COMUNICACIÓN: LA SEGURIDAD EN EL FUTURO REGLAMENTO UE SOBRE IA.

Francisco L. Pérez Guerrero.

RESUMEN

La Seguridad Pública recibe la atención del proyecto de nuevo Reglamento de la UE de IA, no sólo como bien jurídico a proteger, sino también en algunas manifestaciones que se consideran de alto riesgo si usan la IA, como en lo relativo al uso de la identificación biométrica, las infraestructuras críticas, el intercambio de información policial o el control de la inmigración. Preocupa la apertura a la identificación biométrica, así como la exclusión de lo relativo a la actividad militar o intercambio de información a nivel internacional, así como la nula alusión directa a las armas y explosivos. Supondrá un enorme avance en una regulación hasta ahora inexistente, pero traerá consigo un esfuerzo en adaptación de normativa nacional a nuevos escenarios.

ABSTRACT

Public Security receives attention in the draft new EU Regulation on AI, not only as a legal good to be protected, but also in some manifestations that are considered high-risk if they use AI, such as in relation to the use of biometric identification, critical infrastructures, the exchange of police information or immigration control. The openness to biometric identification is of concern, as is the exclusion of military activity or international information sharing, as well as the lack of any direct reference to weapons and explosives. It will represent a huge step forward in a regulation that did not exist until now, but it will entail an effort to adapt national regulations to new scenarios.

PALABRAS CLAVE

Seguridad, IA, Biometría, Exclusiones, Adaptación.

KEY WORDS

Security, AI, Biometrics, Exclusions, Adaptation.

A) **SUMARIO:** ***1. Introducción. 2. La presencia de la seguridad en el Reglamento UE de Inteligencia Artificial.*** *A) Las alusiones directas. B) Las exclusiones. C) Las prohibiciones: un riesgo inaceptable.* **3. *La aplicación a actividades relacionadas con la seguridad consideradas de alto riesgo.*** *A) El uso de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de aplicación de la ley. B) Los sistemas de IA en relación con las infraestructuras críticas. C) Las actuaciones policiales: las actuaciones de las autoridades encargadas de la aplicación de la ley que implican determinados usos de sistemas de IA. D) Los sistemas de IA empleados en la gestión de la migración, el asilo y el control fronterizo.* ***4. Ausencias y retos de adaptación.***

1. Introducción.

Hacer un análisis del futuro Reglamento de la Unión Europea sobre Inteligencia artificial, desde la perspectiva de la Seguridad, puede aportarnos una interesante visión de la trascendencia que, en esta materia, en sus términos más amplios, pero particularmente en la Seguridad Pública, va a tener la incorporación de sistemas de inteligencia artificial, de ahí el sentido de esta comunicación. No sólo se acredita dicha trascendencia, sino que también, se deduce la futura tarea de adaptación de las normativas nacionales de los Estados miembros, como España. A este propósito se dedican estas líneas.

2. La presencia de la seguridad en el Reglamento UE de Inteligencia Artificial[1].

A) Las alusiones directas.

De la lectura de los Considerando 1, 3 y 5[2], se observa que, entre los fines imperiosos de interés general que persigue el RIA, se cita expresamente la seguridad y los derechos humanos, de modo coherente, en nuestra opinión, dada la histórica indisoluble relación entre ambos conceptos. Y el artículo 3. 44 del RIA, define lo que considera un <<Incidente grave>> como: "todo incidente que, directa o indirectamente, tenga, pueda haber tenido o pueda tener alguna de las siguientes consecuencias: a) el fallecimiento de una persona o daños graves para su salud, para los bienes o para el medio ambiente; (…)" lo que entronca, exactamente, con la definición de los propósitos que persigue la

[1] En adelante RIA.
[2] En adelante, Cnum. Por ejemplo: C1.

Seguridad Pública, que son los de prevenir, proteger y evitar daños a la vida de personas y de los bienes públicos, con mayor razón en casos de fallecimiento.

Los riesgos que se pretenden evitar con la aplicación del RIA a los sistemas de IA afectan a tres bienes jurídicos mencionados expresamente[3]: la salud, la seguridad y los derechos fundamentales, de ahí la relevancia y centralidad de la seguridad en esta materia de la IA[4].

En coherencia con el enfoque decidido, basado en los riesgos, y excluidas las prácticas prohibidas, los sistemas de IA-AR están permitidos en la UE siempre que cumplan determinados requisitos obligatorios y sean sometidos a una evaluación de la conformidad con anterioridad a su aplicación[5]. La clasificación de un sistema como IA-AR depende de varios factores: (1) la función que lleve a cabo, (2) la finalidad específica y (3) las modalidades para las que se use. Se consideran 2 categorías principales de sistemas de IA-AR: (1) los sistemas de IA diseñados para utilizarse como componentes de seguridad de productos sujetos a una evaluación de la conformidad "ex ante" realizada por terceros; y (2) otros sistemas de IA independientes con implicaciones relacionadas principalmente con los derechos fundamentales, los cuales se indican explícitamente en el anexo III. Dicha lista es susceptible de ser ampliada por la Comisión con determinadas condiciones. Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a: (1) la calidad de los conjuntos de datos utilizados, (2) la documentación técnica y el registro, (3) la transparencia y la comunicación de información a los usuarios, (4) la vigilancia humana, (5) la solidez, (6) la precisión y (7) la ciberseguridad. Siendo todos ellos susceptibles de detallados análisis, haremos alusión al último, dada la directa relación con nuestro enfoque: la ciberseguridad como respuesta a los ciberataques. El RIA califica como fundamental la ciberseguridad para contrarrestar o defender los sistemas de actuaciones de terceros maliciosos. Tales actuaciones pretenden aprovechar las vulnerabilidades de los mismos para alterar el uso, conducta o funcionamiento previstos, o para poner en peligro sus propiedades de seguridad. Dichos ciberataques podrían tener

[3] Considerando 43.
[4] Además, el RIA, respecto del espacio de libertad, seguridad y justicia gestionado por EU-LISA (Agencia de la UE para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud), en lo que respecta a los sistemas de IA que son componentes de sistemas de gran magnitud en este espacio, contempla un plazo de no aplicación de 1 año, a los que entren en el mercado en ese período de tiempo anterior a la entrada en aplicación del RIA.
[5] Título III del RIA.

3 tipos de planos: (7.1) los dirigidos contra elementos específicos de la IA, como los conjuntos de datos de entrenamiento, o los modelos entrañados, (7.2) los que puedan aprovechar las vulnerabilidades de los elementos digitales del sistema de IA, o (7.3) los que pueden dirigirse contra la infraestructura de TIC subyacente.

B) Las exclusiones.

Antes de entrar a analizar los sistemas de IA que pudieran estar relacionados con la seguridad contemplados en el RIA es importante detenerse en dos exclusiones de la regulación que tienen clara relación con nuestro enfoque.

La exclusión de los sistemas de IA aplicados a el intercambio de información y pruebas con fines de cooperación policial y judicial (C11). Para respetar los acuerdos existentes a nivel internacional con terceros países, así como las necesidades especiales de cooperación con socios extranjeros. Esto implica no aplicación a las autoridades públicas de un tercer país, ni a las organizaciones internacionales, si se actúa en acuerdos internacionales, celebrados a escala nacional o europea, para la cooperación policial y judicial, ya sea con la UE o con sus Estados miembros. Se refiere el RIA a dos tipos de acuerdo: (1) los celebrados bilateralmente entre los Estados miembros y terceros países, y (2) los celebrados entre la UE, Europol y otras Agencias de la UE y terceros países y organizaciones internacionales.

La exclusión de los sistemas de IA con fines militares (C12). Quedan excluidos los sistemas de IA cuyo desarrollo o utilización sea con fines exclusivamente militares, cuando su uso sea competencia exclusiva de la política exterior y de seguridad común (Título V del TFUE). Esta última exclusión puede generar más dudas, acerca del acotamiento de su extensión, ya que las líneas entre lo militar y lo civil, por ejemplo, en materia de armas, están cada vez más difusas, así como las amenazas a la seguridad tampoco permiten seguir un esquema más clásico de la seguridad que divide ésta en interior y exterior.

C) Las prohibiciones: un riesgo inaceptable.

La prohibición a las autoridades públicas de la utilización de ciertos sistemas de IA que pudieran estar relacionados con la seguridad (Articulo 5.1.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". Se prohíben ante la existencia del riesgo cierto de que estos sistemas, que generan calificaciones sociales, puedan tener resultados discriminatorios de personas, atacando directamente al derecho de la dignidad de la persona, la no discriminación e igualdad y al valor de la justicia, además de no fiables, abriendo la posibilidad de un trato desfavorable o perjudicial a personas físicas y a colectivos que pueden sufrir un trato injusto derivado de situaciones y contextos que anteceden a la aplicación del sistema.

3. La aplicación a actividades relacionadas con la seguridad consideradas de alto riesgo.

A) *El uso de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de aplicación de la ley (C8, 9, 18 a 24).*

Cabe comenzar el análisis de este apartado aclarando que se ha manejado el texto que fue recibido en el Parlamento Europeo, anterior a la presentación de enmiendas, de tal forma que lo aquí indicado está basado en lo hasta ahora publicado[6].

El artículo 5.1.d) establece la prohibición de "El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley …" y excepciona, es decir, permite su uso, en tres supuestos tasados: "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

[6] Como es conocido, tras los trílogos, se ha llegado a acuerdos sobre el texto, que habrá de someterse de nuevo a aprobación, esta vez definitiva, si bien del contenido de dicho resultado tan sólo es, en el momento de escribir esta comunicación (debiendo entregarse antes del 20 de diciembre), lo conocido a través de un comunicado de prensa de las instituciones europeas.

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, 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." Con respecto a esta última medida, existen 32 delitos enumerados en la citada Decisión.

Es evidente que el uso de este tipo de sistemas de IA invade, de modo muy relevante, derechos y libertades, fundamentalmente relacionados con la privacidad, que puede conducir a efectos no tolerados por un Estado de Derecho como la sensación de estar bajo una vigilancia constante, o la falta de libertad para ejercer derechos tan elementales como el de reunión. El hecho de operar en tiempo real, su inmediatez, hace inviables técnicas que aseguran las decisiones tales como la comprobación o la corrección, lo que las hace más susceptibles aún de poner en riesgo los derechos fundamentales más elementales. Coherentemente con ello, la decisión es prohibirla y sólo permitirla en tres situaciones acotadas.

Todo ello se somete a una serie de garantías, contrapesos, requisitos y condiciones de muy diversa índole, debiendo hacerse una valoración de diversos intereses contrapuestos. Así, debe valorarse la naturaleza de la situación que dé lugar al posible uso, concretamente, debe valorarse la gravedad, probabilidad y magnitud del perjuicio que se produciría en caso de no utilizarse el sistema. Igualmente, las consecuencias de su utilización respecto de los derechos y libertades de las personas implicadas, valorando también su gravedad, probabilidad y magnitud. En cuanto a su uso, se le aplicará criterios de necesidad y proporcionalidad desde el punto de vista de tres parámetros: las limitaciones temporales, geográficas y personales.

Se requiere la concesión de la una autorización previa por una autoridad judicial o por una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse. Con ello, se establece un control preventivo de estas actuaciones, garantizando la independencia de la autoridad otorgante, utilizando una técnica clásica de control como

es la autorización. Ha de solicitarse, con motivación, de acuerdo con la normativa de Derecho interno. Se exige que la autoridad esté convencida de su necesidad y proporcionalidad para alcanzar los objetivos del RIA, a la vista de las pruebas objetivas e indicios claros presentados. Cabe la posibilidad, ante una situación de urgencia debidamente justificada, comenzar a utilizar el sistema sin autorización, pudiéndose solicitar durante el uso o después de éste, si bien las fuerzas y cuerpos de seguridad deben tratar de obtenerla lo antes posible e indicar los motivos por lo que no han podido hacerlo antes.

Se habilita a los Estados miembros a dotarse de estos sistemas dentro de los límites contemplados en el RIA. Para ello, deberán aprobar en su Derecho interno las normas aplicables a la solicitud, la concesión y el ejercicio de autorizaciones, señalando cuáles de los objetivos y delitos de los indicados en el RIA serían afectados por la medida.

El propio RIA, utiliza varios Considerandos para precisar la terminología que emplea. Comienza aclarando que la expresión <<datos biométricos>> que utiliza el RIA es la misma que la que ya se viene utilizando por la UE en otros Reglamentos que abordan materias relacionadas con los mismos[7]. Por «sistema de identificación biométrica remota» debe entenderse, "de manera funcional, como un sistema de IA destinado a identificar a distancia a personas físicas comparando sus datos biométricos con los que figuren en una base de datos de referencia, sin saber de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen". Pero, como se puede observar, el RIA habla de sistemas <<en tiempo real>>, lo que los distingue de los sistemas <<en diferido>>. Cuando se refiere a los sistemas <<en tiempo real>>, se tiene en cuenta que la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea, casi, o sin una demora significativa, no permitiéndose que bajo el argumento de demoras mínimas se eluda la aplicación del RIA. Para ser considerado <<en diferido>> la demora debe ser significativa. Por otra parte, otro factor de diferenciación viene determinado por el tipo de grabaciones que usamos,

[7] definida en el artículo 4, punto 14, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo35; en el artículo 3, punto 18, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo36; y en el artículo 3, punto 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo.

de tal forma que el sistema en tiempo real maneja grabaciones de video generadas por una cámara o un dispositivo similar en directo o casi en directo, mientras que los sistemas en diferido usan datos ya recabados, grabados y almacenados procedentes de cámaras de televisión de circuito cerrado o dispositivos privados, generados antes de aplicar este sistema a la persona a identificar. Finalmente, el RIA aclara qué se entiende por <<espacio de acceso público>>, refiriéndose a cualquier lugar físico al que tenga acceso el público, con independencia de si es de propiedad privada o pública. Entrando en detalle y situaciones concretas que pudieran generar dudas: (1) no abarca aquellos lugares privados a los que no pueden acceder libremente terceros, incluidas las fuerzas o cuerpos de seguridad, a menos que se hayan invitado o autorizado, como viviendas, clubes privados, oficinas, almacenes y fábricas; (2) Tampoco cubre los espacios en línea, ya que no son espacios físicos; (3) el simple hecho de que se cumpla determinadas condiciones para acceder a un espacio concreto, como la adquisición de entradas o restricciones en relación con la edad.

El hecho de tratar con datos biométricos hace que la coordinación con la normativa europea que regula los mismos, concretamente, la DIR (EU) 2016/680.

B) *Los sistemas de IA en relación con las infraestructuras críticas (C34).*

El RIA menciona los sistemas de IA cuando son componentes de seguridad en la gestión y el funcionamiento de 5 de ellas, concretamente, las de tráfico rodado, suministro de agua, gas, calefacción y electricidad, y ello porque un fallo en dichos sistemas puede generar efectos sobre la vida y la salud de las personas a gran escala, alterando gravemente el desarrollo habitual de las actividades sociales y económicas. La duda a resolver es por qué se queda en esa enumeración, ya que como todas genera la incertidumbre de si estamos ante una relación tasada o, por el contrario, ejemplificativa, siendo evidente que hay más infraestructuras que admiten el adjetivo de críticas.

C) *Las actuaciones policiales: las actuaciones de las autoridades encargadas de la aplicación de la ley que implican determinados usos de sistemas de IA (C38).*

El artículo 3. 40 del RIA, define «Autoridad encargada de la aplicación de la ley» como: a) toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública; o b) cualquier

otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública. Por su parte, en el apartado 41, se define qué se entiende por «Aplicación de la ley»: las actividades realizadas por las autoridades encargadas de la aplicación de la ley para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública. El factor que preocupa en la UE por este uso de IA es el desequilibrio de poder dado en esta relación, pues el resultado del sistema puede amparar la vigilancia, la detención o la privación de libertad de una persona física, acciones de gran trascendencia sobre los derechos de una persona y que el poder público puede decidir. Si no se aseguran requisitos a ese sistema, podría generarse incorrectas, injustas y discriminatorias aplicación de la norma, llevando a impedir el ejercicio de derechos procesales como la presunción de inocencia, defensa, tutela judicial efectiva y al juez imparcial. Tales requisitos son los ya reiterados en otras aplicaciones de la IA, cuya importancia se acentúa dada la gravedad y trascendencia de los derechos y libertades afectados por tales medidas: (1) la buena calidad de los datos con los que se dota al sistema de IA, (2) el cumplimiento de la exigencia de precisión o solidez, (3) la prueba previa antes de la introducción en el mercado y puesta en servicio, (4) la transparencia y documentación.

Es obvia la consideración de estos sistemas de IA como de alto riesgo, señalando varios que no ofrecen dudas: (1) los de realización de evaluaciones del riesgo individuales; (2) los polígrafos y herramientas similares; (3) los sistemas utilizados para detectar el estado emocional de una persona física; (4) los de detección de ultra falsificaciones; (5) los que evalúan la fiabilidad de la prueba en un proceso penal; (6) los utilizados para predecir la comisión o reiteración de un delito real o potencial mediante la elaboración de perfiles de personas físicas; (7) los que evalúan rasgos y características de la personalidad o conductas delictivas pasadas de personas físicas o grupos; (8) las utilizadas para elaborar perfiles durante la detección, la investigación o el enjuiciamiento de infracciones penales, y para realizar análisis penales en relación con personas físicas. Excluye de la consideración de alto riesgo a los sistemas de IA usados para prevenir, detectar, investigar

y enjuiciar infracciones penales, si las autoridades fiscales y aduaneras los utilizan en los procesos administrativos con esta finalidad.

D) *Los sistemas de IA empleados en la gestión de la migración, el asilo y el control fronterizo (C39).*

El riesgo que se detecta en este ámbito de actuación se basa en la situación de especial vulnerabilidad de las personas que se encuentran incursas en estas operaciones lideradas por las autoridades públicas. Los derechos fundamentales potencialmente afectados son 5: los de libre circulación, no discriminación, intimidad personal y protección de datos personales, la protección internacional y la buena administración. Por ello, se exige que estos sistemas de IA sean precisos, no discriminatorios y transparentes. De nuevo, el RAI nos relaciona un listado de sistemas que deben considerarse de alto riesgo, utilizados como: (1) polígrafos y herramientas similares o para detectar el estado emocional de una persona física; (2) evaluación de ciertos riesgos que presenten personas físicas que entren en el territorio de un Estado miembro o soliciten un visado o asilo; (3) verificación de la autenticidad de los documentos pertinentes de personas físicas; (4) ayuda a las autoridades públicas competentes a examinar las solicitudes de asilo. Todo ello, sin perjuicio del cumplimiento de la normativa específica que regula esta materia y sus requisitos procedimentales[8].

Una precisión interesante es la que realiza el RIA, en su C41, a propósito de los varias veces mencionados polígrafos o dispositivos de similar utilidad que pretenden la detección del estado emocional de una persona física. Lo hace en relación a la protección de datos y a su normativa específica, aclarando que el hecho de la consideración de uno de esos sistemas como de alto riesgo no implica un indicador del uso legal de dichos datos, sino que habrá que estar, a efectos de cumplimiento de la legalidad, a la aludida normativa específica tanto de la UE como del Derecho interno de los Estados miembros. Este RIA no puede considerarse fundamento jurídico para el tratamiento de los datos personales, incluidas categorías especiales de datos personales.

[8] Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para la concesión o la retirada de la protección internacional (DO L 180 de 29.6.2013, p. 60) y Reglamento (CE) n.º 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados) (DO L 243 de 15.9.2009, p. 1),

4. Ausencias y retos de adaptación.

La falta de mención a las armas, con lo que la IA está avanzando en esto, aunque deben considerarse sistemas de alto riesgo, y la necesaria adaptación de la normativa nacional como la Ley Orgánica de Protección de la Seguridad Ciudadana, la de videovigilancia o las relativas al manejo de datos por la policía en investigaciones, serán objeto de preocupación.

BIBLIOGRAFÍA

Ballesteros Moffa, Luis Ángel (2020): *Las fronteras de la privacidad: el conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica.* Granada, Ed. Comares, 247pp.

Gamero Casado, Eduardo (Dir) (2023): *Inteligencia Artificial y Sector Público. Retos, límites y medios.* Valencia, Tirant lo Blanch, 792pp.

Suárez Xavier, Paulo Ramón (2022): *Reconocimiento facial y policía predictiva: entre seguridad y garantías procesales.* A Coruña, Colex, 117pp.