IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ARTÍCULO

# Empleo de *big data* y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras

Pilar Martín Ríos
Universidad de Sevilla

Fecha de presentación: diciembre 2021
Fecha de aceptación: abril 2022
Fecha de publicación: octubre 2022

## Resumen

En el presente trabajo analizamos el uso de *big data*, así como de tecnologías vinculadas a la inteligencia artificial, en las labores de ciberpatrullaje y ciberinvestigación que realizan las fuerzas y cuerpos de seguridad. Nuestro objetivo principal es evidenciar aquellos aspectos que, en relación con dicho empleo, precisan de un abordaje legal que asegure la transparencia y el control de su funcionamiento, reduciendo, asimismo, los riesgos implícitos en su potencial capacidad de afectar derechos fundamentales. No puede examinarse el recurso a estas nuevas tecnologías sin alertar, igualmente, de los peligros de incurrir en una deriva probabilística que acabe reduciendo la actuación policial a la aplicación acrítica y automática de fórmulas algorítmicas.

## Palabras clave

*big data*; inteligencia artificial; ciberpatrullaje; garantías procesales

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu



# *The use of big data and artificial intelligence in cyber patrols: the tyranny of algorithms and other dark areas*

## *Abstract*

*This work will analyse the use of big data as well as that of technology linked to Artificial Intelligence in the cyber-patrolling and cyberinvestigation work carried out by security forces. Our main aim is to demonstrate those aspects which, in relation to said work, require a legal approach that ensures the transparency and control of their function, thus reducing the risks implicit in their potential capacity to affect fundamental rights. The use of these new technologies cannot be examined without also highlighting the dangers of falling into a probabilistic drift which ends up reducing police intervention to acritical and automatic application of algorithmic formulae.*

## *Keywords*

*big data; artificial intelligence; cyber patrols; procedural guarantees*

## 1. Delimitando el objeto de estudio

En nuestro estudio hemos optado por distinguir dos nociones que, aunque están íntimamente relacionadas, responden a realidades diferentes: el ciberpatrullaje y la ciberinvestigación. A pesar de que ambas actividades policiales se desenvuelven en el mundo digital, encontramos divergencias importantes entre ellas.

Posiblemente, uno de los principales obstáculos que se afrontan a la hora de analizar cualquier aspecto vinculado a tales conceptos sea la falta de definiciones oficiales al respecto. La ausencia de instrumentos normativos que, en nuestro país, aborden esta materia justifica que surjan interpretaciones dispares acerca de su alcance.

A los efectos de este trabajo,[1] partimos de la tesis de que el ciberpatrullaje consiste en un conjunto de técnicas que atienden a las finalidades de detectar actividad ilegal en la red y descubrir a los delincuentes, así como de prevenir la perpetración de delitos. No se limita al monitoreo de las redes, sino que también comprende la obtención y recolección de información, además del almacenamiento y análisis del contenido que existe en ellas. Se trata de actuaciones que se llevan a cabo cuando aún no existe la certeza de la comisión de delito alguno. No tienen lugar, en consecuencia, en el marco de un proceso penal, por lo que discurren al margen de cualquier control judicial.

Consideramos, por otro lado, que la ciberinvestigación se refiere a la labor de identificación de los responsables de un delito concreto, caracterizada por desenvolverse en un entorno virtual. Hablamos, pues, de intervenciones policiales realizadas en el curso de un proceso que se ha abierto para la investigación de ilícitos determinados, en el que los efectivos de las fuerzas y cuerpos de seguridad realizan –bajo los controles preceptivos– aquello que la autoridad judicial les encomienda. A pesar de que tanto en una como en otra se emplean técnicas muy similares, sus finalidades son distintas. La importancia de deslindar adecuadamente estas dos facetas justifica que ambas sean objeto de atención en las páginas que siguen.

En el desempeño de estas dos funciones, el recurso a la inteligencia artificial (IA) es muy frecuente. Pese a su indiscutible utilidad, no debemos obviar que existe una cara menos amable de la IA que –singularmente, en este campo– ha de llevarnos a desechar cualquier aceptación acrítica de sus potencialidades. Por todo ello, resultará de interés examinar el uso de tecnologías de IA por parte de las fuerzas y cuerpos de seguridad en el cumplimiento de sus labores de prevención, vigilancia e investigación en la red.[2] En el trabajo que se presenta se realiza una primera aproximación a la cuestión, sin que sea nuestro propósito profundizar en el funcionamiento de dichas herramientas. Recurriremos a la clasificación que realiza Miró Llinares (2018, pág. 94 y 95) para analizar un aspecto concreto de lo que él denomina «Inteligencia Artificial Policial» (IAP), que es –por contraposición a la que se aplica en el proceso de determinación judicial de la responsabilidad–[3] la que se utiliza para la prevención e investigación policial de la delincuencia.

Con el ánimo de acotar aún más el objeto de estudio, conscientemente dejamos fuera de este el examen de VeriPol que, si bien utiliza también IA, lo hace con una finalidad muy distinta[4] a la que aquí analizaremos. Lo mismo sucede con VioGén, que es empleado como instrumento de valoración del riesgo para la adopción de medidas y que, como tal, no será objeto de atención en estas páginas.

1. Nos servimos de una definición que ofrece el Cuerpo Nacional de Policía: https://www.actualidadenseguridad.com/2020/05/que-es-ciberpatrullaje-policia-nacional-de-espana/
2. Aun cuando las herramientas tecnológicas que hemos seleccionado para su estudio no son plenamente homogéneas, todas ellas presentan un denominador común: constituyen valiosos y modernos instrumentos policiales en la lucha contra la delincuencia, tanto aquella que se libra en entornos virtuales como la que se desenvuelve en el mundo analógico.
3. Que denomina «Inteligencia Artificial Judicial» (IAJ) y que es, con notable diferencia, la que más ha concitado la atención de la doctrina.
4. Que se creó para la detección de denuncias falsas.

# 2. Ciberpatrullaje de prevención y de predicción

## 2.1. Vigilancia de fuentes abiertas y de medios sociales: ¿labor de prevención o herramienta de inteligencia?

Junto a la persecución del crimen, una de las principales funciones que se atribuyen a las fuerzas y cuerpos de seguridad es su prevención. Ciertamente, la intervención policial en la red permite recopilar información muy valiosa para la evitación de la comisión de ilícitos y para el descubrimiento de otros ya consumados.

Cuando se trata de prevenir la comisión de delitos en el entorno digital, es lógico que se acuda, principalmente, a técnicas de ciberpatrullaje. Además del manejo de motores de búsqueda de acceso público, se recurre a la vigilancia de fuentes abiertas (OSINT) y de medios sociales (SOCMINT).[5] A pesar de su importancia, existe un alarmante vacío legal en torno a ambas modalidades de actuación policial. Como consecuencia, no será posible establecer *a priori* en qué hipótesis delictivas cabe hacer uso de ellas, qué programas o procedimientos son permitidos o con qué alcance pueden ser empleados. Esta situación de anomia legitima, *de facto*, una vigilancia indiscriminada en redes que, con las enormes posibilidades que brinda la IA, puede alcanzar proporciones desmesuradas. Además, al tratarse de actuaciones policiales que no tienen origen en la comisión de ningún delito en particular que haya motivado la apertura de una causa, se desarrollarán sin control judicial.

En la praxis, es común que las autoridades policiales realicen búsquedas paramétricas, y tampoco es extraño que, como fruto de ellas, se inicien indagaciones sobre personas concretas que, únicamente, han hecho uso de ciertos términos o expresiones en su actividad digital. Todo ello se traduce en un constante monitoreo de nuestras conversaciones y relaciones privadas que, además de adentrarse peligrosamente en el campo de las investigaciones prospectivas, convierte al ciudadano en un delincuente potencial.[6] El hecho de que estas intervenciones se produzcan en redes abiertas no legitima este género de actuaciones. Si bien puede entenderse que cuando alguien publica información en una fuente de acceso libre está renunciando tácitamente a su derecho a la intimidad y a la protección de sus datos personales, ha de tenerse en cuenta que, en ningún caso, está consintiendo que dicha información sea permanentemente observada, registrada, analizada y tratada.

En definitiva, aquella labor de ciberpatrullaje que consiste en la realización de investigaciones OSINT y SOCMINT vulnera, a nuestro juicio, las exigencias propias de los principios de especialidad y de proporcionalidad. No creemos que pueda sostenerse que el rastreo de redes sea equiparable a las labores preventivas que se ejercen cuando se patrullan las calles, ni entendemos que esté justificado el empleo de técnicas y procedimientos de investigación tan proactivos como los examinados cuando solo existe la mera posibilidad de que se haya cometido cualquier tipo de delito.[7]

Discrepamos de la concepción de la vigilancia de fuentes abiertas y de medios sociales como meras herramientas para la prevención del delito o como instrumentos de investigación policial al uso. Se trata, pensamos, de verdaderos informes de inteligencia, como los propios acrónimos OSINT[8] y SOCMINT[9] indican. No en vano, las fuentes de información OSINT fueron creadas con la intención de ser utilizadas por las agencias de inteligencia gubernamentales. Se ha generalizado su uso, pero se está haciendo sin contar con el debido respaldo legal.

5. El análisis de redes sociales (*social media intelligence*) consiste en la recolección y el procesamiento de información en las diversas plataformas (Twitter, Instagram, Facebook, YouTube, Snapchat...).
GANNON, J. «The Strategic Use of Open-Source Information», disponible en: https://www.cia.gov/readingroom/docs/DOC_0006122487.pdf
6. En Argentina, el Ministerio de Seguridad presentó el 17 de abril de 2020 un Proyecto de Protocolo de Ciberpatrullaje. Las principales objeciones que ha recibido responden al hecho de que se habilite a las fuerzas de seguridad a buscar información, de manera indiscriminada, en las fuentes abiertas.
7. También leves, por tanto.
8. *Open-source intelligence*, o inteligencia de fuentes abiertas.
9. *Social media intelligence*, o inteligencia de medios sociales.

## 2.2. De la prevención a la predicción, con ayuda del algoritmo

En ocasiones, el cumplimiento de la función policial de prevención implica la realización de cierto ejercicio de *predicción*.[10] Si bien tradicionalmente este tipo de actuaciones se ha vinculado a la mera intuición, a la experiencia o al «olfato policial», hoy en día se cuenta con otros recursos que tratan de facilitar esta tarea. En estas labores predictivas, el empleo de tecnologías de IA cuenta con una particular importancia.[11] Haciendo uso de dichas técnicas, se realizan juicios probabilísticos sobre la base de los algoritmos elaborados,[12] trazando mapas de criminalidad que pueden determinar qué posibilidad existe de que en un concreto lugar se produzcan ciertos delitos. Se obtiene, en definitiva, información muy relevante para proceder, por ejemplo, a la planificación y distribución de medios humanos y materiales.

Predecir comportamientos en un área establecida, en unas condiciones ambientales dadas, con una mayor o menor visibilidad o afluencia de personas –entre otros posibles factores–, no resulta complejo. La utilidad de las técnicas predictivas variará según el delito de que se trate,[13] pero bastará con tener los datos suficientes para que el algoritmo correspondiente arroje información acerca de la probabilidad de que una conducta se realice, como mero reflejo estadístico. En cualquier caso, es indispensable que las autoridades policiales y judiciales puedan siempre separarse de esa interpretación, evitando las consecuencias potencialmente graves que derivan de la tiranía del algoritmo.[14] Como se destacó en la Resolución del Parlamento Europeo 2020/2016 sobre la inteligencia artificial en el derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales, de 6 de octubre de 2021, depositar una confianza excesiva en la naturaleza aparentemente objetiva y científica de las herramientas de IA, que ignore la posibilidad de que sus resultados sean incorrectos, incompletos, irrelevantes o discriminatorios, trae consigo riesgos nada desdeñables.

Paradójicamente, el desconocimiento acerca del funcionamiento de la actividad algorítmica puede hacer surgir dos posiciones tan extremas como enfrentadas: la aceptación acrítica de las conclusiones que alcance,[15] como veíamos, o la general desconfianza respecto a las

10. Acerca de los riesgos de la «Justicia predictiva», *vid*., ampliamente, ARMENTA DEU, T. (2012). *Derivas de la Justicia*. Madrid: Marcial Pons, págs. 263-282. La importancia del *big data* para el desarrollo de la «justicia predictiva» es destacada por GUZMÁN FLUJA, V. (2021). «Proceso penal y justicia automatizada». En: *Revista General de Derecho Procesal*, núm. 53, pág. 41.
11. Como resaltan GONZÁLEZ-ÁLVAREZ, J. L.; SANTOS-HERMOSO, J. y CAMACHO-COLLADOS, M. (2020) («Policía predictiva en España. Aplicación y retos de futuro». En: *Behavior and Law Journal*, vol. 6, núm. 1, pág. 27), la policía predictiva supone un cambio de paradigma en la forma de actuar de los cuerpos policiales que, previsiblemente, redundará –con un menor coste– en una disminución de la delincuencia.
12. Como sucede con el programa EuroCop, desarrollado en 2014 por la Universidad Jaume I de Castellón.
13. Pone de manifiesto la CEPEJC (Comisión Europea para la Eficiencia de la Justicia), en la *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment* (https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, pág. 50), que existen delitos que no presentan una naturaleza tan regular, o que, simplemente, se caracterizan por que sus efectos se producen en diferentes localizaciones. En estos casos, las predicciones que se puedan hacer serán menos relevantes.
14. Acerca de los problemas que plantea el sistema de «caja negra», *vid*. GONZÁLEZ-ÁLVAREZ, J. L.; SANTOS-HERMOSO, J. y CAMACHO-COLLADOS, M. (2020), *cit*., pág. 28. Cfr., asimismo, PÉREZ ESTRADA, M. J. (2019). «El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías». En: BARONA VILAR, S. (dir.). *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*. Valencia: Tirant lo Blanch, pág. 250 y 251. *Vid*. también SIMÓN CASTELLANO, P. (2021). «Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?». En: *Revista de Internet, Derecho y Política (IDP)*, núm. 33, pág. 3.
Acerca de la necesaria transparencia en el empleo de algoritmos, *vid*. COTINO HUESO, L. (2017), *cit*., pág. 142 y 143. *Vid*., igualmente, DONATI, F. (2020). «Intelligenza Artificiale e Giustizia». En: *Rivista AIC*, 1-2020, págs. 10 y 11). En similar sentido, SAN MIGUEL CASO, C. (2021). «La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?». En: *Ius et Scientia*, vol. 7, núm. 1, pág. 11.
15. La «tiranía del algoritmo» a que aludíamos como *retro*.

respuestas que ofrezca.[16] A este respecto, la ya referida Resolución 2020/2016 recuerda la conveniencia de que se emplee *software* de código abierto y subraya el derecho de las partes en un procedimiento penal a tener acceso al proceso de recopilación de datos y a las evaluaciones conexas realizadas u obtenidas mediante el uso de aplicaciones de IA. En otros términos, pide que los algoritmos sean explicables, transparentes, trazables y comprobables como parte necesaria de la supervisión, a fin de garantizar que el desarrollo, el despliegue y el uso de los sistemas de IA por las autoridades judiciales y policiales respeten los derechos fundamentales y sean dignos de la confianza de los ciudadanos.

Mucho más delicado que elaborar mapas de criminalidad sería realizar una predicción de la tendencia criminal de una persona sobre la base de fórmulas matemáticas.[17] Aunque la toma de decisiones judiciales vinculadas a la consideración de posibles comportamientos futuros no es una novedad en nuestro enjuiciamiento penal,[18] sería distinto que las técnicas de IA se emplearan para realizar pronósticos de peligrosidad que trataran de justificar la adopción de medidas predelictuales o, incluso, la realización de clasificaciones de ciudadanos según su propensión criminal. Esas fronteras nunca han de ser rebasadas.[19]

### 2.3. «*Big data* policial»: una mirada (recelosa) al sistema SIGO

A pesar de las reservas que ello pueda suscitar, es una realidad que las fuerzas y cuerpos de seguridad manejan patrones predictivos en el ejercicio de su labor preventiva. Elaborados conforme a ingentes cantidades de datos masivamente almacenados y tratados conforme a tecnologías de IA, ofrecen información que –no puede negarse– resulta de gran utilidad.[20]

Los diferentes recursos que emplean IA se nutren esencialmente[21] de datos proporcionados por el hombre. Puesto que cualquier prejuicio[22] en su selección e inclusión afecta a la presunción de inocencia de los sujetos analizados y a la imparcialidad de los juzgadores (Martín Diz, 2019, pág. 548), el debate acerca del origen de los algoritmos empleados sigue siendo pertinente. Seguramente, el temor a que se basen en recolecciones indiscriminadas de datos (Nieva Fenoll, 2018, págs. 151-153) solo se disipará

16. Desconfianza que ha acompañado a programas como Compass desde sus inicios y, de forma más acusada, a raíz del caso Loomis. *Vid*., al respecto, MARTÍNEZ GARAY, L. (2018). «Peligrosidad, Algoritmos y *Due Process*: el Caso *State v Loomis*». En: *Revista de Derecho Penal y Criminología*, núm. 20, págs. 485-502.
ROMEO CASABONA, C. (2020) («Inteligencia artificial, derechos fundamentales y proceso penal». En: *Comunicaciones en Propiedad Industrial y Derecho de la Competencia*, núm. 89, enero-abril 2020, pág. 265) critica que el razonamiento que se realiza en este caso implica «una inversión del rango de derechos en conflicto», haciendo primar los intereses de la empresa privada frente al derecho fundamental a la tutela judicial efectiva («Inteligencia artificial, derechos fundamentales y proceso penal». En: *Comunicaciones en Propiedad Industrial y Derecho de la Competencia*, núm. 89, enero-abril 2020, pág. 265).
También PredPol, Precobs o XLAW han sido objeto de críticas muy severas.
17. Subraya BARONA VILAR, S. (2019) («Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia». En: *Revista Jurídica Digital UANDES*, 3/1, pág. 13) los riesgos implícitos en la determinación de futuros comportamientos delictivos, fundamento del creciente recurso a la tutela preventiva.
18. Piénsese, por ejemplo, en la adopción de medidas cautelares, o en la suspensión de la ejecución de la pena privativa de libertad. *Vid*. QUATTROCOLO, S. (2020). *Artificial Intelligence, Computational Modelling and Criminal Proceedings*. Berlín: Springer, págs. 124-125.
19. Entiende WILSON, D. (2018) («Algorithmic patrol. The futures of predictive policing». En: ZAVRSNIK, A. (ed.), *Big Data, Crime and Social Control*. Nueva York: Routledge, pág. 124) que el uso de técnicas de policía predictiva presagia, desgraciadamente, un incremento de la respuesta punitiva frente al delito.
20. Especialmente relevante es aquella que resulte del trabajo colaborativo de diferentes cuerpos policiales. Como bien advierte RATCLIFFE, J. (2007) (*Integrated intelligence and crime analysis: enhanced information management for law enforcement leaders*. Washington: COPS-Police Foundation, págs. 11 y 12), contar con muchos datos no implica, necesariamente, disponer de mucha información. La información que no se comparte y que se maneja de forma compartimentada acaba, invariablemente, por perder relevancia.
21. Con independencia del *machine learning*.
22. De diversa índole, aunque, con mayor frecuencia, se denuncian sesgos relativos al género y a la raza.
Más raramente se centra la atención en otra circunstancia igualmente relevante, como destaca COTINO HUESO, L. (2017). («Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales». En: *Dilemata*, año 9, núm. 24, pág. 138): el surgimiento de «nuevos parias», que serían todos aquellos que, no aportando datos, permanecerían en la «periferia del Big data» y, en consecuencia, verían ignoradas sus preferencias y necesidades en el proceso de toma de decisiones basadas en él.

cuando el modo en que se realiza su selección pueda ser fiscalizado.[23]

Lo anterior no excluye que, en ocasiones, sea difícil incluso para sus propios programadores explicar el funcionamiento de los mecanismos creados (de Miguel Beriain y Pérez Estrada, 2019, pág. 537). Sin embargo, la aceptación de esas limitaciones no debería llevar implícita la renuncia a conocer cuáles son las fuentes de las que emanan dichos algoritmos, sobre qué datos se elaboran y quién se encarga de su selección.

En la materia que nos ocupa, las fuerzas y cuerpos de seguridad recopilan información de muy variada procedencia: grabaciones de circuitos cerrados, cámaras de tráfico, registros y fotografías realizadas a través de diferentes sistemas (drones y satélites, entre otros), y, de manera especial, la propia red. A este respecto, nos suscita ciertas dudas el modo en que se incorporan datos al Sistema Integrado de Gestión Operativa, Análisis y Seguridad Ciudadana (SIGO), creado en 2006. Se trata de una gran base de datos creada para prevenir e investigar la comisión de delitos que, entre otras funcionalidades, permite conocer en tiempo real todos los datos asociados a la matrícula de un vehículo, determinar los antecedentes de una persona y la existencia de órdenes de protección o de requisitorias nacionales o internacionales sobre ella.

Los datos seleccionados para formar parte de SIGO permanecen alojados en un fichero llamado *Intpol*. Creemos de particular interés hacernos eco de la denuncia[24] de que, en la praxis, se está procediendo a la recopilación –indiscriminada y abusiva– de información de personas que, en ningún caso, deberían encuadrarse en la categoría policial de *sospechoso*.[25] Dejando a un lado el fundamento que puedan tener tales denuncias, lo cierto es que la falta de información y de transparencia en torno al funcionamiento de SIGO incrementa la incertidumbre acerca de los criterios que determinan la inclusión en la citada base de datos y el destino de la información que en ella se almacena.

## 3. Utilización de IA en la ciberinvestigación: de la realidad aumentada a la construcción de perfiles

En el ámbito de la ciberinvestigación policial, la IA se aplica en la lucha contra la delincuencia ya cometida, es decir, no con ánimo de evitar que se perpetre un delito, sino con el propósito de descubrir su comisión e identificar a su autor. El empleo de la realidad aumentada (RA), por ejemplo, permite a la policía recrear la escena del crimen e interactuar con ella de una manera hasta ahora desconocida,[26] lo que se traduce en un aumento de la llamada «conciencia situacional».[27]

Igualmente, se han desarrollado técnicas vinculadas a la IA que sirven a la detección de tipos delictivos con-

23. Es muy frecuente que, en el curso de una investigación criminal, las autoridades soliciten a las compañías prestadoras de servicios de telefonía o de internet que faciliten datos de sus usuarios. La polémica Patriot Act estadounidense, por ejemplo, o el programa Tempora que se aplica en el Reino Unido amparan estas prácticas. Una visión muy ilustrativa de la situación puede obtenerse en SCHNEIER, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Nueva York: WW Norton & Co, pág. 448.
Con independencia de esas actuaciones «visibles», es también conocido que las fuerzas y cuerpos de seguridad acceden habitualmente a los sistemas a través de las llamadas «puertas de atrás». Acerca de la falta de legitimación de tal vigilancia masiva, *vid*. VALLS PRIETO, J. (2018). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante Inteligencia Artificial*. Madrid: Dykinson, págs. 137-145.
24. Realizada por algunos integrantes de las propias fuerzas y cuerpos de seguridad: https://www.genbeta.com/activismo-online/sigo-el-sistema-informatico-de-la-guardia-civil-que-almacena-demasiado (consultado el 5 de octubre de 2021) y https://www.europapress.es/nacional/noticia-iu-sospecha-guardia-civil-almacena-datos-sensibles-ciudadanos-acusa-oscurantismo-interior-20120827181305.html (consultado el 5 de octubre de 2021).
25. Así, se afirma que esta práctica incluye –entre otras recolecciones indiscriminadas y, por tanto, igualmente abusivas– el registro en *Intpol* de los datos de vehículos de ciudadanos que acuden a hacer cualquier gestión a dependencias de la Guardia Civil.
26. A este respecto, puede consultarse la información relativa al proyecto DARLENE, financiado por la UE, que culmina en 2023 (https://www.darleneproject.eu/arranca-el-proyecto-darlene-contra-la-delincuencia-y-el-terrorismo/).
27. A veces se utiliza, igualmente, para realizar actividades de formación policial, entre las que destaca el entrenamiento de situaciones complejas.

cretos. Así, por ejemplo, el MArIA Project se dedica a la localización de plantaciones de marihuana mediante el tratamiento de datos de los consumidores de energía eléctrica.[28] En esta misma línea, el CERT[29] ha creado una nueva herramienta de cibervigilancia (ELISA) que permite –mediante el examen de fuentes abiertas– la detección de nuevas amenazas en el ciberespacio. A pesar de lo prometedora que pueda resultar la idea, llama la atención que en su ejecución se recurra a «indicadores de desconfianza», que son conceptos tradicionalmente vinculados al mundo empresarial.

Una parte importante de los esfuerzos policiales se concentra en la lucha contra los delitos que suponen un atentado contra la libertad e indemnidad sexual de menores de edad. Es sabida la existencia de unidades operativas constituidas *ex profeso* con tal fin, que cuentan con múltiples herramientas que emplean tecnología de IA, que permiten identificar, cruzar y procesar datos con una velocidad inaudita. Así, por ejemplo, PhotoDNA Cloud Service es un programa de identificación de archivos que se utiliza para reconocer situaciones que pudieran constituir abusos a menores. En las redes P2P está muy difundido, asimismo, el uso de GnuWatch.

En el marco de la represión policial de la pederastia, también se utiliza IA para construir perfiles falsos que, tratando de ser atractivos para determinados tipos de criminales, son empleados como señuelos. Algo similar sucede con los conocidos como *honey pots* o *honey monkeys*, aunque en estos casos el reclamo es el propio sitio web, creado *ad hoc* con idéntica finalidad. Con sus diferencias, creemos que en ambos supuestos se corre el riesgo de que la frontera con la provocación policial se difumine en exceso y se frustre, como resultado, el buen fin del proceso.

## 4. El empleo de patrones biométricos en la investigación criminal: especial mención al reconocimiento facial

Las características externas de un sujeto siempre han servido para su identificación. En el curso de una investigación criminal, el reconocimiento en rueda y el practicado sobre libros de fotografías son, de hecho, ampliamente usados. Sin haber supuesto el abandono de los métodos tradicionales de investigación, ha de admitirse que los elementos biométricos[30] revisten, actualmente, una importancia singular en la determinación de la identidad personal.

Numerosas compañías recopilan información de esta naturaleza para prestar servicios de acceso rápido y seguro a sus clientes e, incluso, algunas empresas los utilizan para velar por el cumplimiento de las obligaciones laborales de sus trabajadores. Como es lógico, también la investigación criminal trata de aprovechar las posibilidades que brinda la biometría. Las bases de datos de ADN de sospechosos, por ejemplo, facilitan la identificación de autores de delitos mediante el examen de su huella genética.

La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, prevé expresamente el uso de esta información. Así, en su artículo 13.2 se establece que las autoridades competentes, en el marco de sus respectivas atribuciones, podrán tratar[31] datos biométricos dirigidos a identificar de manera unívoca a una persona física, siempre que tal actuación resulte idónea y proporcionada con el fin de la prevención, investigación o detección de infracciones penales que, en su caso, se persiga.

28. En ocasiones, estos resultan reveladores de patrones anormales de comportamiento y dan origen a la apertura de una investigación policial.
29. Perteneciente al Centro Criptológico Nacional (CCN).
30. Como son la huella dactilar, el iris, la voz o los rasgos faciales de una persona.
31. Tratamiento que se caracterizará por su automatización, como subraya GUZMÁN FLUJA, V. (2021), *cit*., nota núm. 12.

El reconocimiento facial es una técnica de identificación que se basa, precisamente, en la detección de patrones biométricos.[32] La importancia de esta tecnología[33] ya fue advertida por el grupo de trabajo del artículo 19 en el dictamen que elaboraron acerca de su uso en los servicios en línea y móviles.[34] En este, se advirtió de los efectos potencialmente negativos que el seguimiento, la localización o el establecimiento de perfiles automatizados puede tener sobre los derechos a la intimidad y a la protección de datos personales. Es su capacidad de suministrar información altamente sensible la que ha motivado que el artículo 9 RGPD prohíba su tratamiento, salvo en las excepciones que relaciona en su apartado segundo.

Debe reseñarse, además, que el análisis de los rostros puede realizarse «en vivo» o, por el contrario, derivar de grabaciones almacenadas en bases de datos. Esta segunda circunstancia supone alguna complejidad adicional, ligada a la necesidad de regular de manera suficiente y adecuada tanto la competencia para autorizar su captación, mantenimiento y procesamiento, como la responsabilidad de salvaguardar la indemnidad de la cadena de custodia de los datos obtenidos.

Por otro lado, el debido respeto al derecho de defensa exige que se conozca si algún dato obtenido mediante sistemas de reconocimiento facial[35] ha servido de fundamento para la adopción de una medida desfavorable en el curso de un proceso penal (Domingo Jamarillo, 2021, pág. 12). Es evidente el peligro que comporta una recolección de rasgos faciales que se realice de manera automatizada y masiva, esto es, sin consentimiento –ni, posiblemente, conocimiento– de los sujetos afectados y, precisamente por ello, la UE ha considerado ilegal la utilización de la aplicación Clearview AI.[36] Habida cuenta de su compromiso con la tarea de crear una IA fiable[37] y un «ecosistema de confianza» en esta materia,[38] era esperable que la UE rechazara el uso de una base de datos de fotos biométricas que permite buscar rostros entre millones de imágenes que circulan por la red.

No podemos finalizar el examen de este punto sin advertir de que los sistemas de reconocimiento facial se están empleando, también, con una finalidad distinta a la expuesta. En los últimos tiempos, está cobrando especial auge la búsqueda de microexpresiones en los rostros que puedan considerarse reveladoras de una voluntad de delinquir. No se trataría ya de individualizar al responsable de un delito cometido, sino de determinar la probabilidad de que una determinada persona pudiera llegar a cometerlo. En otros términos, un sujeto podría ser considerado sospechoso en atención, únicamente, a las emociones[39] que sus gestos faciales denotaran. Pese a las incuestionables connotaciones frenológicas que posee, esta técnica viene siendo usada desde hace tiempo en diversos sectores.[40] Aunque en España aún no sea una realidad en el campo de la investigación penal, ha de hacerse notar que en otros sistemas jurídicos existen ya diversos *softwares*[41] que están aplicando estos procedimientos en la lucha contra la criminalidad.

32. Resulta muy interesante el examen que realiza IZQUIERDO CARRASCO, M. (2020) («La utilización policial de los sistemas de reconocimiento facial automático». En: *Revista Ius et Veritas*, núm. 60, mayo 2020, págs. 86-103) de la sentencia dictada por el Alto Tribunal de Justicia de Inglaterra y Gales, de 4 de septiembre de 2019, en el que expone los problemas jurídicos que supuso la utilización por parte de la policía de un sistema de reconocimiento facial automático (AFR, por sus siglas en inglés).
33. Ampliamente utilizada en banca, telefonía móvil y, en general, en el acceso a cualquier dispositivo electrónico.
34. Dictamen 2/2012, de 2 de marzo.
35. Entre los que se incluye el empleo de gafas de identificación biométrica.
36. Que goza de una extraordinaria difusión en EE. UU.
37. *Vid*., por ejemplo, la Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno de la Comisión Europea para la Eficacia de la Justicia (CEPEJ) del Consejo de Europa, la Comunicación de la Comisión, de 8 de abril de 2019, «Generar confianza en la inteligencia artificial centrada en el ser humano» (COM(2019)0168) o el *Libro Blanco de la Comisión*, de 19 de febrero de 2020, titulado «Inteligencia artificial – Un enfoque europeo orientado a la excelencia y la confianza» (COM(2020)0065).
38. La Resolución del Parlamento Europeo 2020/2016(INI) se ha pronunciado, de hecho, en contra del tratamiento de datos biométricos para la vigilancia masiva.
39. Intranquilidad o nerviosismo, básicamente.
40. Entre otros, cada vez se difunde más su uso en los controles que se realizan en los aeropuertos.
41. Así, por ejemplo, Vaak (en Japón) o Cortica (en Israel).

## Conclusiones

El recurso a los múltiples servicios y utilidades que la IA pone a nuestra disposición facilita la realización de muchos de los quehaceres diarios. El ámbito de la Administración de Justicia –en el que contribuye a aliviar la carga de trabajo de los distintos operadores jurídicos– no es una excepción. Su creciente aplicación en el seno de la justicia penal nos sitúa en un escenario en el que los derechos fundamentales se ven claramente expuestos.

Si la tensión en el binomio libertad-seguridad acompaña con frecuencia a las discusiones que se suscitan en torno al proceso penal, en estos casos el debate cuenta con ciertas singularidades que no deben pasar inadvertidas. Las posibilidades *quasi* infinitas que proveen las nuevas tecnologías en la investigación y represión del crimen albergan –como contrapartida– el riesgo de que extralimitaciones en su empleo puedan comportar un compromiso de las más elementales garantías procesales. Así, por ejemplo, el ciberpatrullaje de fuentes abiertas presenta una ambivalencia que ha de destacarse: si bien proporciona resultados muy relevantes en la lucha contra la cibercriminalidad, ha de acogerse con mayor escepticismo su uso para el trazado de perfiles de los ciudadanos.

Es indudable que la IA ofrece enormes posibilidades a la hora de facilitar el desempeño de tareas policiales de prevención e investigación. En concreto, la labor preventiva policial que se articula en atención a patrones predictivos precisa, para su ejecución, de un volumen considerable de datos. Reviste particular importancia que exista cierto control acerca del modo en que se procede a su recolección, así como de las fuentes empleadas para ello. El sistema SIGO ha sido, a este respecto, objeto de una atención singular en estas páginas.

Aunque constituya una cuestión importante, es también paradójico que las mayores suspicacias acerca de la labor de la IA en la detección de patrones y, como consecuencia de ello, en la predicción de comportamientos delictivos –especialmente delicada cuando se trata de vaticinar tendencias criminales de sujetos individualizados–, radiquen en aspectos vinculados a la intervención humana en dicho proceso. Sin duda, ha de tenderse a la erradicación de los diferentes sesgos –que, cierto es, inutilizan los resultados que se obtengan–, pero, junto a ello, ha de huirse de la consideración de que las máquinas operan de manera infalible, so riesgo de acabar incurriendo en una verdadera «tiranía del algoritmo».

**Esta publicación es parte del Proyecto I+D+i PID2019-108155RB-I00, Biomedicina, Inteligencia Artificial, Robótica y Derecho: los Retos del Jurista en la Era Digital, financiado por el Ministerio de Ciencia, Innovación y Universidades.**

## Referencias bibliográficas

ALFARO FERRERES, E.; VÁZQUEZ ORELLANA, N.; PÉREZ GARCÍA, I.; REAL MARTÍNEZ, S. (2016). «Percepción y reconocimiento facial: bases teóricas de las ruedas de reconocimiento». En: *Gaceta Internacional de Ciencias Forenses*, núm. 18, págs. 5-11.

ARIZA COLMENAREJO, Mª. J. (2020). «Garantías procesales en el uso de drones en la investigación penal». En: FUENTES SORIANO, O. (dir.). *Era Digital, Sociedad y Derecho*, págs. 321-340 [en línea]. Disponible en: https://dialnet.unirioja.es/servlet/libro?codigo=766742. Valencia: Tirant lo Blanch.

ARMENTA DEU, T. (2012). *Derivas de la Justicia*. Madrid: Marcial Pons.

BARONA VILAR, S. (2019). «Cuarta revolución industrial (4.0.) o ciberindustria en el proceso penal: revolución digital, inteligencia artificial y el camino hacia la robotización de la justicia». En: *Revista Jurídica Digital UANDES*, vol. 3, núm. 1, págs. 1-21. DOI: https://doi.org/10.24822/rjduandes.0301.1

BUJOSA VADELL, L. (2019). «Tecnologías digitales y delitos ambientales». En: *Revista Eletrônica de Direito Processual*, año. 13, vol. 20, núm. 3, págs. 268-292. DOI: https://doi.org/10.12957/redp.2010.45021

COTINO HUESO, L. (2017). «Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales». *Dilemata*, año. 9, núm. 24, págs. 131-150.

DE MIGUEL BERIAIN, I.; PÉREZ ESTRADA, M.J. (2019). «La Inteligencia Artificial en el proceso penal español: un análisis a su admisibilidad sobre la base de los derechos fundamentales implicados». En: *Revista de Derecho de la UNED*, núm. 25, págs. 531-561. DOI: https://doi.org/10.5944/rduned.25.2019.27013

DOMINGO JARAMILLO, C. (2021). «Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana». En: *El Criminalista Digital*, I época, núm. 9, págs. 20-37.

DONATI, F. (2020). «Intelligenza Artificiale e Giustizia». En: *Rivista AIC*, núm. 1-2020, págs. 415-436.

GANNON, J. «The Strategic Use of Open-Source Information» [en línea]. Disponible en: https://www.cia.gov/readingroom/docs/DOC_0006122487.pdf

GONZÁLEZ-ÁLVAREZ, J.L.; SANTOS-HERMOSO, J.; CAMACHO-COLLADOS, M. (2020). «Policía predictiva en España. Aplicación y retos de futuro». En: *Behavior and Law Journal*, vol. 6, núm. 1, págs. 26-41. DOI: https://doi.org/10.47442/blj.v6.i1.75

GUZMÁN FLUJA, V. (2021). «Proceso penal y justicia automatizada». En: *Revista General de Derecho Procesal*, núm. 53, págs. 1-40.

IZQUIERDO CARRASCO, M. (2020, mayo). «La utilización policial de los sistemas de reconocimiento facial automático». En: *Revista Ius et Veritas*, núm. 60, págs. 86-103. DOI: https://doi.org/10.18800/iusetveritas.202001.004

MARTÍN DIZ, F. (2019). «Aplicaciones de Inteligencia Artificial en procesos penales por delitos relacionados con la corrupción». En: RODRÍGUEZ GARCÍA, N. (dir.), *Corrupción, compliance, represión y recuperación de activos*, págs. 533-568. Valencia: Tirant lo Blanch.

MARTÍNEZ GARAY, L. (2018). «Peligrosidad, Algoritmos y *Due Process*: el Caso *State v Loomis*». En: *Revista de Derecho Penal y Criminología*, núm. 20, págs. 485-502. DOI: https://doi.org/10.5944/rdpc.20.2018.26484

MESAS CARRASCOSA; GARCÍA-FERRER PORRAS (2015). «Los drones y sus aplicaciones a la ingeniería civil», pág. 211 [en línea]. Disponible en: https://www.fenercom.com/pdf/publicaciones/Los-Drones-y-sus-aplicaciones-a-la-ingenieria-civil-fenercom-2015.pdf. Madrid: FENERCOM. [Fecha de consulta: 4 de diciembre de 2021].

MIRÓ LLINARES, F. (2018). «Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots». En: *Revista de Derecho Penal y Criminología*, núm. 20, pág. 87-130. DOI: https://doi.org/10.5944/rdpc.20.2018.26446

NIEVA FENOLL, J. (2018). *Inteligencia artificial y proceso judicial*, págs. 151-153 y 168. Madrid: Marcial Pons.

PÉREZ ESTRADA, M.J. (2019). «El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías». En: BARONA VILAR, S. (dir.), *Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad*, págs. 235-254. Valencia: Tirant lo Blanch.

QUATTROCOLO, S. (2020). *Artificial Intelligence, Computational Modelling and Criminal Proceedings*. Berlín: Springer. DOI: https://doi.org/10.1007/978-3-030-52470-8

RATCLIFFE, J. (2007). *Integrated intelligence and crime analysis: enhanced information management for law enforcement leaders*. Washington: COPS-Police Foundation.

ROMEO CASABONA, C. (2020). «Inteligencia artificial, derechos fundamentales y proceso penal». En: *Comunicaciones en Propiedad Industrial y Derecho de la Competencia*, núm. 89, págs. 253-271.

SAN MIGUEL CASO, C. (2021). «La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?». En: *Ius et Scientia*, vol. 7, núm. 1, págs. 1-18. DOI: https://doi.org/10.12795/IETSCIENTIA.2021.i01.15

SCHNEIER, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Nueva York: WW Norton & Co.

SIMÓN CASTELLANO, P. (2021). «Inteligencia artificial y Administración de Justicia: *¿Quo vadis, justitia*?». En: *Revista de Internet, Derecho y Política (IDP)*, núm. 33, págs. 1-15. DOI: https://doi.org/10.7238/idp.v0i33.373817

VALLS PRIETO, J. (2018). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante Inteligencia Artificial*. Madrid: Dykinson. DOI: https://doi.org/10.2307/j.ctt22nmcqg

WILSON, D. (2018). «Algorithmic patrol. The futures of predictive policing». En: ZAVRSNIK, A. (ed.), *Big Data, Crime and Social Control*, págs. 108-127. Nueva York: Routledge. https://doi.org/10.4324/9781315395784-6

**Cita recomendada**

MARTÍN RÍOS, Pilar (2022). «Empleo de *big data* y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras». *IDP. Revista de Internet, Derecho y Política*, núm. 36. UOC [Fecha de consulta: dd/mm/aa]
http://dx.doi.org/10.7238/idp.v0i36.394511



**Sobre el autor**

Pilar Martín Ríos
Universidad de Sevilla
pilarmar@us.es

Profesora titular de Derecho Procesal de la Universidad de Sevilla.

Cuenta con publicaciones en numerosas revistas jurídicas de primer nivel, recogidas en JCR, IN-RECJ, LATINDEX, Scopus, ISOCS, CIRC, MIAR y WOS, así como con monografías y participaciones en libros colectivos en editoriales especializadas de prestigio reconocido. Es directora y promotora de REDHITEC, Red Iberoamericana de Investigadores auspiciada por la AUIP.