

Prácticas de inteligencia artificial prohibidas

1. Estarán prohibidas las siguientes prácticas de inteligencia artificial:

a) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.

b) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.

c) La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, de forma que la clasificación social resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales

que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;

ii)un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.

d)El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i)la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;

ii)la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;

iii)la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo 62 , para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.

2.El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de

aplicación de la ley para conseguir cualquiera de los objetivos mencionados en el apartado 1, letra d), tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra d), cumplirá salvaguardias y condiciones necesarias y proporcionadas en relación con el uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales.

3. Con respecto al apartado 1, letra d), y el apartado 2, cualquier uso concreto de un sistema de identificación biométrica remota «en tiempo real» en un espacio de acceso público con

finde aplicación de la ley estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema, que la otorgarán previa solicitud motivada y de conformidad con las normas detalladas del Derecho interno mencionadas en el apartado 4. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar el sistema antes de obtener la autorización correspondiente, que podrá solicitarse durante el uso o después de este.

La autoridad judicial o administrativa competente únicamente concederá la autorización cuando esté convencida, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos que figuran en el apartado 1, letra d), el cual se indicará en la

solicitud. Al pronunciarse al respecto, la autoridad judicial o administrativa competente tendrá en cuenta los aspectos mencionados en el apartado 2.

4. Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley dentro de los límites y en las condiciones que se indican en el apartado 1, letra d), y los apartados 2 y 3. A tal fin, tendrán que establecer en sus respectivos Derechos internos las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión de estas. Dichas normas especificarán también para cuáles

de los objetivos enumerados en el apartado 1, letra d), y en su caso en relación con cuáles de los delitos indicados en su inciso iii), se podrá autorizar que las autoridades competentes utilicen esos sistemas con fines de aplicación de la ley.