA pueden resumirse en: desinformación, sustitución humana y el propósito en sí mismo de la IA.

Por lo que respecta a la desinformación, los sistemas de inteligencia artificial contemporáneos ya compiten con los humanos en tareas generales, y debemos preguntarnos: ¿Debemos dejar que las máquinas inunden nuestros canales de información? ¿Debemos dejar que lo hagan con propaganda y falsedades?

Sobre la sustitución de los humanos: ¿Deberíamos automatizar todos los trabajos, incluidos los satisfactorios? ¿Deberíamos desarrollar mentes no humanas que con el tiempo nos superen en número, inteligencia, obsolescencia y reemplazo? ¿Deberíamos arriesgarnos a perder el control de nuestra civilización?. En cuanto al propósito de la IA, solamente deberían desarrollarse sistemas de IA potentes cuando estemos seguros de que sus efectos serán positivos y sus riesgos controlables. Entre otros aspectos preocupa hondamente los modelos de caja negra, impredecibles, cada vez más grandes y con capacidades emergentes[8].

Ante estos riesgos, debe instaurarse una regulación adecuada del uso de la IA, adaptada a las recomendaciones y directrices europeas (principalmente, el Reglamento sobre IA). El Reglamento IA parte de una clasificación de riesgos entre: a) *Riesgo inaceptable: prohibición*; b) *Sistemas de Alto Riesgo*; c) *Sistemas de Riesgo limitado,* comprendiendo sistemas sometidos a obligación de información al usuario de que está interactuando con un sistema de IA (robots, por ejemplo); y d) *Sistemas de Riesgo mínimo*, referidos a modelos que pueden desarrollarse conforme a la legislación vigente sin obligaciones jurídicas adicionales.

8. Reflexiones sacadas de la conferencia pronunciada por la Prof. Teresa Armenta Deu en la Universidad de Génova, junio de 2023, y titulada: *La inteligencia artificial entre la fe, el control del riesgo y la responsabilidad.*

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

Claro está que debemos aprovechar las ventajas de la IA y afrontar sus desafíos (que no son y serán pocos) a «golpe de normativa». No se trata de dar una visión de rechazo (nos estaríamos equivocando), pero hay que pasar a la acción normativa (Gascón Inchausti, 2022). Si existe regulación puede que no sea tan difícil la adaptación a los nuevos (y muy cambiantes) tiempos procesales.

Bibliografía

Agostino, L. (en prensa). «*Intelligenza artificiale e contrasto alla violenza di genere: spunti di riflessione a partire dall'esperienza in corso nell'ordinamento spagnolo*», en *Processi, rappresentazioni e piattaforme digitali*, dirigida por B. Galgani. Torino: Giappichelli. .

Armenta Deu, T. (2021). *Derivas de la justicia. Tutela de los derechos y solución de controversias en tiempos de cambio.* Madrid: Marcial Pons.

Barona Villar, S. (2021). *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*. Valencia: Tirant lo Blanch.

Borgia, G. (2022). «*Reconocimiento facial automatizado y derechos fundamentales en el proceso penal: entre las experiencias nacionales y la perspectiva de la Unión Europea*» en *Modernización, eficiencia y aceleración del proceso,* dirigida por Pereira Puigvert, S. y Pesqueira Zamora, M. J. Pamplona: Aranzadi, pp. 175-198.

Borgia, G. (2024). «*Biometría, evolución tecnológica y proceso penal: urge un cambio de ritmo en nombre de la proporcionalidad*» en *Retos de la prueba en el proceso actual,* coordinada por Della Torre, J. y Gimeno Beviá, J. y dirigida por Borgia, G. y Pereira Puigvert, S. Madrid: Aranzadi.

De la Oliva Santos, A. (2019). «Justicia predictiva», interpretación matemática de las normas, sentencias robóticas y la vieja historia del «Justizklavier». *El Cronista del Estado Social y Democrático de Derecho,* número 80, pp. 30-37.

Della Torre, J. (2020). Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della *High Court of Justice. Diritto penale contemporaneo – Rivista trimestrale,* número 1, pp. 231-247.

Galgani, B (2019). Giudizio penale, *habeas data* e garanzie fondamentali en *Archivio penale,* número 8 de febrero de 2019, pp. 1-32.

Galgani, B. (2022). *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale «virtuoso»*, Milano: Cedam.

Gascón Inchausti, F. (2022). «*Eficiencia procesal y sistemas de inteligencia artificial: la necesidad de pasar a la acción normativa*» en *Modernización, eficiencia y aceleración del proceso,* dirigida por Pereira Puigvert, S. y Pesqueira Zamora, M. J. Pamplona: Aranzadi, pp. 40-76.

Gialuz, M. y Quattrocolo, S. (2023). Predictive Justice in Italy. *Revue Internationale de Droit Pènal*, 195-210.

Llorente Sánchez-Arjona, M. (2022). Hacia una justicia penal predictiva. *Cuadernos de política criminal,* número 136, pp. 91-124.

Luaces Gutiérrez, A. I. y Vázquez González, C. (2014). La dilación del proceso penal medioambiental en España. *Revista de Derecho Penal y Criminología,* número 11, pp. 543-562.

Marrero Guanche, D. (2021). «*Inteligencia artificial e investigación de delitos contra el medioambiente*» en *Investigación y proceso penal en el s. XXI: nuevas tecnologías y protección de datos,* coordinada por Pesqueira Zamora, M. J. y dirigida por Pereira Puigvert, S. Pamplona: Aranzadi, pp. 541-556.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03

Martín Ríos, P. (2024). Predictive algorithms and criminal justice: expectations, challenges and a particular view of the Spanish VioGén system. *Rivista Italiana di Informatica eDiritto,* número 2, pp. 1-16.

Ortuño Rodríguez, A. E. (2019). Doctrina constitucional en relación con el control mediante cámaras de videovigilancia. *Cuadernos de Derecho Local,* número febrero, pp. 234-280.

Ortiz Pradillo, J. C. (2021). Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal. *Diario La Ley*, número 9955, Sección Doctrina.

Pereira Puigvert, S. (2019). «*Las medidas de investigación tecnológicas y su injerencia en la privacidad de las personas y la protección de datos personales*» en *Investigación y prueba en los procesos penales de España e Italia,* coordinada por Caro Catalán, J. y dirigida por Villar Fuentes, I. Pamplona: Aranzadi, pp. 297-307.

Pereira Puigvert, S. (2024). «*Justicia penal predictiva y medidas cautelares*» en *Next Generation Justice: Digitalización e Inteligencia Artificial*, dirigida por Calaza López, S. y Ordeñana Gezuraga, I. Madrid: La Ley.

Pesqueira Zamora, M. J. (2021). «*La inteligencia artificial aplicada al proceso: tratamiento del reconocimiento facial en los juicios virtuales*» en *Investigación y proceso penal en el s. XXI: nuevas tecnologías y protección de datos,* coordinada por Pesqueira Zamora, M. J. y dirigida por Pereira Puigvert, S. Pamplona: Aranzadi, pp. 463-486.

Schumann Barragán, G. (2021). «*La inteligencia artificial aplicada al proceso penal desde la perspectiva de la UE*» en *Investigación y proceso penal en el s. XXI: nuevas tecnologías y protección de datos,* coordinada por Pesqueira Zamora, M. J. y dirigida por Pereira Puigvert, S. Pamplona: Aranzadi, pp. 517-540.

Soba Bracesco, I. (2023). *La empatía en las sentencias judiciales y más allá. Blog de Derecho Procesal de Ignacio Soba.*

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 66-79
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.03