¿CÓMO ENCAJA EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL DE LA UE EN EL SISTEMA PENAL DEMOCRÁTICO?

HOW DOES THE EU ARTIFICIAL INTELLIGENCE REGULATION FIT INTO THE DEMOCRATIC CRIMINAL JUSTICE SYSTEM?

Paz M. De la Cuesta Aguado[1]

1. INTRODUCCIÓN

Con carácter general, y muy grosso modo, podría afirmarse que la aparición de tecnologías de la información disruptivas, tales como las que se suelen denominar, Inteligencia Artificial (en adelante IA) están acelerando procesos de acumulación de capital y cambios en las forma de comunicación -quizá también en la forma de ver el mundo-. El Derecho penal se ve, evidentemente, afectado por los cambios económicos, y sociales, pero también por las ideologías o formas de percibir la realidad mayoritarias, también muy sensibles a los procesos de difusión de información condicionados por IA. Si la estabilización económica y política de los Estados del Primer Mundo tras la Segunda Guerra Mundial generó sistemas políticos democráticos y derechos penales garantistas basados en un modelo de Derecho penal mínimo, la aparición de nuevas tecnologías augura importantes novedades en el Derecho penal.

En este estado de cosas, a la vista de algunas alarmantes noticias en el ámbito internacional que ponen en tela de juicio la supervivencia de modelos garantistas penales basados en el respeto a la ley -también a la internacional- y en la separación de poderes, es preciso preguntarse si este ideal de Derecho penal racional y garantista sigue vigente. La respuesta para sistemas democráticos es, indudablemente, sí. Sin embargo, más allá de abstractas posiciones doctrinales conviene detenerse en las palabras: los ladrillos con los que la sociedad y, sobre todos, los penalistas, construimos la realidad que regulamos. Esta cuestión es singularmente importante en relación con la tecnologías relacionadas con el uso de

[1] Catedrática de Derecho penal. Universidad de Cantabria

algoritmos y a las que designaremos como “sistemas algorítmicos”; pues, si bien observamos, con ellas se está construyendo un “relato”; un discurso legitimador basado en imágenes y estereotipos generados con fines comerciales y en beneficio de la parte productora.

Tras años de debate acerca de la “no intervención” legislativa en las tecnologías basadas en algoritmos e Internet, la Unión Europea ha iniciado un tímido, pero importantísimo proceso para someter a control las actividades económicas y de todo tipo que utilizan estas tecnologías. Obviando alguna sectorial previa, es preciso detenerse en el REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

Este reglamento, rompedor en algunos de sus preceptos, al menos aparentemente; menos intervencionista de lo que podría parecer, ha sido objeto de fuertes presiones tendentes a su derogación o suspensión. Con independencia de ello, el reglamento también utiliza la extendida expresión “Inteligencia Artificial” -con mayúsculas, como nombre propio- para designar a partir de unas cualidades (inteligencia y artificial) no se sabe exactamente qué. Esta primera apreciación es importante dos razones: primero, porque es una expresión que condiciona la comunicación a partir de juicios de valor positivos -lo que incide sobre la percepción del receptor del mensaje comunicativo- y, segunda, porque en la medida en que no designa objetos o acciones, sino que valora los objetos así designados, no es una terminología eficiente para su uso en la ley penal. O, dicho de otro modo, al tratarse de términos imprecisos y no descriptivos, están impregnados de una ambigüedad contraria a la necesaria taxatividad propia de los tipos penales[1].

En consecuencia, se hace preciso buscar fórmulas lingüísticas que, siendo descriptivas, sean reconocibles por la ciudadanía y por quienes deben aplicar la ley penal. El Reglamento UE 2024/1689, de 13 de junio[2] (en adelante, RIA), aunque en sus Considerandos se refiere a

[1] Más ampliamente DE LA CUESTA AGUADO, P.M. “El Derecho penal frente al Reglamento de Inteligencia Artificial”, en *Ius Criminale* 1(2024), pp. 85 ss.

[2] REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de junio de 2024 *por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828* (Reglamento de Inteligencia Artificial)

la tecnología basada en algoritmos como *Inteligencia Artificial*, en el texto articulado utiliza la fórmula *sistema de IA* y lo define como *sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*. En España, el *Anteproyecto de ley para el buen uso y la gobernanza de la Inteligencia Artificial* de marzo de 2025, también acoge este concepto en su texto articulado[3].

En consecuencia -y con muchas prevenciones-, utilizaremos la expresión "sistemas de IA" para referirnos a lo que vulgarmente se designa -con fines comerciales- como Inteligencia Artificial y, salvo que posteriormente surja una fórmula lingüística más precisa, también debería hacerlo la ley penal en su caso[4]. En todo caso, creo que sería más descriptivo, más neutro valorativamente y más realista denominarlos "sistemas algorítmicos".

Esta precisión es importante, porque no debemos olvidar que la ley penal -y la norma secundaria- cumple funciones simbólicas y la calificación como inteligente a una máquina[5], puede tener el efecto de potenciar valoraciones positivas que interesan exclusivamente a un sector social -el de los productores que ponen estas máquinas en el mercado con fines lucrativos- y que no se corresponden exactamente con la realidad, puesto que su principal característica es su capacidad enorme para manejar datos, lo que sería "memoria" en el lenguaje humanizador con que se designa esta tecnología. Y, en términos coloquiales, al menos, memoria aún no es sinónimo de inteligencia.

Es necesario, en segundo lugar -pero incidiendo en la misma idea-, advertir de la necesidad de que la ley penal (y también la administrativa) renuncien a expresiones humanizadoras de esta tecnología, tales como que "toma decisiones", "crea", "miente", etc. Y ello, no solo por las razones expuestas en relación con la racionalidad propia de la ley penal,

[3] Por más que, también, en su Exposición de Motivos el Anteproyecto de ley para el buen uso y gobernanza de la Inteligencia Artificial los designe como IA.

[4] Sobre el concepto de IA puede verse el documento *A Definition of AI: Main Capabilities and Scientific Disciplines, de la Comisión Europea.* Puede verse en https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines [citado 20.03.2025]. Este documento, en su p. 7 ofrece una definición compleja que atribuye a dicho término un doble significado, por un lado, el producto a partir de sus funciones, y, por otro, la(s) disciplina(s) científica(s) y técnicas que lo desarrollan. Esta definición, sin perjuicio de su validez a efectos de definir una realidad compleja, plantea dificultades para ser utilizada con fines de tipificación de conductas (para imponer sanciones administrativas o penales), por lo que nos remitiremos a la ya indicada del art. 3.1 RIA-

[5] Por utilizar la terminología utilizada en el art. 3.2 del RIA.

sino también porque lo contrario significaría utilizar la ley penal en defensa de los intereses comerciales del sector productivo en perjuicio de los consumidores.

Pero más allá de cuestiones terminológicas, que, desde luego deben condicionar el texto legal, las nuevas tecnologías que se basan en sistemas algorítmicos plantean retos importantes al Derecho penal. El primero es el de la conveniencia de la intervención penal, cuando desde hace años, la industria y los textos normativos apuestan por la idea de la autorregulación, a partir de una "Inteligencia Artificial ética" o expresiones similares. En los últimos años se ha ido despertando, al menos en Europa, la conciencia de la necesidad de regulación de la utilización, comercialización y efectos de estas tecnologías, pero también es cierto que la UE se encuentra con importantes obstáculos económicos y geopolíticos que tienen un peso importante a la hora de optar por la regulación y muy especialmente si se trata de una ley penal. Pero, además, en el ámbito penal, las dificultades para conocer el funcionamiento interno de los propios sistemas algorítmicos imponen dificultades añadidas, lo que exigiría, probablemente, partir de la posibilidad de que los tribunales penales obligaran a desvelar datos – también probablemente- amparados por patentes… siempre que fuera posible, porque, según parece, hay sistemas lo suficientemente autónomos como para que no sea posible determinar cómo se ha producido un determinado resultado -consistente en una respuesta a un *promt*[6]- cualquiera que sea la forma en que se presente-.

2. LAS PALABRAS CONSTRUYEN LA REALIDAD: EL PARADIGMA LIBERTARIO

La rapidez de la implantación social de las tecnologías relacionadas con sistemas algorítmicos (o, quizá también, la rapidez con que diversos medios tecnológicos han acogido a sistemas algorítmicos) ha acabado por impulsar un cierto movimiento crítico con algunos postulados defendidos por representantes, estudiosos y usuarios de las tecnologías informáticas emergentes; movimiento crítico que insta a superar el "paradigma de la libertad en Internet" que se ha venido manteniendo desde los últimos años del siglo XX, cuando se empezó a reflexionar acerca del control jurídico de estas tecnologías. En este punto se pueden distinguir, *grosso modo*, dos líneas argumentativas distintas, que coinciden, sin embargo, en las conclusiones y los coincidentes intereses y perspectivas que subyacen a ambas:

[6] Conjunto de palabras con significado dirigido a un sistema algorítmico con una orden de activación.

La primera es la del "paradigma libertario". La libertad absoluta en Internet se instaló entre jóvenes (generalmente varones) tecnólogos, inspirados y potenciados por empresas y empresarios muy interesados en actuar sin límites. Pero no puede negarse que consiguió un efecto importante, y este ideal libertario, de los años 90 del siglo pasado, se ha mantenido respecto de cualquier tipo de intervención normativa en la "web" o Ciberespacio e, incluso, se ha extendido al mundo real. En este punto es preciso recordar, sin embargo, algo tan básico para el jurista de que no hay derechos o libertades absolutas: todos ellos tienen límites, al menos, en los derechos y libertades de los demás.

Junto a lo anterior, el discurso sobre la ética en la tecnología y la tecnología "ética" se presenta como salvación a los evidentes abusos en el uso de tales tecnologías, en un ámbito, Internet, en el que la ausencia de control era utilizada para la comisión de delitos (los delitos informáticos, ciberdelitos, etc.), pero, sobre todo, para garantizar posiciones de fortaleza de las empresas productoras o distribuidoras respecto de los consumidores. En cualquier caso, pese a las exigencias de respeto a la ética se han mantenido conductas de apropiación masiva de datos, imposición de fórmulas para obtener consentimientos poco informados o condicionados a la necesidad de uso, entre otras.

Más allá de eventuales beneficios, estas pretensiones éticas significaban, por un lado, el reconocimiento de que la libertad absoluta no era admisible, pero sin ponerle límites efectivos. La reclamación de códigos éticos intentó generar un sistema de control social que no solo no fue efectivo, sino que ha servido, de nuevo, como argumento para legitimar el avance de una tecnología que empieza a utilizar el argumento de la "´ética, seguridad, fiabilidad" entre otros, como técnica de marketing.

Ahora bien, el recurso a la ética no deja de ser una apelación a la autorresponsabilidad y autocontrol ejercido por las propias empresas, derivada de la (¿sorprendente?) ausencia de controles normativos, de normas de comportamiento y el mantenimiento de la idea de que las empresas generadoras o que utilizan software "inteligente" o que se mueven en el mundo virtual han de quedar exentar de cualquier control externo procedente de los Estados.

En la actualidad, la aparición de un modelo de negocio que se construye sobre la exposición pública y la utilización de datos personales y de todo tipo y que los convierte en materia prima -y a quienes los generan en fuente de tales materias primas- con la consiguiente presión y riesgos, ha despertado las alarmas. Así, en Europa se ha empezado a romper con el paradigma de la libertad sin límites y del de la tecnología ética y confiable, para iniciar un

proceso legislativo innovador que tiene como finalidad el control de la comercialización, uso y efectos de los sistemas algorítmicos (al menos de momento) y está obligando a los Estados miembros a subirse al tren de la regulación. Ahora bien, este movimiento regulatorio, dada la actual situación geopolítica, previsiblemente se encuentre con importantes obstáculos y si bien inicialmente se alegaba -de forma quizá optimista- que, dado el peso económico y político de Europa, muy probablemente muchos otros Estados se sumarían a esta iniciativa, está por ver si esta presunción se materializa.

No puede negarse, sin embargo, que las presiones para limitar la intervención y el control de sistemas algorítmicos por parte de sectores con poder económico y político relacionados con el desarrollo de la IA son muy fuertes y se recurre a conocidos argumentos contra la intervención penal en entornos económicos (fraude fiscal, protección ambiental, etc.). O sea, nuevas tecnologías, pero viejos argumentos.

3. EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: EL REFLEJO DE LO QUE ESTÁ PASANDO

En este contexto, el RIA marca un antes y un después en el sometimiento de los sistemas algorítmicos al control normativo, porque rompe el paradigma de la desregulación en que consiste la "autorregulación bajo prismas éticos" para establecer organismos que fiscalizan y controlan los sistemas algorítmicos puestos en el mercado, por un lado, y, por otro, prohíbe determinadas conductas a la vez de enumera y designa los que denomina "riesgos" derivados de la utilización de sistemas algorítmicos.

El RÍA clasifica a los *sistemas de IA* en función de los riesgos que pueden generar (inadmisibles, de alto riesgo, de bajo riesgo y sin riesgo) para, a continuación, afrontar tres retos de suma importancia: prohibir prácticas comerciales y de uso de sistemas algorítmicos que generan riesgos inaceptables; instaurar un sistema institucionalizado de control de tecnologías de IA que generen riesgos e imponer sanciones a quienes infrinjan las prohibiciones o incumplan las medidas de control previstas.

La opción reguladora ha sido objeto fuertes críticas, primero, y mayores presiones políticas, después. Así, se alega que la regulación limitará el desarrollo de estas tecnologías en Europa -idéntico argumento, por cierto, al que se ha utilizado contra cualquier intervención penal que afectara a los intereses económicos, como, por ejemplo, contra los delitos ambientales, los delitos fiscales o los delitos dirigidos a proteger los derechos de los

trabajadores-. El fácil argumento de que, si la materia se regula, el mayor *coste penal* forzaría a las empresas a abandonar los Estados en los que la intervención penal protegiera los intereses generales en perjuicio de los particulares, sin ser falso, no ha hecho más que poner de manifiesto la necesidad de ampliar las regulaciones protectoras de los derechos de las personas más vulnerables a todos los Estados para evitar el denominado *fórum shopping* y paraísos de desregulación.

La realidad actual, la capacidad que han demostrado estas tecnologías para alterar o intervenir (manipulando) en la comunicación pública o para intervenir en situaciones de conflicto bélico, como podrían ser las "guerras híbridas", no hace más que poner de manifiesto la necesidad de someter a control democrático -esto es, mediante leyes y normas jurídicas dictadas por los órganos que ostentan la representación de la ciudadanía- la tecnología basada en sistemas algorítmicos.

Se suele alegar, contra esta pretensión reguladora, que sería necesario pactar globalmente la regulación; es decir, implicando a todos los Estados. Sin negar lo conveniente de que ello fuera así, lo cierto es que, en el fondo, este argumento es otra forma más de impedir la regulación puesto que, hoy en día, este *desiderátum* es inalcanzable, ya que existen Estados que se están beneficiando abiertamente de esta situación y empresas y personas económicamente beneficiadas. En sentido contrario, la regulación se hace cada vez más imprescindible para garantizar derechos personalísimos e incluso, los propios sistemas democráticos que, en estos momentos históricos, están sometidos a fortísimas tensiones[7].

4. EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: EL REFLEJO DE UNA NUEVA REALIDAD

El RIA, como hemos visto, trata de someter a control el uso de tecnologías algorítmicas, pero no contiene normas penales, en sentido estricto -es decir, normas dirigidas a jueces penales para que impongan una sanción penal- sino que enuncia una serie de prohibiciones y aquellos supuestos en los que estas pueden ser excepcionadas (por los Estados miembros) así como límites máximos a la posible sanción pecuniaria.

[7] En este punto, conviene poner de manifiesto que el RIA obvia completamente cualquier referencia al alto coste energético que exige esta tecnología y que está tensionando los mercados de la energía, reabriendo debates ya (aparentemente) superados sobre el uso de técnicas de fisión nuclear para la producción de energía eléctrica y el componente expropiatorio de riqueza común que puede llevar aparejada la contaminación.

En consecuencia, se está anunciando un nuevo sistema normativo, complejo y con numerosos actores, que incluirá normas administrativas (europeas y estatales) y que, probablemente, deba cerrarse con normas penales. La necesaria coordinación entre normas administrativas sancionadoras y Derecho penal va a ser, sin duda, tarea nada fácil, entre otras razones porque el RIA establece una serie de prohibiciones que recuerdan mucho lo que serían normas penales y porque las sanciones administrativas derivadas del RIA –.

El Art. 5 RIA contiene, efectivamente, las denominadas prohibiciones. Es decir, aquellas conductas que no son admisibles en ningún caso y que darán lugar a sanciones. Son las denominadas prácticas prohibidas. Adviértase ya que el RIA regula y prohíbe prácticas comerciales y el uso para determinados fines, pero no prohíbe ni la creación ni la existencia de sistemas de IA.

Lo más llamativo, probablemente, del RIA no es lo que prohíbe, sino lo que describe. Es decir, al establecer las normas prohibitivas (las prohibiciones), el precepto en sus distintos apartados está dibujando una realidad a la que va dirigida, y, por tanto, que ya existe, auténticamente estremecedora y de la que la sociedad es poco (o nada) consciente. Así, muy resumidamente, el Art. 5 RIA prohíbe la introducción en el mercado o uso de sistemas de IA que:

a) utilicen técnicas subliminales, manipuladoras o engañosas, que puedan afectar al comportamiento, o producir perjuicios considerables
b) exploten vulnerabilidades de personas o colectivos y puedan afectar al comportamiento de una persona y producirle perjuicios considerables
c) realicen ciertas clasificaciones de personas que provoquen "trato perjudicial o desfavorable" -o sea, discriminación- en otros contextos o injustificada.
d) realicen ciertas evaluaciones de riesgos de cometer delitos sin la intervención humana.
e) generen ciertas bases de datos de reconocimiento facial mediante "extracción no selectiva"
f) sirvan para inferir emociones en algunos contextos, excepto por motivos médicos o de seguridad
g) realicen ciertas clasificaciones biométricas con fines de deducir información personalísima y protegida (raza, afiliación, vida sexual, etc.) con excepciones
h) realicen identificación biométrica remota en tiempo real en lugares públicos, con excepciones.

Si se lee con detenimiento, el art. 5 RIA nos está indicando que ya existen bases de datos de reconocimiento facial; que los sistemas algoritmos están infiriendo emociones; realizando clasificaciones biométricas para inferir información personalísima; manipulan emociones; etc. Como hemos advertido, el art. 5 RIA prohíbe una serie de prácticas comerciales y de uso de sistemas algorítmicos bajo la fórmula de prohibir la comercialización y explotación de sistemas algorítmicos que utilizando un medio determinado pueda generar ciertos peligros o perjuicios.

De ello se puede deducir lo siguiente:

1) Lo que se prohíbe, en contra de lo que pudiera parecer, no es el sistema de IA; ni siquiera su creación, sino su comercialización y uso. Esto significa que al Derecho penal le quedarían -para una eventual intervención- la creación de sistemas algorítmicos dañinos y la propia existencia del sistema de IA.
2) Se prohíben sistemas que realizan determinados procesos que se consideran no aceptables por los riesgos que generan. Es decir, el desvalor se vierte sobre el sistema en función del resultado (de peligro), pero no en función de la propia peligrosidad del sistema de IA o del desvalor de la propia "conducta" o resultado inmediato del proceso de funcionamiento del algoritmo. Esto se puede ver con claridad en el apartado 2 del art. 5.a) del Ria que prohíbe sistema que "manipulen emociones" que puedan afectar a una persona y le haga cambiar de opinión de forma que se genere un riesgo -muy simplificadamente-

La estructura de estas denominadas prohibiciones, entonces, se articulan en un proceso que exige la comprobación de determinados requisitos: (1) un sistema IA que realiza un proceso; (2) proceso que tiene incidencia en el comportamiento de la(s) persona(s) y (3) como consecuencia, se produce un resultado peligroso o lesivo. Es la suma de los tres requisitos lo que generaría el reproche sancionador, pero no cada uno de ellos por separado. Sin embargo, desde una perspectiva de los derechos de las personas afectadas, de los derechos humanos o incluso de la propia convivencia, la "manipulación" de la persona que genera engaño, ya podría merecer, probablemente un juicio de desvalor, sobre todo cuando esa manipulación es "subliminal" y puede afectar a un amplísimo e indeterminado número de personas, muchas de ellas, menores y, en cualquier caso, objetivos diana como consecuencia de su vulnerabilidad. Estas conductas no solo manipulan o atentan contra principios esenciales de la convivencia -

buena fe contractual, etc.- sino que, además, cosifican a las personas con unos niveles de intensidad y extensión que las convierten, más allá del hecho concreto sobre la persona concreta, en muy peligrosas para la sociedad en su conjunto.

El art. 5 RIA distingue entre las que denominaremos "prohibiciones absolutas", que prohíben ciertas prácticas en todo caso -apartados a) y b) del art. 5 RIA- y prácticas permitidas, pero prohibidas en determinados supuestos -resto de los apartados- . En ambos casos, y sin necesidad de reformas legislativas, el Derecho penal sería de aplicación cuando los "perjuicios considerables" a que hacen referencia los párrafos a) y b) del art. 5.1 RIA sean subsumibles en un tipo penal. En los demás supuestos, al menos, el papel del Derecho penal, además de subsidiario, sería dependiente de la regulación administrativa, conforme a lo que se conoce doctrinalmente como un modelo de Derecho penal accesorio del Derecho administrativo.

Pero más allá del contenido concreto de las conductas y de las dificultades de técnica jurídica para someterlas a control e, incluso, para enunciarlas, sí se puede afirmar ya que nos encontramos ante normas que recuerdan mucho las normas penales, primero, porque establecen pautas de conducta (prohibiciones o permisos) y, en segundo lugar, porque involucran a bienes jurídicos importantísimos de carácter persona: la salud; la intimidad; la propia imagen; la libertad… es decir, bienes jurídicos clásicos, ya sean de carácter individual o colectivo muy valorados por los ordenamientos jurídicos basados en el respeto a la dignidad de las personas y de los derechos humanos. Ahora bien, lo más importante es que, junto a ellos, están apareciendo nuevos bienes jurídicos necesitados de protección; valores hasta ahora ajenos al debate y a la intervención penal. Empiezan así a detectarse como valores que pueden ser afectados por tales prácticas algunos de nuevo corte, pero esenciales para la colectividad, para la democracia o para la paz. Los bulos, la manipulación de emociones, los ataques sistemáticos a instituciones y personas representativas en el sistema democráticos pueden tener efectos que exceden con mucho lo conocido y que abren la puerta a plantearse la necesidad de proteger al propio sistema democrático o a la veracidad de la información como bienes jurídicos; lo que legitimaría el uso del Derecho penal para protegerlos.

Pero es que también otros bienes jurídicos clásicos se pueden ver afectados y es posible que necesiten una reinterpretación. Por ejemplo, el concepto de intimidad (frente al control de personas mediante sistemas biométricos o a la acumulación masiva de datos de particulares borrados por estos) o de honor (como consecuencia de las expresiones amparadas por el anonimato en RRSS) pueden estar adquiriendo nuevos significados y, desde luego, contornos

más amplios, el primero, y más reducidos, el segundo -cuestión esta, sin embargo, que debe ser sometida a severa crítica-. Piénsese en el hecho de que los buscadores y, en general, los sistemas algorítmicos "guardan" los contenidos de las interacciones (conversaciones en chats; correos electrónicos, búsquedas en Internet, etc.). Esta información se almacena en algún lugar (¿nube? ¿ordenadores de la empresa?) y, aunque el particular los destruya -los borre-, la empresa gestora del sistema sigue "almacenando" los datos *sine die* -lo que permite a los tribunales, por ejemplo, acceder a ellos, aunque también podrían ser utilizados con otros fines que desconocemos-.

Como consecuencia se hace necesario abrir el debate sobre la existencia o necesidad de protección de nuevos bienes jurídicos – ¿"sistema democrático" ?; ¿"diálogo social" ...-, y, en consecuencia, el debate dogmático acerca de los ámbitos de intervención del Derecho penal. Volveremos a la tensión entre Derecho penal mínimo y expansión de la intervención penal, y en su caso, estos nuevos valores tan amplios, genéricos, abstractos quizá fuercen a la adopción de nuevas modalidades de tipos penales, con estructuras típicas controvertidas, pero quizá necesarios cuando la intervención penal ha de centrarse en "el arma" y no en el "resultado", habida cuenta de su posible intensidad, gravedad y extensión.

5. LA TIPICIDAD PENAL: EL DISEÑO DE LO PROHIBIDO

Efectivamente, deberán buscarse nuevas fórmulas típicas que no se limiten al binomio delitos de resultado/delitos de mera actividad -siempre legitimados por un bien jurídico protegido-. Probablemente sea necesario recurrir a delitos de infracción de deber, categoría no siempre admitida por la Doctrina penal, aunque sí lo haya hecho abiertamente la Jurisprudencia, por ejemplo, en el delito de fraude fiscal -si bien de una forma *híbrida,* es decir, junto con un bien jurídico protegido-[8]. Pues bien, es muy probable que sea necesario hacer depender la acción penal de la infracción de deberes de conducta (obligaciones de hacer o prohibiciones) tal y como hace, precisamente, el art. 5 del RIA -si bien, en este caso, como veremos, la imposición de una sanción administrativa exige, aparentemente, además de la infracción de la prohibición la producción de un resultado lesivo o de puesta en peligro.

Ahora bien, para evitar excesos frente a los que la Doctrina ha reclamado la razón legitimante del bien jurídico protegido, sería conveniente vincular la intervención penal

[8] Pue de verse más ampliamente sobre esta cuestión DE LA CUESTA AGUADO, "Redistribución de la riqueza y delito tributario", en *Estudios Penales y Criminológicos*, 42 (2022), p. 9.

derivada de la infracción de un deber a la protección de un bien jurídico protegido. Por ejemplo, una de las conductas permitidas con restricciones es la de la identificación biométrica en determinadas circunstancias. Pues bien, en aquellos supuestos en los que se infrinjan los deberes de control o de prudencia -siempre que tales deberes puedan ser enunciados suficientemente- su infracción podría ser constitutiva de delito en la medida en que el control biométrico de la población y de las personas atenta gravísimamente contra la intimidad, el derecho a la propia imagen, la autonomía de la voluntad y, probablemente, la integridad moral. En este supuesto, entre otros posibles, la realización de tales conductas es tan peligrosa para las personas y el propio sistema social que infracción de los deberes que establecen límites de actuación podría ser ya constitutivo de delito -y por tanto, de un delito de infracción de un deber- siempre que tales deberes derivaren de la protección de bienes jurídicos personalísimos o de la infracción de deberes reconocidos constitucionalmente[9].

Para hacer frente a sistemas algorítmicos autónomos, es decir, aquellos cuyos resultados (o decisiones) no dependen de un actuar humano y no se pueda saber exactamente cuál puede ser la respuesta a la solicitud o demanda (*prompt*) que se le hace – o sea, cuando el algoritmo toma "sus propias decisiones"-, los sistemas de imputación actualmente existentes se muestran insuficientes. De modo que se deberán buscarse fórmulas típicas que permitan responsabilizar a las personas que utilicen los sistemas algorítmicos para producir resultados lesivos o cometer delitos y, también, se deberá exigir responsabilidad penal a las personas jurídicas en cuyo seno o en cuyo beneficio surja el delito. Además, se hace necesario arbitrar sistemas de exigencia de responsabilidad personal "en cascada" de forma similar a como lo hace el art. 30 del Código penal español en relación con la comisión de delitos en publicaciones tradicionales[10].

---

[9] Esta última posibilidad era propuesta, en relación con el art. 320 CP, por DIPSE, V., *Las omisiones típicas en el delito de prevaricación urbanística*, Tirant Lo Blanch, Valencia, 2021, p. 104.

[10] Dice el artículo 30 del Código penal español:

"1. En los delitos que se cometan utilizando medios o soportes de difusión mecánicos no responderán criminalmente ni los cómplices ni quienes los hubieren favorecido personal o realmente.

2. Los autores a los que se refiere el artículo 28 responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden:

1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo.

2.º Los directores de la publicación o programa en que se difunda.

3.º Los directores de la empresa editora, emisora o difusora.

4.º Los directores de la empresa grabadora, reproductora o impresora.

3. Cuando por cualquier motivo distinto de la extinción de la responsabilidad penal, incluso la declaración de rebeldía o la residencia fuera de España, no pueda perseguirse a ninguna de las personas comprendidas en

Pero, si nos enfrentamos a "decisiones autónomas", con resultados -fruto de "cajas negras"- imposibles de prever o de explicar por quienes han construido, puesto en marcha o utilizado el sistema de IA, se hace necesario buscar nuevos modelos de imputación y de exigencia de responsabilidad penal[11], o, al menos, nuevos sistemas de imputación que conduzcan a adoptar decisiones similares a la imposición de una pena a una persona física o jurídica. Y de esta afirmación van a derivar, al menos, dos consecuencias. En primer lugar, la exigencia de responsabilidad penal ha de dirigirse de forma autónoma -es decir, independiente de la responsabilidad de las personas físicas o jurídicas implicadas- y en base a nuevos criterios de imputación, que en estos momentos aparecen muy difíciles de precisar y, en segundo lugar, las penas o sanciones penales han de ser distintas a las tradicionales. Así, si la pena por antonomasia para las personas físicas es la privación de libertad y, para las personas jurídicas, la multa; para estos sistemas algorítmicos la pena prioritaria probablemente haya de ser la supresión, destrucción o desaparición del sistema (algo equivalente a la pena de muerte, en personas físicas, o la pena de disolución, en personas jurídicas). Ahora bien, la aplicación (o configuración) de esta sanción penal ha de implicar la desaparición del algoritmo -probablemente en otros sistemas algorítmicos, lo que generará nuevas prohibiciones- y la desaparición incluso del propio modelo matemático que constituye el algoritmo. Ciertamente, ambas cuestiones se tornan francamente inaccesibles en este momento y ponen de manifiesto los importantes obstáculos que ha de vencer el sistema penal para hacer frente a estas nuevas realidades. A todo ello habrá que sumar que los sistemas de prevención (también sistemas informáticos o algorítmicos) destinados a evitar la utilización de tal software prohibido como si de un software malicioso se tratare.

Una aproximación a la realidad social y de los efectos que producen las tecnologías que utilizan sistemas algorítmicos, cualquiera que sea su finalidad, y muy especialmente, una aproximación al uso que puede hacerse en entornos de comunicación social como pudieran ser RRSS, programas de "Inteligencia generativa", buscadores, etc., invitan a pensar que, mientras que algunos de los efectos pueden ser delictivos, conforme a tipos penales ya existentes tal y como están – o con adaptaciones mínimas-, en otras ocasiones, los efectos reales o posibles

alguno de los números del apartado anterior, se dirigirá el procedimiento contra las mencionadas en el número inmediatamente posterior."

[11] DE LA CUESTA AGUADO, PM., "Inteligencia artificial y responsabilidad penal", en *Revista penal México*, N.º 16-17, 2019-2020, pp. 51-62. Disponible en línea en https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/336/266 [citado:21.04.2025].

altamente perjudiciales no están actualmente previstas por la legislación penal, simplemente, porque son consecuencia de comportamientos que no eran imaginables porque no existía la tecnología que los genera.

En el primer supuesto -conductas susceptibles de ser típicas conforme a la actual legislación penal- entrarían posibles estafas, delitos contra la intimidad, delitos de odio, revelación de secretos -o, más bien, de datos personalísimos-, o injurias o calumnias. Ahora bien, aunque los efectos e incluso el *modus operandi* pudiera ser similar a alguna de estas conductas típicas o producir resultados similares a otros delitos clásicos, las modalidades de conducta pueden ser muy innovadoras y, sobre todo, los posibles efectos muy graves y extensos en cuanto al número de víctimas o de perjuicios.

Entre estos perjuicios, podemos encontrar algunos no previstos hasta este momento. Algunos incluso, como ya hemos advertido, afectarían a modelos de comunicación social, a las posibilidades reales de participación política o al propio sistema democrático. Todos ellos, intereses necesitados de protección genéricos, pero respecto de los que la modalidad de conducta puede ser muy parecida a las descritas en el párrafo anterior. De modo que, tal vez, sea necesario recurrir a nuevas "especies de tipicidad", tipos "universales" o "de extensos efectos no completamente determinados", y que podrían estar configurados por un elemento estructural -una conducta "clásica" o un delito ya existente- al que se sumaría un elemento nuevo, que determina y condiciona el salto punitivo de delito tradicional o conducta atípica a la nueva modalidad delictiva cometida con sistemas algorítmicos. Este nuevo elemento condicionante podría tratarse de un elemento circunstancial, que constituiría una especie de criterio de asignación de la conducta o, de un elemento tendencial -como sucede, al menos, en los delitos de terrorismo, genocidio o lesa humanidad-.

En cualquier caso, estas construcciones típicas partirían de modalidades delictivas ya preexistentes (o muy parecidas). La incorporación de normas que obliguen a las empresas que pongan en circulación o exploten comercialmente o, sencillamente, usen sistemas algorítmicos prohibidos o de alto riesgo invita a pensar en la posibilidad de incorporar normas penales que sancionen penalmente a quienes infrinjan de forma graves dichas obligaciones o actúen en contra de lo autorizado o sin autorización, ya sea provocando con ello nuevos peligros o lesiones, o, simplemente, mediante la infracción de los deberes impuestos normativamente para el control de la actividad. De nuevo, surgirían modalidades típicas que sancionan infracciones de deberes normativamente impuestos. Ahora bien, quizá, solo quizá, la gravedad de los

peligros que derivan de estas actividades, la dificultad para detectarlos y el altísimo número de personas afectadas (en su caso) exija replantearse adecuar a los requisitos propios de un Estado de Derecho estas modalidades típicas no siempre bien recibidas por la doctrina.

6. LA DIGNIDAD HUMANA Y LAS MINAS DE DATOS

Es muy llamativo que las prácticas permitidas del art. 5 RIA -sistemas biométricos que no se usen en tiempo real, por ejemplo- prescindan absolutamente del consentimiento. El RIA no hace referencia alguna a si es preciso, para que tales prácticas sean autorizadas, permitidas o consentidas por la persona afectada; es decir, no hace referencia a la necesidad de que dicha persona otorgue su consentimiento y con qué requisitos, tal y como, por ejemplo, exige el Tribunal Constitucional español. Es más, el considerando (15) del RIA dice expresamente que *[E]l concepto de «identificación biométrica» a que hace referencia el presente Reglamento debe definirse como el reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla, a fin de determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos de referencia,* ***independientemente de que la persona haya dado o no su consentimiento***[12]**.**

Es decir, en sus Considerandos, el RIA *prescinde* de la necesidad de recabar el consentimiento del sujeto pasivo. El argumento fácil aquí es afirmar la necesidad de estos sistemas de identificación biométrica por razones de seguridad. No podemos entrar en esta cuestión en este momento, pero, permítaseme preguntar al lector qué es más importante, la seguridad pública -concepto absolutamente indefinido y en manos de quien detenta el uso de la fuerza- o la dignidad de las personas. La respuesta a esta pregunta, por cierto, históricamente a delimitado las democracias de "otras formas de gobierno".

Pero más allá de esta cuestión, la ausencia de relevancia del consentimiento en esta y otras prohibiciones o conductas descritas por el RIA trae a la palestra una cuestión que se está convirtiendo en central en el debate sobre la intervención penal. O dicho de otra forma: la forma de emisión y la validez del consentimiento se está revelando como un elemento que debería ser

[12] La negrita es mía.

esencial para cualquier conducta o práctica de sistemas de IA autorizado que afectare a datos sensibles y, en el ámbito penal o, incluso, sancionado-administrativos, debería considerarse como elemento imprescindible para excluir la tipicidad.

Por ello, también aquí, se hace necesario afrontar cuestiones como cuál será la validez del consentimiento otorgado cuando no queda más remedio (porque si no, no puedes acceder a la red, por ejemplo); qué consecuencias se asumen cuando se otorga el consentimiento y este va a permitir utilizar los propios datos personales de forma insospechada para quien lo otorga; o cuál sería la responsabilidad de quien conserva datos cuyo titular ha querido destruir y luego, incluso a requerimiento judicial, los difunde en su contra o sin su consentimiento. Y, como se puede intuir, en estas cuestiones no se trata solo de limitar el (eventual) abuso por parte de particulares (empresas), sino también y muy especialmente, de limitar el poder del Estado contra las personas -lo que, por cierto, es una de las funciones más importantes del Derecho penal democrático-.

Especialmente sensible es el problema del consentimiento para el uso de estas tecnologías por menores, algo que, hasta ahora, ha quedado obviado por la férrea negativa de las empresas a admitir restricciones protectoras de los menores y del desconocimiento de los riesgos de gran parte de la población. En España, la situación parece empezar a cambiar con el Anteproyecto de Ley Orgánica para la protección de menores de edad en los entornos digitales[13], pero ello no evita que esta cuestión deba recibir también una respuesta penal.

El problema del consentimiento, en los sistemas penales que conocemos es una cuestión no resuelta. Muy someramente podría afirmarse que en aquellos supuestos en los que el sujeto pasivo es reconocido como personas -es decir, en plenitud de derechos y deberes- al consentimiento se le da una eficacia plena, cualquiera que sea la forma en que este se vea anulado (violencia, intimidación, fuerza o engaño). Este es el caso de los delitos patrimoniales, donde el consentimiento válido tiene efectos destipificadores y el consentimiento inválido -incluso mediando engaño- convierte la conducta en típica y generadora de la responsabilidad penal.

Sin embargo, en aquellos otros delitos en los que al sujeto pasivo no se le reconoce tal "plenitud de derechos", generalmente porque es muy vulnerable frente al sujeto activo o porque se le considera inferior en derechos, solo se tiende a reconocer como causa que excluye el

[13] https://www.congreso.es/public_oficiales/L15/CONG/BOCG/A/BOCG-15-A-52-1.PDF [citado: 5 de mayo de 2025]

consentimiento la fuerza o, en su caso, la intimidación -caso de los delitos contra la libertad sexual-. O dicho de otro modo, el consentimiento, que es la llave de la dignidad de la persona (concepto que debe ser entendido en sentido kantiano como fin en sí mismo y nunca instrumento de otro) solo se reconoce cuando al sujeto pasivo se le reconoce como igual. Pues bien, las fórmulas vacías para la obtención del consentimiento a que los sistemas basados en las nuevas tecnologías nos tienen acostumbrados; la ausencia de mención -o incluso expresa ineficacia- del consentimiento en el RIA o la utilización de nuestros datos personales por las plataformas, aplicaciones o *chatbots*, nos obliga a preguntarnos sobre qué papel juegan las personas frente a las empresas que explotan tales tecnologías.

¿Nos habremos convertido las personas en meras minas de datos frente a la IA de forma que el consentimiento, que es el reconocimiento de la dignidad de la persona, deviene innecesario?

ANEXO I

Artículo 5 del Reglamento de Inteligencia Artificial

Prácticas de IA prohibidas

1.Quedan prohibidas las siguientes prácticas de IA:

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 o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;
b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;
c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a

características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas 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 de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;
e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;
f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad;
g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;
h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de víctimas concretas de secuestro trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

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

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y 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 tendría el uso del sistema en 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 garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), del presente artículo deberá cumplir garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con el Derecho nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el

sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.

3. A los efectos del apartado 1, párrafo primero, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le aporten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos especificados en el apartado 1, párrafo primero, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el apartado 2. Dicha autoridad no podrá adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota «en tiempo real».

4. Sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

5. 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 garantía del cumplimiento del Derecho dentro de los límites y en las condiciones que se indican en el apartado 1, párrafo primero, letra h), y los apartados 2 y 3. Los Estados miembros de que se trate deberán establecer en sus respectivos Derechos nacionales 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 y la presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho. Los Estados miembros notificarán dichas normas a la Comisión a más tardar treinta días después de su adopción. Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

6. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho con arreglo al apartado 4 presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o una autoridad administrativa independiente cuya decisión sea vinculante en relación con las solicitudes de autorización de conformidad con el apartado 3, así como su resultado.

7. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho elaborados basados en datos agregados relativos a los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de garantía del cumplimiento del Derecho conexas.

8. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de Derecho de la Unión.