P9_TA(2021)0405

La inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales

Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI))

(2022/C 132/02)

El Parlamento Europeo,

— Vistos el Tratado de la Unión Europea, en particular sus artículos 2 y 6, y el Tratado de Funcionamiento de la Unión Europea, en particular su artículo 16,

— Vista la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), y en particular sus artículos 6, 7, 8, 11, 12, 13, 20, 21, 24 y 47,

— Visto el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales,

— Visto el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (ETS 108) y su Protocolo modificativo («Convenio 108+»),

— Vista 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,

— Vista la Comunicación de la Comisión, de 8 de abril de 2019, titulada «Generar confianza en la inteligencia artificial centrada en el ser humano» (COM(2019)0168),

— Vistas las directrices éticas para una IA fiable publicadas por el Grupo de expertos de alto nivel sobre inteligencia artificial de la Comisión el 8 de abril de 2019,

— Visto 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),

— Vista la Comunicación de la Comisión, de 19 de febrero de 2020, titulada «Una Estrategia Europea de Datos» (COM(2020)0066),

— Visto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por la que se deroga la Directiva 95/46/CE («Reglamento General de Protección de Datos») ([1]),

— Vista la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo ([2]),

— Visto el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE ([3]),

— Vista la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) ([4]),

([1]) DO L 119 de 4.5.2016, p. 1.
([2]) DO L 119 de 4.5.2016, p. 89.
([3]) DO L 295 de 21.11.2018, p. 39.
([4]) DO L 201 de 31.7.2002, p. 37.

Miércoles 6 de octubre de 2021

— Visto el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo ([5]),

— Vista su Resolución, de 19 de junio de 2020, sobre las protestas contra el racismo tras la muerte de George Floyd ([6]),

— Vista su Resolución, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley ([7]),

— Vista la audiencia celebrada en la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) el 20 de febrero de 2020 sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales,

— Visto el informe de la misión de la Comisión LIBE a los Estados Unidos de febrero de 2020,

— Visto el artículo 54 de su Reglamento interno,

— Vistas las opiniones de la Comisión de Mercado Interior y Protección del Consumidor y de la Comisión de Asuntos Jurídicos,

— Visto el informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (A9-0232/2021),

A. Considerando que las tecnologías digitales en general y la proliferación del tratamiento y el análisis de datos por medio de la inteligencia artificial (IA) en particular ofrecen posibilidades y riesgos extraordinarios; que el desarrollo de la IA ha experimentado un gran avance en los últimos años, convirtiéndola en una de las tecnologías estratégicas del siglo XXI, que puede generar considerables beneficios en términos de eficiencia, precisión y adecuación y que, por consiguiente, aporta una transformación positiva a la economía y la sociedad europeas, pero también enormes riesgos para los derechos fundamentales y las democracias basadas en el Estado de Derecho; que la IA no debe considerarse un fin en sí misma, sino un instrumento al servicio de las personas, con el objetivo primordial de aumentar el bienestar humano, las capacidades humanas y la seguridad;

B. Considerando que, a pesar de los continuos avances en la velocidad de tratamiento informático y la capacidad de memoria, todavía no existen programas que puedan igualar a la flexibilidad humana en ámbitos más amplios o tareas que exigen la comprensión del contexto o un análisis crítico; que algunas aplicaciones de IA han alcanzado los niveles de rendimiento de expertos y profesionales humanos en el desempeño de determinadas tareas específicas (como la tecnología jurídica o «legal tech») y pueden ofrecer resultados a una velocidad muchísimo mayor y una escala más amplia;

C. Considerando que algunos países, incluidos varios Estados miembros, hacen más uso que otros de aplicaciones de IA o de sistemas de IA integrados para fines coercitivos y judiciales, lo que obedece en parte a la ausencia de regulación y las diferencias normativas que permiten o prohíben el uso de la IA para determinados fines; que el creciente uso de la IA en el ámbito del Derecho penal se basa en particular en las promesas de que reduciría determinados tipos de delincuencia y daría lugar a decisiones más objetivas; que estas promesas, sin embargo, no siempre se cumplen;

D. Considerando que los derechos y libertades fundamentales consagrados en la Carta deben garantizarse a lo largo de todo el ciclo de vida de la IA y las tecnologías conexas, en particular durante su diseño, desarrollo, despliegue y uso, y deben aplicarse a la garantía del cumplimiento de la ley en toda circunstancia;

E. Considerando que la tecnología de IA debe desarrollarse de manera que sitúe a las personas en su centro, sea digna de la confianza pública y trabaje siempre al servicio de las personas; que los sistemas de IA siempre deben tener la garantía última de estar diseñados de forma que siempre pueda apagarlos un operador humano;

F. Considerando que, para ser fiables, los sistemas de IA deben diseñarse para que protejan y beneficien a todos los miembros de la sociedad (atendiendo desde el diseño a las personas vulnerables y marginadas), ser no discriminatorios y seguros, tomar decisiones explicables y transparentes, y respetar la autonomía humana y los derechos fundamentales, como se expone en las directrices éticas del grupo de expertos de alto nivel sobre la IA;

([5]) DO L 135 de 24.5.2016, p. 53.
([6]) DO C 362 de 8.9.2021, p. 63.
([7]) DO C 263 de 25.7.2018, p. 82.

G. Considerando que la Unión, junto con los Estados miembros, tiene la responsabilidad fundamental de garantizar que las decisiones relativas al ciclo de vida de las aplicaciones de IA en el ámbito de las actuaciones judiciales y policiales se adopten de forma transparente, salvaguarden plenamente los derechos fundamentales y, en particular, no perpetúen discriminaciones, sesgos o prejuicios allá donde existan; que las decisiones políticas al respecto deben respetar los principios de necesidad y proporcionalidad a fin de garantizar la constitucionalidad y un sistema judicial justo y humano;

H. Considerando que las aplicaciones de IA pueden ofrecer grandes oportunidades en el ámbito de la garantía del cumplimiento de la ley, en particular en lo que respecta a la mejora de los métodos de trabajo de las autoridades policiales y judiciales y al aumento de la eficacia de la lucha contra determinados tipos de delitos, especialmente los delitos financieros, el blanqueo de capitales y la financiación del terrorismo, los abusos sexuales y la explotación sexual en línea, así como determinados tipos de ciberdelincuencia, contribuyendo así a la protección y la seguridad de los ciudadanos de la Unión, si bien pueden entrañar al mismo tiempo riesgos significativos para los derechos fundamentales de las personas; que sería desproporcionada toda aplicación generalizada de la IA para fines de vigilancia masiva;

I. Considerando que el desarrollo y la explotación de sistemas de IA para las autoridades policiales y judiciales implican la contribución de múltiples personas, organizaciones, componentes de máquinas, algoritmos de software y usuarios humanos en entornos a menudo complejos y difíciles; que las aplicaciones de IA en el ámbito de las funciones de las autoridades policiales y judiciales se encuentran en distintas fases de desarrollo, desde la conceptualización hasta el uso posterior a la aprobación, pasando por la creación de prototipos o la evaluación; que pueden surgir nuevas posibilidades de uso en el futuro a medida que maduren las tecnologías gracias a la investigación científica que se está llevando a cabo en todo el mundo;

J. Considerando que es fundamental contar con un modelo claro para establecer la responsabilidad legal en el ámbito del Derecho penal por los posibles efectos nocivos de los sistemas de IA; que las disposiciones reglamentarias en este ámbito deben mantener siempre la obligación de rendición de cuentas humana y deben aspirar, ante todo, a evitar que se produzcan efectos perjudiciales;

K. que, en última instancia, corresponde a los Estados miembros la responsabilidad de garantizar el pleno respeto de los derechos fundamentales cuando se utilicen sistemas de IA en el ámbito policial y judicial;

L. Considerando que la relación entre la protección de los derechos fundamentales y la actuación policial eficaz siempre debe ser un elemento esencial de los debates sobre la utilización de la IA en el sector de la garantía del cumplimiento de la ley, en el que las decisiones pueden tener consecuencias de larga duración para la vida y la libertad de las personas; que ello es particularmente importante, pues la IA puede convertirse en una parte permanente de nuestro ecosistema de justicia penal al proporcionar análisis y asistencia en la investigación;

M. Considerando que la IA es utilizada por las autoridades policiales en aplicaciones como las tecnologías de reconocimiento facial (por ejemplo, para buscar en bases de datos de sospechosos e identificar a víctimas de trata de seres humanos o abuso y explotación sexual infantiles), el reconocimiento automático de matrículas, la identificación por voz, el reconocimiento del habla, las tecnologías de lectura de labios, la vigilancia auditiva (es decir, algoritmos de detección de disparos), la investigación y el análisis autónomos de bases de datos identificadas, la predicción (actuación policial predictiva y análisis de puntos críticos de delincuencia), los instrumentos de detección del comportamiento, las herramientas avanzadas de autopsia virtual para ayudar a determinar la causa de la muerte, las herramientas autónomas para detectar fraudes financieros y la financiación del terrorismo, la vigilancia de las redes sociales (rastreo [scraping] y recopilación de datos para detectar conexiones) y los sistemas automatizados de vigilancia que incorporan diferentes capacidades de detección (como la detección del latido cardíaco y las cámaras térmicas); que las aplicaciones mencionadas, junto con otras aplicaciones potenciales o futuras de la tecnología de IA en el ámbito de la garantía del cumplimiento de la ley, pueden tener grados enormemente variables de fiabilidad y precisión y de repercusión en la protección de los derechos fundamentales y en la dinámica de los sistemas de justicia penal; que muchas de estas herramientas se utilizan en terceros países, pero serían ilegales conforme al acervo y la jurisprudencia de la Unión en materia de protección de datos; que la utilización rutinaria de algoritmos, incluso con una pequeña tasa de falsos positivos, puede dar lugar a que las falsas alertas superen con creces las alertas correctas;

N. Considerando que las herramientas y aplicaciones de IA también son utilizadas por las autoridades judiciales en varios países del mundo, en particular en apoyo de decisiones de prisión preventiva o para dictar sentencias, calcular las probabilidades de reincidencia y determinar la libertad condicional, resolver litigios en línea, gestionar la jurisprudencia y facilitar el acceso a la justicia; que esto ha alterado y ha reducido las oportunidades para las personas de color y otras minorías; que en la Unión, a excepción de algunos Estados miembros, su uso se limita en la actualidad principalmente a asuntos civiles;

O. Considerando que el uso de la IA en el ámbito de la garantía del cumplimiento de la ley entraña riesgos potencialmente elevados y en ocasiones inaceptables para la protección de los derechos fundamentales de las personas, como la opacidad en la toma de decisiones, diferentes tipos de discriminación y errores inherentes al algoritmo subyacente que pueden verse reforzados por bucles de retroalimentación, así como riesgos para la protección de la privacidad y los

datos personales, la protección de la libertad de expresión y la información, presunción de inocencia, la presunción de inocencia, el derecho a tutela judicial efectiva y a un juez imparcial, y riesgos para la libertad y la seguridad de las personas;

P. Considerando que los sistemas de IA utilizados por las autoridades policiales y judiciales también son vulnerables a los ataques mediante IA o a la contaminación de datos, que consiste en la inclusión de un conjunto de datos erróneos a propósito para producir resultados sesgados; que, en esas situaciones, los daños resultantes pueden ser aún más importantes y dar lugar a perjuicios exponencialmente mayores, tanto para los particulares como para grupos;

Q. Considerando que el despliegue de la IA en el ámbito policial y judicial no debe considerarse como una mera posibilidad técnica, sino más bien como una decisión política sobre el diseño y los objetivos de la garantía del cumplimiento de la ley y de los sistemas de justicia penal; que el Derecho penal moderno se basa en la idea de que las autoridades estatales reaccionan ante un delito después de que se haya cometido, sin presuponer que todas las personas son peligrosas y deben ser vigiladas constantemente para evitar posibles infracciones; que las técnicas de vigilancia basadas en la IA cuestionan profundamente este enfoque, por lo que es de urgente necesidad que los legisladores de todo el mundo evalúen exhaustivamente las consecuencias de permitir el despliegue de tecnologías que reducen el papel de los seres humanos en la garantía del cumplimiento de la ley y las decisiones judiciales;

1. Insiste en que, al ser el tratamiento de cantidades ingentes de datos un componente esencial de la IA, el derecho a la protección de la vida privada y el derecho a la protección de los datos personales se aplican a todos los ámbitos de la IA, y en que debe respetarse plenamente el marco jurídico de la Unión sobre protección de datos y privacidad; recuerda, por consiguiente, que la Unión ya ha establecido normas de protección de datos en las actividades de garantía del cumplimiento de la ley, que constituyen la base para cualquier futura reglamentación en el ámbito del uso de la IA por parte de las autoridades policiales y judiciales; recuerda que el tratamiento de datos personales debe ser lícito y leal, los fines del tratamiento deben especificarse y ser explícitos y legítimos, el tratamiento debe ser adecuado, pertinente y no excesivo en relación con la finalidad para la que se tratan los datos, debe ser exacto, estar actualizado y, salvo que se apliquen restricciones, los datos inexactos deben corregirse o suprimirse, los datos no deben conservarse más tiempo del necesario, deben establecerse plazos claros y adecuados para su supresión o para la revisión periódica de la necesidad de su conservación, y deben tratarse de manera segura; subraya asimismo que debe evitarse la posible identificación de personas mediante una aplicación de IA que utilice datos previamente anonimizados;

2. Reitera que todas las soluciones de IA para las autoridades policiales y judiciales también deben respetar plenamente los principios de dignidad humana, no discriminación, libertad de circulación, presunción de inocencia y derecho de defensa, incluido el derecho a guardar silencio, libertad de expresión e información, libertad de reunión y asociación, igualdad ante la ley, igualdad de armas y el derecho a una tutela judicial efectiva y a un juicio justo, de conformidad con la Carta y con el Convenio Europeo de Derechos Humanos; destaca que debe prohibirse todo uso de aplicaciones de la IA que sea incompatible con los derechos fundamentales;

3. Reconoce que la velocidad a la que se están desarrollando las aplicaciones de IA en todo el mundo no permite elaborar una lista exhaustiva de aplicaciones, por lo que resulta necesario un modelo de gobernanza claro y coherente que garantice tanto los derechos fundamentales de las personas como claridad jurídica para los desarrolladores, tomando en consideración la continua evolución de la tecnología; considera, no obstante, habida cuenta del papel y la responsabilidad de las autoridades policiales y judiciales y del impacto de las decisiones que adoptan con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, que el uso de aplicaciones de IA debe clasificarse como de alto riesgo en los casos en que tienen potencial para afectar significativamente a la vida de las personas;

4. Considera, a este respecto, que toda herramienta de IA desarrollada o utilizada por las autoridades policiales o judiciales debe, como mínimo, ser segura, robusta, fiable y apta para su finalidad, así como respetar los principios de minimización de datos, rendición de cuentas, transparencia, no discriminación y explicabilidad, y que su desarrollo, despliegue y uso deben estar sujetos a una evaluación de riesgos y a una estricta comprobación de los criterios de necesidad y proporcionalidad, debiendo guardar proporción las salvaguardas con los riesgos identificados; destaca que la confianza de los ciudadanos en el uso de la IA desarrollada y utilizada en la Unión está supeditada al pleno cumplimiento de estos criterios;

5. Reconoce la contribución positiva de determinados tipos de aplicaciones de IA a la labor de las autoridades policiales y judiciales en toda la Unión; destaca, por ejemplo, la mejora de la gestión de la jurisprudencia lograda merced a herramientas que permiten opciones de búsqueda adicionales; considera que podrían estudiarse otros varios usos posibles

de la IA para actuaciones de las autoridades policiales y judiciales teniendo en cuenta en el proceso los cinco principios de la Carta Ética sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno adoptados por la CEPEJ, y prestando especial atención a los «usos que han de estudiarse con la cautela más extrema», identificados por la CEPEJ;

6. Destaca que toda tecnología puede aplicarse a una nueva finalidad y pide, por lo tanto, una supervisión y un control democráticos estrictos de cualquier tecnología basada en IA utilizada por las autoridades policiales y judiciales, en particular las que puedan readaptarse para fines de vigilancia masiva o de elaboración masiva de perfiles; observa, por tanto, con gran preocupación el potencial de determinadas tecnologías de IA utilizadas en el ámbito de la garantía del cumplimiento de la ley para fines de vigilancia masiva; destaca la obligación legal de prevenir la vigilancia masiva mediante tecnologías de IA, que por definición no cumple los principios de necesidad y proporcionalidad, y de prohibir el uso de aplicaciones que puedan dar lugar a dicha vigilancia masiva;

7. Hace hincapié en que el enfoque adoptado en algunos países no pertenecientes a la Unión en relación con el desarrollo, el despliegue y el uso de tecnologías de vigilancia masiva interfiere de manera desproporcionada con los derechos fundamentales y, por lo tanto, no debe ser seguido por la Unión; destaca, por tanto, que también deben regularse de manera uniforme en toda la Unión las salvaguardias contra el uso indebido de las tecnologías de inteligencia artificial por parte de las autoridades policiales y judiciales;

8. Destaca el potencial de sesgo y discriminación derivado del uso de aplicaciones de IA, como el aprendizaje automático, en particular por lo que se refiere a los algoritmos en los que se basan dichas aplicaciones; observa que los sesgos pueden ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos, introducidos por los desarrolladores de los algoritmos o generados cuando los sistemas se aplican en entornos del mundo real; señala que los resultados de las aplicaciones de inteligencia artificial dependen necesariamente de la calidad de los datos utilizados, y que estos sesgos inherentes tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente, en particular con respecto a las personas pertenecientes a determinados grupos étnicos o comunidades racializadas;

9. Subraya el hecho de que muchas tecnologías de identificación basadas en algoritmos utilizadas actualmente identifican y clasifican incorrectamente en un número desproporcionado de casos a las personas racializadas, a las personas pertenecientes a determinadas comunidades étnicas, a las personas LGBTI, a los niños y a las personas de edad avanzada, así como a las mujeres; recuerda que las personas no solo tienen derecho a ser identificadas correctamente, sino que también tienen derecho a no ser identificadas en absoluto, salvo que lo exija la ley por motivos de interés público imperioso y legítimo; destaca que las predicciones de IA basadas en las características de un grupo específico de personas acaban amplificando y reproduciendo formas de discriminación existentes; considera que deben hacerse grandes esfuerzos para evitar discriminaciones y prejuicios automatizados; pide que se establezcan salvaguardias adicionales sólidas en caso de que los sistemas de IA de las autoridades policiales y judiciales se utilicen en relación con menores;

10. Subraya la asimetría de poder entre quienes emplean tecnologías de IA y quienes se encuentran sujetos a las mismas; es imperativo que el uso de herramientas de IA por parte de las autoridades policiales y judiciales en asuntos penales no se convierta en un factor de desigualdad, fractura social o exclusión; subraya el impacto del uso de herramientas de IA en los derechos de defensa de los sospechosos, la dificultad para obtener información significativa sobre su funcionamiento y la consiguiente dificultad para impugnar sus resultados ante los tribunales, en particular por parte de las personas investigadas;

11. Toma nota de los riesgos relacionados con las fugas de datos, los fallos de seguridad de los datos y el acceso no autorizado a datos personales y otra información, por ejemplo en relación con investigaciones penales o asuntos judiciales procesados por sistemas de IA; subraya que los aspectos relacionados con la seguridad de los sistemas de IA empleados por las autoridades policiales y judiciales deben examinarse cuidadosamente y ser suficientemente sólidos y resilientes para evitar las consecuencias catastróficas potenciales de ataques malintencionados contra los sistemas de IA; destaca la importancia de la seguridad desde el diseño, así como la supervisión humana específica antes de gestionar determinadas aplicaciones críticas, por lo que pide a las autoridades policiales y judiciales que utilicen únicamente aplicaciones de inteligencia artificial que respeten el principio de privacidad y protección de datos desde el diseño con el fin de evitar la perturbación de funciones;

12. Hace hincapié en que los sistema de IA utilizados por las autoridades policiales o judiciales no deben poder dañar la integridad física de seres humanos ni distribuir derechos o imponer obligaciones jurídicas a las personas;

13. Reconoce las dificultades de atribuir correctamente la responsabilidad legal por posibles daños, habida cuenta de la complejidad del desarrollo y el funcionamiento de los sistemas de IA; considera necesario establecer un régimen claro y justo para determinar la responsabilidad jurídica de las posibles consecuencias adversas derivadas de estas tecnologías

digitales avanzadas; subraya, sin embargo, que el objetivo primordial debe ser ante todo evitar que se materialice cualquier consecuencia de este tipo; pide, por consiguiente, la observancia del principio de precaución en todas las aplicaciones de IA en el contexto policial; subraya que la responsabilidad legal debe recaer siempre en una persona física o jurídica, que siempre debe estar identificada en el caso de las decisiones adoptadas con el apoyo de la IA; hace hincapié, por tanto, en la necesidad de garantizar la transparencia de las estructuras empresariales que producen y gestionan sistemas de IA;

14. Considera esencial, tanto para la eficacia del ejercicio del derecho de defensa como para la transparencia de los sistemas nacionales de justicia penal, que un marco jurídico específico, claro y preciso regule las condiciones, las modalidades y las consecuencias del uso de herramientas de IA en el ámbito de las actuaciones policiales y judiciales, así como los derechos de las personas afectadas y procedimientos eficaces y fácilmente accesibles de reclamación y recurso, incluidos los recursos judiciales; 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 inteligencia artificial; destaca la necesidad de que las autoridades de ejecución participantes en la cooperación judicial, al decidir sobre una solicitud de extradición (o entrega) a otro Estado miembro o a un tercer país, evalúen si el uso de herramientas de IA en el país solicitante podría manifiestamente comprometer el derecho fundamental a un juicio justo; pide a la Comisión que elabore directrices sobre cómo llevar a cabo dicha evaluación en el contexto de la cooperación judicial en materia penal; insiste en que los Estados miembros, de conformidad con la legislación aplicable, deben velar por la información de las personas que sean objeto de aplicaciones de IA utilizadas por parte de las autoridades policiales o judiciales;

15. Señala que si los seres humanos se basan únicamente en datos, perfiles y recomendaciones generados por máquinas, no podrán realizar una evaluación independiente; resalta las consecuencias negativas potencialmente graves, particularmente en el ámbito de las actividades policiales y judiciales, que pueden derivarse de una confianza excesiva en la naturaleza aparentemente objetiva y científica de las herramientas de IA, sin tener en cuenta la posibilidad de que sus resultados sean incorrectos, incompletos, irrelevantes o discriminatorios; hace hincapié en que debe evitarse el exceso de confianza en los resultados ofrecidos por sistemas de IA y destaca la necesidad de que las autoridades adquieran confianza y conocimientos para poner en cuestión recomendaciones algorítmicas o hacer caso omiso de ellas; considera importante tener expectativas realistas sobre estas soluciones tecnológicas y no prometer soluciones policiales perfectas y la detección de todas las infracciones que se cometan;

16. Subraya que, en el contexto de las actividades judiciales y policiales, todas las decisiones con efectos legales deben ser tomadas siempre por un ser humano al que puedan pedirse cuentas de las decisiones adoptadas; considera que todas las personas objeto de sistemas de IA deben poder acceder a vías de recurso; recuerda que, en virtud del Derecho de la Unión, una persona tiene derecho a no ser objeto de una decisión que produzca efectos jurídicos que la conciernan o la afecte significativamente y que se base únicamente en el tratamiento automatizado de datos; subraya asimismo que la toma automatizada de decisiones individuales no debe basarse en las categorías especiales de datos personales, salvo que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; destaca que el Derecho de la Unión prohíbe la elaboración de perfiles que dé lugar a la discriminación de personas físicas sobre la base de categorías especiales de datos personales; recuerda que las decisiones en el ámbito policial son casi siempre decisiones que tienen un efecto jurídico en la persona en cuestión, debido a la naturaleza ejecutiva de las autoridades policiales y sus acciones; destaca, en este sentido, que el uso de la IA puede influir en las decisiones humanas y afectar a todas las fases del procedimiento penal; considera, por tanto, que las autoridades que recurren a los sistemas de IA deben respetar unas normas jurídicas extremadamente estrictas y garantizar la intervención humana, especialmente cuando analicen los datos derivados de dichos sistemas; exige, por consiguiente, que se defiendan la discrecionalidad soberana de los jueces y las decisiones caso por caso; pide a la Comisión que prohíba el uso de la IA y las tecnologías conexas para proponer decisiones judiciales;

17. 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, así como para asegurar que los resultados generados por los algoritmos de la IA sean inteligibles para los usuarios y las personas a las que se aplican esos sistemas, y que haya transparencia sobre los datos de origen y sobre la forma en que el sistema llega a una determinada conclusión; señala que, con el fin de garantizar la transparencia técnica, la solidez y la exactitud, solo debe permitirse la adquisición por las autoridades policiales o judiciales de la Unión de herramientas y sistemas cuyos algoritmos y lógica sean auditables y accesibles al menos por parte la policía y el poder judicial así como de auditores independientes a fin de permitir su evaluación, auditoría y verificación, y que no deben estar cerrados ni etiquetados por los vendedores como sujetos a derechos de propiedad; señala asimismo que debe facilitarse documentación en un lenguaje claro e inteligible sobre la naturaleza del servicio, las herramientas desarrolladas, el rendimiento y las condiciones en que cabe esperar que

funcionen y los riesgos que podrían entrañar; pide, por tanto, a las autoridades judiciales y policiales que dispongan la transparencia proactiva y plena de las empresas privadas que les proporcionen sistemas de IA para fines policiales y judiciales; recomienda, por tanto, el uso de software de código abierto siempre que sea posible;

18. Anima a las autoridades policiales y judiciales a que identifiquen y evalúen los ámbitos en los que podrían resultar beneficiosas soluciones de IA elaboradas a medida y a que intercambien las mejores prácticas sobre el despliegue de la IA; pide que los Estados miembros y las agencias de la Unión adopten procedimientos adecuados de contratación pública para los sistemas de IA que vayan a utilizarse en un contexto policial o judicial, a fin de garantizar su conformidad con los derechos fundamentales y la legislación aplicable, garantizando también que estén disponibles la documentación del software y los algoritmos y sean accesibles para las autoridades competentes y de supervisión para su revisión; pide, en particular, normas vinculantes que obliguen a hacer públicos las asociaciones público-privadas, los contratos y las adquisiciones y la finalidad de la contratación; hace hincapié en la necesidad de proporcionar a las autoridades la financiación precisa y dotarlas de los conocimientos especializados necesarios para garantizar el pleno cumplimiento de los requisitos éticos, jurídicos y técnicos ligados al despliegue de la IA;

19. Pide una trazabilidad de los sistemas de IA y los procesos decisorios que, mediante una documentación obligatoria, exponga sus funciones, defina las capacidades y limitaciones de estos sistemas y haga un seguimiento de dónde se originan los atributos definitorios de una decisión; subraya la importancia de mantener una documentación completa de los datos de formación, su contexto, finalidad, exactitud y efectos colaterales, así como su tratamiento por parte de los constructores y desarrolladores de los algoritmos y su cumplimiento de los derechos fundamentales; destaca que siempre debe ser posible reducir los cálculos de un sistema de IA a una forma comprensible para los seres humanos;

20. Pide que se lleve a cabo una evaluación obligatoria del impacto sobre los derechos fundamentales antes de la implementación o el despliegue de sistemas de IA en el ámbito policial o judicial, a fin de evaluar posibles riesgos para los derechos fundamentales; recuerda que es obligatoria la evaluación previa del impacto sobre la protección de datos de cualquier tipo de tratamiento, en particular mediante el uso de nuevas tecnologías, que pueda entrañar un alto riesgo para los derechos y las libertades de las personas físicas, y opina que este es el caso de la mayoría de las tecnologías de IA en el ámbito policial y judicial; subraya que los conocimientos especializados de las autoridades de protección de datos y las agencias de derechos fundamentales son esenciales para evaluar estos sistemas; subraya que estas evaluaciones del impacto en los derechos fundamentales deben llevarse a cabo de la forma más abierta posible y con intervención activa de la sociedad civil; pide que las evaluaciones de impacto también definan claramente las salvaguardias necesarias para atajar los riesgos identificados y que se publiquen, en la mayor medida posible, antes del despliegue de todo sistema de IA;

21. Destaca que solo una gobernanza europea sólida de la IA, con una evaluación independiente, permite la necesaria puesta en práctica de los principios relativos a los derechos fundamentales; pide que se efectúen auditorías periódicas obligatorias, a cargo de una autoridad independiente, de todos los sistemas de IA utilizados por las autoridades policiales y judiciales siempre que puedan afectar significativamente a la vida de personas, a fin de evaluar los sistemas algorítmicos, su contexto, finalidad, exactitud, rendimiento y escala y, una vez que estén en funcionamiento, a fin de detectar, investigar, diagnosticar y subsanar cualquier efecto indeseado y adverso y garantizar que los sistemas de IA funcionen según lo previsto; pide, por tanto, un marco institucional claro para este fin, que incluya una vigilancia adecuada en materia de regulación y supervisión, para velar por la plena aplicación y garantizar un debate democrático plenamente informado sobre la necesidad y proporcionalidad de la IA en el ámbito de la justicia penal; subraya que los resultados de estas auditorías deben divulgarse en registros públicos para que los ciudadanos sepan qué sistemas de IA se han desplegado y qué medidas se toman para reparar la vulneración de derechos fundamentales;

22. Destaca que los conjuntos de datos y los sistemas algorítmicos utilizados cuando se realizan clasificaciones, evaluaciones y predicciones en las distintas fases del tratamiento de datos en el desarrollo de la IA y las tecnologías conexas también pueden dar lugar a un trato diferenciado y una discriminación tanto directa como indirecta de grupos de personas, especialmente porque los datos utilizados para el entrenamiento de los algoritmos de actuación policial predictiva reflejan las prioridades de vigilancia actuales y, por consiguiente, pueden terminar amplificando y reproduciendo sesgos existentes; hace hincapié, por tanto, en que las tecnologías de IA, especialmente las desplegadas para actividades policiales y judiciales, requieren una investigación y unas contribuciones interdisciplinares, incluidos estudios científicos y tecnológicos, estudios críticos sobre la raza, estudios sobre discapacidad y otras disciplinas atentas al contexto social, en particular sobre la manera en que se construye la diferencia, el trabajo de clasificación y sus consecuencias; hace hincapié, por lo tanto, en la necesidad de invertir sistemáticamente en la integración de estas disciplinas en el estudio y la investigación de la IA a todos los niveles; hace hincapié asimismo en la necesidad de garantizar que los equipos que diseñan, desarrollan, prueban, mantienen, implantan y adquieren estos sistemas reflejen la diversidad de sus usos y de la sociedad en general como medio no técnico para reducir los riesgos de una mayor discriminación;

23. Destaca asimismo que la rendición de cuentas y la responsabilidad adecuadas requieren una formación especializada considerable, especialmente para el personal policial y judicial, con respecto a las disposiciones éticas, los posibles peligros, las limitaciones y el uso adecuado de la tecnología de IA; subraya que es necesario garantizar, mediante una formación y cualificaciones profesionales adecuadas, que los responsables de la toma de decisiones conozcan el potencial de sesgo, puesto que los conjuntos de datos pueden estar basados en datos discriminatorios y sesgados; apoya la puesta en marcha de iniciativas de concienciación y educación para garantizar que las personas que trabajan en el ámbito policial o judicial conozcan y comprendan las limitaciones, las capacidades y los riesgos que entraña el uso de sistemas de IA, incluido el riesgo de sesgos de automatización; recuerda que la inclusión en los conjuntos de datos para formación en IA de casos de racismo por parte de las fuerzas policiales en el desempeño de sus funciones conducirá inevitablemente a sesgos racistas en los resultados, resultados y recomendaciones generados por la IA; reitera, por tanto, su llamamiento a los Estados miembros para que promuevan políticas de lucha contra la discriminación y desarrollen planes de acción nacionales contra el racismo en las actividades policiales y el sistema judicial;

24. Observa que la actuación policial predictiva está entre las aplicaciones de IA utilizadas en el ámbito de la garantía del cumplimiento de la ley, pero advierte de que si bien la actuación policial predictiva puede analizar los conjuntos de datos necesarios para la determinación de patrones y correlaciones, no puede responder a la cuestión de la causalidad y no puede hacer predicciones fiables del comportamiento individual, por lo que no puede constituir la única base de una intervención; señala que varias ciudades de los Estados Unidos han puesto fin tras la realización de auditorías a su uso de sistemas policiales predictivos; recuerda que, durante la misión de la Comisión LIBE a los Estados Unidos llevada a cabo en febrero de 2020, los departamentos de policía de la ciudad de Nueva York y de Cambridge (Massachusetts) informaron a los miembros de que habían eliminado gradualmente sus programas de actuación policial predictiva por su falta de eficacia, sus consecuencias discriminatorias y sus fracasos en la práctica, y en su lugar habían recurrido a la actuación policial de proximidad; recuerda que esto condujo a una disminución de las tasas de delincuencia; se opone, por tanto, al uso de la IA por parte de las autoridades policiales para hacer predicciones conductuales relativas a individuos o grupos sobre la base de datos históricos y comportamientos pasados, pertenencia a un grupo, ubicación o cualquier otra característica de este tipo, para tratar así de identificar a personas que probablemente vayan a cometer un delito;

25. Toma nota de los diferentes tipos de uso del reconocimiento facial, como, entre otros, la verificación/autenticación (es decir, la correspondencia entre una cara en vivo y una fotografía en un documento de identidad, por ejemplo, fronteras inteligentes), la identificación (es decir, la correspondencia de una foto con una base de datos de fotografías) y la detección (es decir, la detección de caras en tiempo real desde fuentes como las imágenes de CCTV y su correspondencia con bases de datos, por ejemplo, la vigilancia en tiempo real), cada una de las cuales tiene distintas implicaciones para la protección de los derechos fundamentales; cree firmemente que el despliegue de sistemas de reconocimiento facial por parte de las autoridades policiales debe limitarse a fines claramente justificados y hacerse con pleno respeto de los principios de proporcionalidad y necesidad y de la legislación aplicable; reitera que, como mínimo, el uso de la tecnología de reconocimiento facial debe cumplir los requisitos de minimización de datos, exactitud de los datos, limitación del almacenamiento, seguridad de los datos y rendición de cuentas, además de ser legal, justo y transparente y perseguir un fin específico, explícito y legítimo que esté definido claramente en la legislación de los Estados miembros o la Unión; opina que los sistemas de verificación y autenticación solo pueden seguir desplegándose y utilizándose con éxito si sus efectos adversos pueden mitigarse y si se cumplen los criterios anteriores;

26. Pide, además, la prohibición permanente del uso de análisis automatizados o el reconocimiento en espacios accesibles al público de otras características humanas, como los andares, las huellas dactilares, el ADN, la voz y otras señales biométricas y de comportamiento;

27. Pide que se imponga una moratoria al despliegue de sistemas de reconocimiento facial para fines coercitivos con funciones de identificación, a menos que se utilicen estrictamente para fines de identificación de víctimas de delitos, hasta que las normas técnicas puedan considerarse plenamente acordes con los derechos fundamentales, los resultados obtenidos no estén sesgados y no sean discriminatorios, el marco jurídico prevea salvaguardias estrictas contra el uso indebido y un control y supervisión democráticos estrictos y existan pruebas empíricas de la necesidad y proporcionalidad del despliegue de estas tecnologías; señala que, cuando no se cumplan los criterios anteriores, los sistemas no deben utilizarse ni desplegarse;

28. Expresa su gran preocupación por el uso por parte de las fuerzas del orden y los servicios de inteligencia de bases de datos de reconocimiento facial privadas, como Clearview AI, una base de datos de más de 3 000 millones de imágenes que se han recopilado de redes sociales y otros lugares de internet, incluidas imágenes de ciudadanos de la Unión; pide a los Estados miembros que obliguen a los agentes de garantía del cumplimiento de la ley a revelar si están utilizando la tecnología Clearview AI o tecnologías equivalentes de otros proveedores; recuerda la opinión del Comité Europeo de Protección de Datos (CEPD) de que el uso de un servicio como Clearview AI por parte de las autoridades policiales en la Unión probablemente no sería compatible con el régimen de protección de datos de la Unión; pide a la Comisión que prohíba el uso de las bases de datos de reconocimiento facial privadas en el ámbito de la garantía del cumplimiento de la ley;

29. Toma nota del estudio de viabilidad de la Comisión sobre posibles cambios en la Decisión Prüm ([8]), también en lo relativo al reconocimiento facial; toma nota de una investigación anterior que indicaba que ningún posible nuevo identificador, por ejemplo el reconocimiento del iris o facial, sería tan fiable en el contexto forense como el ADN o las huellas dactilares; recuerda a la Comisión que toda propuesta legislativa debe basarse en pruebas empíricas y respetar el principio de proporcionalidad; insta a la Comisión a que no amplíe el marco de la Decisión Prüm a menos que haya pruebas científicas sólidas de la fiabilidad del reconocimiento facial en un contexto forense en comparación con el ADN o las huellas dactilares, después de realizar una evaluación del impacto completa y teniendo en cuenta las recomendaciones del Supervisor Europeo de Protección de Datos (SEPD) y el CEPD;

30. Destaca que el uso de datos biométricos está relacionado más en general con el principio del derecho a la dignidad humana que constituye la base de todos los derechos fundamentales garantizados por la Carta; considera que el uso y la recopilación de datos biométricos para fines de identificación remota, por ejemplo mediante reconocimiento facial en lugares públicos, así como las puertas automáticas de control fronterizo utilizadas en los controles fronterizos en los aeropuertos, pueden plantear riesgos específicos para los derechos fundamentales, cuyas consecuencias podrían variar considerablemente en función de la finalidad, el contexto y el alcance del uso; destaca, además, la controvertida validez científica de la tecnología de reconocimiento de emociones, como las cámaras que detectan movimientos oculares y cambios en el tamaño de la pupila, en contextos policiales; opina que el uso de la identificación biométrica en el contexto de las actuaciones policiales y judiciales siempre debe considerarse de «alto riesgo» y, por tanto, estar sujeto a requisitos adicionales, de conformidad con las recomendaciones del Grupo de Expertos de Alto Nivel sobre IA de la Comisión;

31. Expresa su gran preocupación por los proyectos de investigación financiados en el marco de Horizonte 2020 que implantan inteligencia artificial en las fronteras exteriores, como el proyecto iBorderCtrl, un «sistema inteligente de detección de mentiras» que elabora perfiles de los viajeros a partir de una entrevista automatizada por ordenador realizada a través de la cámara web del viajero antes del viaje y un análisis de 38 microgestos basado en la inteligencia artificial, probado en Hungría, Letonia y Grecia; pide, por consiguiente, a la Comisión que, por medios legislativos y no legislativos y si es necesario a través de procedimientos de infracción, aplique una prohibición de cualquier tratamiento de datos biométricos, incluidas las imágenes faciales, con fines coercitivos que dé lugar a una vigilancia masiva en espacios públicos; pide a la Comisión que deje de financiar la investigación biométrica o el despliegue de programas que puedan dar lugar a vigilancia masiva en espacios públicos; destaca, en este contexto, que debe prestarse especial atención y aplicarse un marco estricto al uso de drones en operaciones policiales;

32. Respalda las recomendaciones del grupo de expertos de alto nivel sobre la IA de la Comisión, favorables a la prohibición de la puntuación de las personas a escala masiva mediante IA; considera que cualquier forma de evaluación normativa de los ciudadanos a gran escala por parte de las autoridades públicas, en particular en el ámbito policial y judicial, da lugar a pérdida de autonomía, pone en peligro el principio de no discriminación y no puede considerarse conforme con los derechos fundamentales, en particular la dignidad humana, codificados en el Derecho de la Unión;

33. Pide una mayor transparencia general con el fin de llegar a una comprensión global respecto a la utilización de las aplicaciones de IA en la Unión; solicita a los Estados miembros que faciliten una visión general de las herramientas utilizadas por sus autoridades policiales y judiciales, los tipos de herramientas utilizadas, los fines para los que se utilizan, los tipos de delitos a los que se aplican y los nombres de las empresas u organizaciones que han desarrollado dichas herramientas; pide a las autoridades policiales y judiciales que también informen a los ciudadanos y ofrezcan suficiente transparencia con respecto a su uso de la IA y las tecnologías conexas cuando ejercen sus competencias, especialmente la divulgación de las tasas de falsos positivos y falsos negativos de la tecnología en cuestión; solicita que la Comisión recopile y actualice la información en un solo lugar; pide a la Comisión que publique y actualice asimismo información sobre el uso de la IA por parte de las agencias de la Unión encargadas de tareas policiales y judiciales; pide al CEPD que evalúe la legalidad de estas tecnologías y aplicaciones de IA utilizadas por las autoridades policiales y judiciales;

34. Recuerda que las aplicaciones de IA, incluidas las aplicaciones utilizadas en el contexto policial y judicial, se están desarrollando a gran velocidad a nivel mundial; insta a todas las partes interesadas europeas, incluidos los Estados miembros y la Comisión, a que garanticen a través de la cooperación internacional la participación de socios de fuera de la Unión con el fin de elevar el nivel de las normas a escala internacional y encontrar un marco jurídico y ético común y complementario para el uso de la IA, en particular para fines coercitivos y judiciales, que respete plenamente la Carta, el acervo europeo en materia de protección de datos y los derechos humanos en general;

([8]) Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, (DO L 210 de 6.8.2008, p. 1).

35. Pide a la Agencia de los Derechos Fundamentales de la Unión Europea que, en colaboración con el CEPD y el SEPD, elabore directrices generales, recomendaciones y mejores prácticas a fin de especificar en mayor medida los criterios y las condiciones para el desarrollo, el uso y el despliegue de aplicaciones y soluciones de IA para su uso por las autoridades policiales y judiciales; se compromete a realizar un estudio sobre la aplicación de la Directiva sobre servicios con funciones coercitivas ([9]) con el fin de determinar cómo se ha garantizado la protección de los datos personales en las actividades de tratamiento por parte de las autoridades policiales y judiciales, en particular cuando se desarrollen o desplieguen nuevas tecnologías; pide asimismo a la Comisión que examine si es necesaria una acción legislativa específica para especificar con más precisión los criterios y las condiciones para el desarrollo, el uso y el despliegue de aplicaciones y soluciones de IA por parte de las autoridades policiales y judiciales;

36. Encarga a su presidente que transmita la presente Resolución al Consejo y a la Comisión.

([9]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. (DO L 119 de 4.5.2016, p. 89).