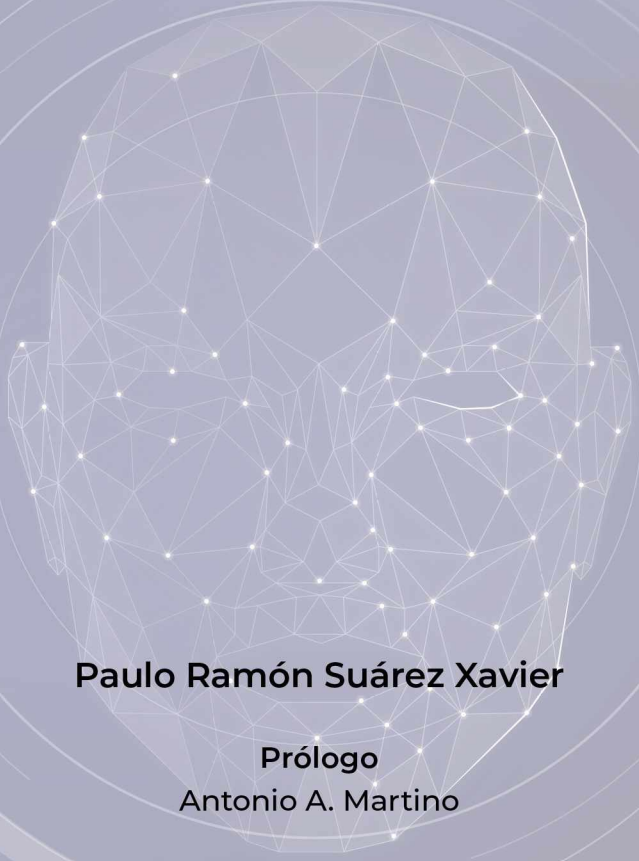
RECONOCIMIENTO FACIAL Y POLICÍA PREDICTIVA: ENTRE SEGURIDAD Y GARANTÍAS PROCESALES



Paulo Ramón Suárez Xavier

Prólogo
Antonio A. Martino

COLEX READER

eBook en www.colex.es

1.ª EDICIÓN

COLEX

RECONOCIMIENTO FACIAL Y POLICÍA PREDICTIVA: ENTRE SEGURIDAD Y GARANTÍAS PROCESALES

1.ª EDICIÓN

Paulo Ramón Suárez Xavier

COLEX 2022

Calle Costa Rica, número 5, 3º B (local comercial)
A Coruña, C.P. 15004
info@colex.es
www.colex.es

I.S.B.N.: 978-84-1359-409-5
Depósito legal: C 77-2022

SUMARIO

PRESENTACIÓN

La chispa encendida por los estudios de la máquina conceptual de Charles Babbage y los pioneros trabajos de Ada Lovelace sobre los distintos ámbitos de aplicación del artilugio de Babbage se ha cobrado proporciones globales.

La sociedad moderna, en este sentido, se ve sumergida en una interminable carrera tecnológica y de innovación que se manifiesta en los distintos ámbitos y de la vida social, política y económica, en un proceso denominado por algunos de digitalización o, por otros, de smartificación.

Sobejan estudios sobre los impactos de la implementación de estas tecnologías en el ámbito judicial y su entorno, pero apenas unos pocos alcanzan la multiplicidad de este fenómeno, cuyos impactos son tan distintos como lo son los ámbitos en los que se implementan dichas tecnologías.

En nuestro libro «Transformación Digital de la Administración de Justicia: viejos paradigmas, nuevos horizontes», señalábamos hacia la necesidad de clasificar las distintas esferas de aplicación de la inteligencia artificial en la Administración de Justicia. Se trata de una cuestión compleja, ya que también son complejas las relaciones que se establecen entre la Administración de Justicia, los justiciables y los organismos públicos.

Sin embargo, hay un ámbito de la Administración de Justicia cuya importancia y complejidad demandan la realización de estudios más específicos y profundizados: las políticas de seguridad pública.

Las políticas de seguridad pública o la seguridad interior tienen como premisa básica el hecho de que se realizan en colaboración entre las fuerzas y cuerpos de seguridad y las autoridades jurisdiccionales, por lo que la implementación de todo y cualquier recurso tecnológico debe tener en cuenta estas especificidades.

Por otro lado, es también en este ámbito donde nos encontramos con actuaciones que, por lo general, conllevan la restricción de derechos fundamentales, como el derecho de reunión pacífica y sin armas, el derecho a la libertad, el derecho a la intimidad personal y familiar o el derecho a la integridad física y moral.

En este sentido, comprendiendo la necesidad de realización de estudios más específicos sobre la implementación de la inteligencia artificial en la Administración de Justicia y su entorno, la presente obra aborda el uso de la IA en el ámbito de políticas de seguridad pública, mediante el uso de algoritmos predictivos: la policía predictiva.

Dicho concepto puede ser examinado desde dos formas. La primera forma, general, que busca estudiar los impactos del desarrollo y uso de este género de algoritmos y los impactos que pueden tener frente a los derechos fundamentales y la orientación deontológica impuesta por el legislador en el artículo 18 apartado 4 de la Constitución Española, referente a la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

La segunda manera de estudiar estos temas es, partiendo de una directriz general, examinar la aplicación de cada uno de los sistemas de policía predictiva que se vayan implementando, con especial consideración respecto a los derechos fundamentales y a la normativa del procedimiento específico que se esté automatizando por medio del algoritmo.

El presente estudio se centrará en la primera de las técnicas antes expuestas, si bien es verdad que abordará de forma más detenida un género específico de algoritmos empleado para procedimientos de identificación de personas mediante el reconocimiento facial.

Esta, sin embargo, no es más que la «punta del iceberg», ya que amén de todas las virtudes que pueden presentar los modelos algorítmicos aplicados en la Administración de Justicia y su entorno, existe una serie de riesgos que deben ser objeto de un análisis muy cuidadoso por parte de las autoridades públicas ya que también puede conllevar un regreso del determinismo penal, así como ocultar decisionismos enmascarados por un falso tecnicismo en la Administración de Justicia.

Así, como investigadores del Derecho y miembros de la sociedad, es tarea de todos y cada uno de nosotros traer a la superficie no solamente las ventajas, pero también los riesgos escondidos detrás del aparentemente inofensivo uso de estos sistemas inteligentes y algoritmos frente a los derechos y garantías construidos a lo largo de siglos de la historia humana.

En este sentido, la presente obra constituye nuestra aportación a este embrionario, pero imprescindible debate sobre el uso de algoritmos de policía predictiva en tareas de seguridad interior y sus impactos en lo que afecta a los derechos y garantías fundamentales de los ciudadanos.

En Barcelona, 20 de enero de 2022,

Paulo Ramón Suárez Xavier

PREFACIO

Antonio A. Martino

Profesor emérito de las Universidades de Pisa (Italia) y Salvador (Argentina), miembro de la Academia Nacional de Ciencias Jurídicas y sociales de Córdoba

El presente libro de Paulo Ramon Suarez Xavier se inscribe en el arco que va de la Justicia analógica al Estado inteligente. Obviamente es un proceso largo, fatigoso, complejo y que requiera varias etapas: del analógico a la digital, una vez digitalizado compatibilizar las diferentes fuentes, una vez normalizado comenzar con los procesos de automatización, pasar a los sistemas predictivos y finalmente llegar al Estado inteligente.

Ardua tarea que requiere primero electricidad, luego internet (solo el 63 % de los países tenían disponible Internet en 2020), luego cámaras en ciudades inteligentes, homogenización de datos, uso de sistemas policiales predictivos.

Requiere apoyo político e ir venciendo la normal resistencia de los funcionarios a cualquier cambio.

Lo primero que advierte el autor es el pasaje de la sociedad de riesgo a la de control y esto por un fenómeno bien humano: la creación de cualquier artilugio complejo y eficiente significa un riesgo para la humanidad: en el siglo pasado la fusión atómica e Internet, en este siglo los sistemas predictivos. Por cierto, traen progreso, pero conllevan peligros y es, por ello, que aparecen las invocaciones a la ética.

La pregunta es ¿prefiere una sociedad sin energía atómica, sin internet sin sistemas predictivos? La respuesta no puede ser negativa porque basta que el hombre sepa cómo hacerlo para que no haya limite a su expansión, por lo tanto, la pregunta es solo retórica.

En la breve historia de la I.A se documenta una parte de lo que los informáticos han entendido por ella, pero la IA trasciende la informática y hay también otras maneras de contarla. Para los que nos ocupamos de ciencias del hombre la visión que tengo, habiendo sido un protagonista inconsciente

es que durante la primera parte del desarrollo de la IA había mucho calculo lógico racional, a punto tal que puedo decir que tropezamos con la IA tratando de desarrollar lo mejor posible la lógica y, en particular, la deóntica.

Ninguno de nosotros buscaba nada sobre inteligencia artificial, sino que tratábamos de aceitar lo mejor posible los razonamientos deductivos (o inductivos), por eso digo que tropezamos con la IA. Muchos años después, apareció el *big data* o sea la enorme cantidad de datos que hoy nos apremian hasta el punto de no saber cómo tratarlos y encargarles a redes neuronales que los analicen para extraer datos concurrentes o pequeñas leyes. Esta es la segunda manera de hacer IA y es con métodos más cuantitativos.

La policía predictiva, dice nuestro autor es «una técnica que emplea el conocimiento y una base científico-criminológica y estadística, utilizando cantidades masivas de datos procesados por algoritmos y sistemas expertos de diversa índole, con fines de prestarse a la realización y apoyo de las actividades policiales».

Es una pariente cercana de la Justicia predictiva que se trabaja hoy en diversos laboratorios en el mundo y en casos prácticos:

a) Laboratorio de innovación e inteligencia artificial de la facultad de derecho de la Universidad de Buenos Aires.

b) El Ministerio Público Fiscal de la ciudad de Buenos Aires con el uso de Prometea, un software que sirve de ayuda a la decisión jurídica. Predice la solución de un caso judicial en menos de 20 segundos, con una tasa de acierto del 96%.

En el caso de los expedientes de ejecuciones fiscales, con el sistema de gestión utilizado en lote, actualmente se pueden realizar 255 sentencias de trance y remate en un mes. Con Prometea, de acuerdo con las estimaciones, se podrían realizar 1440 en el mismo período.

En la Corte Interamericana de Derechos Humanos, Prometea fue entrenado como un asistente virtual para la creación de resoluciones y notificaciones en distintos idiomas, y como herramienta de búsqueda avanzada. La Corte Constitucional de Colombia recibe miles de expedientes al año.

Algo parecido sucede con el sistema creado en el *Lib-Lab* de la *Scuola Normale Sant'Anna de Pisa*, con la conducción de Giovanni Comandé.

Un objetivo que se busca hoy es la trazabilidad de la inteligencia artificial. que es la «aptitud para rastrear la historia, la aplicación o la localización de una entidad mediante indicaciones registradas». Una IA basada en un enfoque de derechos humanos debe poder explicar, paso a paso, las operaciones técnicas que realiza desde el inicio hasta el fin de un proceso deter-

minado. Como regla, se debe garantizar la inteligibilidad y la trazabilidad del proceso de toma de decisiones de los algoritmos inteligentes.

La justicia predictiva presupone trazabilidad, interoperabilidad, previsibilidad, transparencia y relación amigable con el usuario.

La policía predictiva agrega un elemento más de control y esto hace que del control se vaya a la vigilancia lo que supone un estado más inquisitivo, más metido en nuestros temas sensibles, más reprochable, donde vuelve a surgir el tema ético de cuanto limite ética debemos poner a la Inteligencia artificial.

El reconocimiento facial, con tantas terminales diseminadas por la ciudad, es un enorme logro en lo que afecta a la eficiencia de las Administraciones Públicas, ya que permite generar multas por infracciones elevables en las computadoras de forma automática, lo que, en países como China o Corea del Norte, claramente autoritarios, puede ofrecer riesgos para la libertad de los ciudadanos.

El libro muestra las ventajas y también los límites. Téngase en cuenta que la Unesco ha logrado un texto de ética universal, cosa que aún se discute que sea posible.

Antiguamente estábamos acostumbrados a trabajar con muestreos de datos mientras que actualmente tenemos todos los datos. Por eso hay que establecer distinciones —como hace la ley orgánica española— que en su artículo quinto distingue entre:

1. Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador.
2. Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física.
3. Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física.
4. Datos relativos a la salud: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Los datos personales reciben (deben recibir) un tratamiento restrictivo en la policía predictiva y, más aún, regulatorio en el tráfico normal que se puede dar a los mismos.

Los éxitos logrados por la policía predictiva en Europa son tales de albergar serias esperanzas para el futuro inmediato. Obviamente, como dijimos al principio los grandes logros traen grandes peligros y, para muestra, basta este relato aparecido hace poco en el diario italiano *Repubblica*:

> «Bérgamo, hospital primario de la ciudad. Un paciente acaba de salir del quirófano, donde ha sido sometido a una delicada operación quirúrgica. El efecto de la anestesia aún no ha desaparecido por completo y el paciente sólo está parcialmente lúcido. De vuelta a su habitación, pide a la enfermera su teléfono móvil, por si alguno de sus seres queridos quiere saber de él o él mismo quiere tranquilizarlos cuando esté totalmente despierto. Entonces, vuelve a perder el conocimiento. Entonces alguien se lo roba. Y no sólo se lo llevan. Para que el teléfono móvil se pueda utilizar o tenga algún valor, tiene que estar desbloqueado. Aprovechando el estado de confusión del pos operado, el ladrón evidentemente coloca el teléfono frente a la cara del propietario adormecido y, utilizando la tecnología de reconocimiento facial que ofrece el modelo, hace uso de ella para hacerlo operativo. Una vez que el ladrón se ha ido, también desactiva la identidad del usuario. Una secuencia rápida de gestos, realizada con confianza y habilidad. Nadie vio nada. Sólo cuando la víctima se despierta finalmente de la anestesia, descubre que el dispositivo robado ya no puede ser localizado. Y el centro de llamadas del fabricante de teléfonos explica cómo sucedieron las cosas».

Y citando periódicos, en *El País* de España encontramos una reflexión que se puede comprender y aceptar o no, pero que trae un tema candente, donde una especialista en derecho a la privacidad, advierte la investigadora Carasa Véliz, escribe hoy una tribuna titulada *Digitalizar es vigilar* en la que analiza esta nueva realidad. Cada nuevo servicio de los gigantes digitales, cada nueva utilidad, es terreno ganado al mundo analógico, más datos y más negocio, explica Véliz.

> «Los titanes tecnológicos nos aseguran que sus nuevas invenciones respetarán nuestra privacidad, por supuesto. Lo que omiten es lo que llamo la ley de hierro de la digitalización: digitalizar es vigilar. No existe tal cosa como una digitalización sin vigilancia. El acto mismo de convertir en datos lo que no lo era es una forma de vigilancia. Digitalizar implica crear un registro, poner etiquetas a las cosas para que sea más fácil encontrarlas y seguirlas. Digitalizar equivale a hacer rastreable aquello que no lo era. ¿Y qué es rastrear, si no vigilar?».
>
> «Necesitamos áreas protegidas similares cuando se trata de la vigilancia. Está en la naturaleza de las empresas tecnológicas convertir lo analógico en digital. Pero convertir todo en un espía potencial es una amenaza para la libertad y la democracia», razona Véliz. «Hay algunos datos que es mejor no crear. Hay datos que es mejor no tener. Hay algunas experiencias de las que nunca debería quedar registro».

> «En el momento de abrir este email, o cualquier otro email, usted ha generado un registro digital. Queda apuntado, vamos. Si pincha en algún enlace, generará todavía más registros. Visitar esa página web (a ser posible, la nuestra) produce datos que son recogidos por la web en cuestión, la compañía que fabrica el navegador que haya usado y el operador de internet que le da la conexión. Cada vez que agarra el móvil, es decir, constantemente, genera datos digitales con cada movimiento del dedo sobre la pantalla y cada cosa que ve o escucha. En el mundo digital todo lo que usted toca, todo lo que mira, todos los sitios a donde va y a veces todo lo que dice, se convierte en datos que están en manos de las empresas que fabrican los aparatos, servicios y apps que haya usado. ¿Privacidad? Privacidad es que yo escriba este boletín con papel y bolígrafo y vaya a entregárselo en mano, o se lo cuente tomando un café»

¿Hay alguna garantía para el uso de los datos personales? Sí, dice nuestro autor y se refiere al artículo 12 de la Ley Orgánica 7/2021, de 26 de mayo (inspirada en la Directiva UE 2016/680) «determina la posibilidad de establecimiento de condiciones específicas para el tratamiento automatizado de estos datos personales, especialmente la prohibición de transmisión de datos o de su utilización para fines distintos para los que fueron transmitidos o, en caso de limitación del derecho a la información, la prohibición de dar información al interesado sin la autorización previa de la autoridad transmisora.

En lo que respecta a la información sensible, incluyendo el origen étnico, orientación sexual, datos biométricos y convicciones religiosas y filosóficas, el artículo 13 establece como imprescindible el atendimiento de tres circunstancias:

a) Que el procedimiento se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.

b) Que resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.

c) Que dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos».

La creación de ciudades inteligentes ha favorecido el desarrollo de policías inteligentes. El CEO de Olivetti, Quang Ngo Dinh, con motivo del evento «Smart Cities in Olivetti's view», organizado en el Pabellón Italiano de la Expo 2020 en Dubai, puso el foco en las ciudades del futuro aprovechando los proyectos ya realizados por la compañía y convertirse en verdaderas mejores prácticas nacionales, desde la Sala de Control Inteligente para la ciudad de Venecia hasta el Gabinete Smart para Milán pasando por la plataforma Smart Ivrea Ciudad y, también, para los proyectos en el campo cultural de Roma con el Mausoleo de Augusto y el sitio arqueológico de Pompeya. Todos estos instrumentos sirven a una mejor policía urbana.

Toda la parte final del libro se ocupa de un tema relevante: ¿hasta dónde la policía preventiva respeta los derechos fundamentales?

Coincidiendo con el autor, estamos convencidos de la bondad de un sistema moderno de policía preventiva, pero claro, con ciertas condiciones. La primera es tener un personal policial preparado y esto es un tema que cubre todo el uso de nuevas tecnologías por parte de las tres Administraciones públicas (la del ejecutivo, la del legislativo y la específica del judicial o administración de Justicia. No es un tema simple y nos lleva a la vieja idea de la Unión europea de la subsidiaridad política (no jurídica). Esta consiste, para decirlo en modo breve, que los problemas se resuelven lo más cerca posible de donde se originaron. Con algunas condiciones:

a) Que haya una buena conexión entre centro y periferia.

b) Que estén en el lugar las maquinas idóneas para absolver los cometidos que se quieren realizar.

c) Que el (o los funcionarios) encargados del tema este (estén) suficientemente preparados para absolver el cometido profesionalmente.

Parece sencillo, pero no lo es. Y en eso se juega toda la credibilidad de pasar de un Estado analógico a un estado inteligente (esto es mucho más que un estado digital).

Se puede hacer una enunciación sumaria y comprendería lo siguiente:

1. **No detención arbitraria**. Si se acusa a cualquier persona, de haber cometido un delito, y no hubo flagrancia, es decir, si no se le sorprendió en el momento mismo de cometerlo o en su huida —no puede ser privado de su libertad sin orden de un juez penal—, no debe ser puesto a disposición de la policía investigadora o del Ministerio Público en calidad de detenido. Fuera del caso de flagrancia, solo podrá ser aprehendido por orden del juez penal competente.
2. **Defensa**. Toda persona debe ser asistido por un defensor, tanto cuando recibe una acusación interna, como cuando es consignado ante la autoridad judicial.
3. **Presunción de inocencia toda persona**. Debe ser considerado inocente hasta que no se pruebe su culpabilidad.
4. **No incomunicación**. Al igual que cualquier ciudadano, en ningún momento el detenido podrá ser incomunicado, ni siquiera antes de declarar. Tampoco puede obligársele a reconocer una falta o declararse culpable de algún delito. tiene derecho a guardar silencio cuando se le acusa de haber cometido algún delito. La confesión rendida sin la asistencia del defensor carecerá de todo valor probatorio.

5. **Audiencia y procedimientos legales**. Para que el detenido sea sancionado internamente, antes tendrá que ser escuchado dentro de un procedimiento de responsabilidad administrativa, si es que correspondiere, o judicial en todos los otros casos.
6. **Sanciones**. Nadie podrá ser arrestado por falta administrativa por más de 36 horas.
7. **No duplicidad de sanciones**. A nadie podrán imponérsele dos veces, por una sola conducta, sanciones de la misma naturaleza.
8. **Prohibición de la tortura**. Nadie podrá ser torturado física ni moralmente. La tortura está terminantemente prohibida para todo ser humano.
9. **Información**. Cualquier persona puede consultar su expediente personal, en el que la institución asienta sus antecedentes y su actuación. De manera especial, tienen derecho a conocer si en los registros o archivos figura algún dato adverso a su persona.
10. **Protección a su vida e integridad física**. Para su vida e integridad física y garantizar su seguridad en la labor específica que desempeña, el detenido debe contar con el equipo que sea necesario. También tiene derecho al ejercicio de la legítima defensa, de acuerdo con la legislación penal, cuando sea agredido ilegítimamente en forma no prevista ni provocada.
11. **No discriminación**. De acuerdo con el art. 2.° de la Declaración Universal de Derechos Humanos toda persona, no debe ser objeto de discriminación de ningún tipo por razones de sexo, color de piel, forma de pensar, creencia religiosa o condición social. Todo policía debe tener las mismas oportunidades para desempeñarse en los distintos servicios prestados por la institución, de manera que las tareas que representen mayor interés, o aquellas que por diversas circunstancias resulten menos atractivas, se asignen de manera equitativa y razonable.
12. **Respeto a su dignidad como persona**. Todo detenido debe recibir un trato respetuoso por parte del personal policial, del personal administrativo y de la ciudadanía, jamás debe ser tratado en forma degradante o despectiva, ni ser humillado, aun en el caso de haber cometido una falta.

Inclusive en un organismo tan refinado como la Unión Europea hay discrepancias entre la Comisión, favorable al uso de sistemas inteligentes de policía y el Parlamento.

El Parlamento Europeo votó, en el pasado inmediato, a favor de prohibir permanentemente el uso de sistemas de vigilancia masiva de la población basados en parámetros biométricos e inteligencia artificial (IA), como por ejemplo el reconocimiento facial.

De hecho, el parlamento lo que hizo fue refrendar —con 377 votos a favor y 248 en contra— el informe sobre esta cuestión elaborado por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento.

En dicho documento, se pide a la Comisión Europea que se «implemente, a través de medios legislativos y no legislativos, y si es necesario mediante procedimientos de infracción, la prohibición de cualquier procesamiento de datos biométricos, incluidas imágenes faciales, con fines policiales que conduzca a una vigilancia masiva en espacios de acceso público». Además, piden que la Comisión «deje de financiar la investigación o el despliegue biométrico o los programas que puedan dar lugar a una vigilancia masiva indiscriminada en los espacios públicos».

Los eurodiputados se centraron en un controvertido proyecto de investigación financiado por la Unión Europea (UE), para crear un detector de mentiras «inteligente» basado en el análisis de expresiones faciales pensado para ayudar en el control de fronteras (llamado *iBorderCtrl*), cuyo desarrolló creen que debería interrumpirse.

En Europa ya hay cuerpos policiales que usan bases de datos privadas de reconocimiento facial, como el sistema de inteligencia artificial creado por la *startup* estadounidense *Clearview* —denunciada en cinco países por alimentarse con fotos de personas robadas de internet—, que los eurodiputados también pidieron que se prohibiera, ya que piensan que la vigilancia policial predictiva también debería estar prohibida.

A todas estas demandas, los eurodiputados añadieron, además, que no se puedan implementar sistemas de puntuación social que se usan para calificar a los ciudadanos en función de su comportamiento o personalidad, como ya sucede en China.

Según los parlamentarios, se ha demostrado la IA tiene tendencia a identificar erróneamente a grupos étnicos minoritarios, personas LGBTI, personas mayores y mujeres en tasas más altas. Por eso, el documento pide que estos sistemas estén siempre bajo supervisión humana —que siempre deberá tomar la decisión final— y sometidos a una estricta regulación legal para prevenir la discriminación y para garantizar que se respeten los derechos fundamentales cuando se utilizan sistemas de identificación basados en IA.

Por este motivo, la resolución del parlamento también pide la prohibición de que la inteligencia artificial ayude a las decisiones judiciales, otro aspecto muy controvertido en la que ya se ha aplicado la automatización, con el riesgo de que esta cimente y amplíe los sesgos en los sistemas de justicia penal. Los diputados reconocen que las tecnologías de vigilancia que usan IA tienen enormes implicaciones para los derechos y libertades fundamentales

y para la privacidad de los ciudadanos, y dejan claro que el reconocimiento de personas solo se debería usar en investigaciones criminales o cuando se sospeche de un crimen.

Luces y sombras. Y hay que decidir rápido pues los instrumentos existen y si no los usa la policía lo harán los hackers.

RECONOCIMIENTO FACIAL Y POLICÍA PREDICTIVA: ENTRE SEGURIDAD Y GARANTÍAS PROCESALES

La Administración de Justicia está cambiando. Surgen nuevas tecnologías que no restringen a la automatización de procesos repetitivos, más que ocupan y papel de suma importancia en la evaluación y predicción del riesgos en la determinación de las medidas más adecuadas y recomendables para determinadas actuaciones, especialmente en el ámbito penal.

Sin embargo, no todo son flores. Si bien la inteligencia artificial puede allanar el camino hacia una justicia más eficiente, su utilización indiscriminada en determinados ámbitos, como en la justicia y en proceso penal pueden ofrecer graves riesgos a la libertad, al libre desarrollo de la personalidad y a la intimidad personal y familiar de los ciudadanos.

En este sentido, en esta obra, Ramón Suárez, Investigador Posdoctoral Margarita Salas de las Universidades de Málaga y Barcelona, examina una de las más actuales e importantes técnicas predictivas que se están implementando en la Administración de Justicia y en políticas de seguridad pública: la policía predictiva, su concepto, orígenes, aplicaciones y las garantías jurídico-procesales necesarias para su utilización desde una perspectiva respetuosa con los derechos y garantías fundamentales de los ciudadanos.

Se trata de una obra dirigida a toda y cualquier persona interesada en conocer la policía predictiva y su aplicación a la seguridad pública y en el proceso penal, sus efectos y los riesgos que puede llegar a ofrecer sin un sistema de garantías jurídicas y procesales.

PAULO RAMÓN SUÁREZ XAVIER

Investigador Posdoctoral Margarita Salas en las Universidades de Barcelona y Málaga. Actualmente realiza una estancia de investigación posdoctoral en el Observatorio de Bioética y Derecho.

Es Doctor en Derecho Procesal, con mención internacional por la Universidad de Málaga, donde también ha cursado estudios de Grado y el Máster de Abogacía. Posé estudios de Máster en Derechos Fundamentales por la Universidad de Granada y Derecho y Administración Pública por la Universidad de Burgos.

Autor de distintos artículos indexados y comunicaciones relacionados a la transformación digital de la Administración de Justicia y al Derecho Procesal.

PVP: 15,00 €

ISBN: 978-84-1359-409-5

9 788413 594095