Autoritat Catalana de Protecció de Dades

Les autoritats de protecció de dades i el Reglament d'intel·ligència artificial

Nous rols i responsabilitats

Autoria: Daniel Duro Millan i Tatiana Bianca Vulpe beneficiaris de les dues beques de formació en matèria de protecció de dades personals per a l'any 2024, convocades mitjançant la Resolució de 10 de maig de 2024 (DOGC núm. 9165, de 17/5/2024).

Coordinació APDCAT: Joana Marí Cardona, delegada de protecció de dades i responsable de Projectes Estratègics, i Guillem López Sanz, responsable de Relacions Institucionals i Organització.

Generalitat de Catalunya

apdcat
Autoritat Catalana de Protecció de Dades

Índex

Abreviatures

AEPD: Agència Espanyola de Protecció de Dades

APD: autoritat de control de protecció de dades

APDCAT: Autoritat Catalana de Protecció de Dades

APDF: autoritat de protecció de drets fonamentals

AVM: autoritat de vigilància del mercat

CEPD: Comitè Europeu de Protecció de Dades

DF: drets fonamentals

DOUE: Diari Oficial de la Unió Europea

EM: estats membres

FRA: Agència Europea de Drets Fonamentals

IA: intel·ligència artificial

NIS2: Directiva (UE) 2022/2555, relativa a les destinades a garantir un elevat nivell comú de ciberseguretat a tota la Unió

NVS: notificació de violació de seguretat

RD: Reial decret

RGPD: Reglament general de protecció de dades

RIA: Reglament d'intel·ligència artificial

RMD: Reglament de mercats digitals

RSD: Reglament de serveis digitals

RT: responsable del tractament

RVM: Reglament de vigilància de mercat

SIA: sistema d'intel·ligència artificial

TFUE: Tractat de funcionament de la UE

TJUE: Tribunal de Justícia de la Unió Europea

UE: Unió Europea

1. Introducció

Tatiana Bianca Vulpe i Daniel Duro Millan

Les paraules de P. Ovidius Naso continuen essent plenament vigents: *Datae leges, ne fortis omnia posset* —s'han donat lleis perquè el fort no ho pugui tot. Al llarg de la història, les normes jurídiques han servit per limitar els abusos de poder i garantir l'equilibri social. En l'era digital, aquesta necessitat es trasllada a l'àmbit tecnològic, on el desenvolupament de sistemes i models d'intel·ligència artificial (IA) planteja desafiaments ètics i jurídics que demanen una regulació clara i efectiva. Avui, més que mai, és essencial comptar amb un marc normatiu que impedeixi que es vulnerin els drets fonamentals, assegurant una IA alineada amb els valors i principis europeus.

En aquesta línia, el 12 de juliol de 2024 es va publicar al Diari Oficial de la Unió Europea (DOUE) el Reglament d'intel·ligència artificial (Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, d'ara endavant RIA). Aquesta disposició, amb efecte normatiu directe, representa un pas significatiu en la regulació i supervisió de tecnologies emergents a Europa, com ara la IA. El RIA es fonamenta principalment en l'article 114 del Tractat de funcionament de la Unió Europea (TFUE), que habilita la Unió a adoptar mesures per garantir l'establiment i el funcionament del mercat interior, respectant els principis de subsidiarietat i proporcionalitat; també es basa en l'article 16 del mateix tractat, que constitueix el fonament jurídic de la protecció de dades.

Tanmateix, la redacció del RIA ha estat marcada per les divergències entre els diferents actors implicats. Això s'exemplifica en els conflictes d'interessos i sobre l'abast normatiu que van sorgir al llarg del procés legislatiu. Alguns canvis significatius entre la proposta inicial i la definitiva són els següents:

- La incorporació de 91 nous considerants, destinats a precisar aspectes que generen inquietud, com ara la biometria.
- La incorporació dels conceptes *model* i *sistema d'IA d'ús general* en relació amb els sistemes d'IA generativa, atesos els riscos significatius de futur que presenten.[1]
- La introducció del concepte de risc sistèmic.[2]

[1] La inclusió dels models i sistemes d'IA d'ús general no estava previst inicialment al RIA, ni a la proposta de la Comissió Europea ni a l'orientació general del Consell. Aquesta incorporació va ser impulsada principalment per la irrupció de ChatGPT, desenvolupat per OpenAI, que va evidenciar la necessitat de regular aquests tipus de models també anomenats *fundacionals* o *de propòsit general*. Els models d'IA d'ús general es caracteritzen per ser entrenats amb grans volums de dades mitjançant diversos mètodes d'aprenentatge, com ara l'aprenentatge autosupervisat, el no supervisat o per reforç. Tot i la seva rellevància en el desenvolupament de la IA, aquests models no constitueixen per si sols sistemes d'IA complets, ja que necessiten altres elements per ser operatius, com ara una interfície d'usuari o mecanismes d'integració en aplicacions específiques (considerant 97 RIA).

[2] Aquest concepte s'integra a la regulació dels models d'IA d'ús general, ja que es reconeix com un dels riscos potencials que poden comportar. Això inclou "cualquier efecto negativo real o razonablemente previsible en relación con accidentes graves, perturbaciones de sectores críticos y consecuencias graves para la salud y la seguridad públicas, cualquier efecto negativo real o razonablemente previsible sobre los procesos democráticos

- L'addició de nous annexos.
- El reconeixement del dret a obtenir una explicació de decisions individuals (art. 86 RIA), en línia amb l'article 22 i el considerant 71 del Reglament general de protecció de dades (RGPD).
- El dret a presentar una reclamació davant una autoritat de vigilància de mercat (art. 85 RIA), novetat que permet als particulars adreçar-se directament a aquestes autoritats.

En aquest context, la solució adoptada finalment ha estat establir un marc normatiu que garanteixi la intervenció pública, però amb un grau de flexibilitat que permeti adaptar les obligacions segons la importància i l'impacte dels riscos associats. Així, el RIA adopta un enfocament basat en el risc (art. 26 i 27 RIA) i classifica els sistemes d'IA en quatre categories de risc diferents: (i) risc inacceptable (art. 5 RIA); (ii) alt risc (art. 6 i annexos I i III RIA); (iii) risc limitat o de transparència (obligacions de transparència d'acord amb l'art. 50 RIA); i (iv) risc mínim o nul.[3]

L'objectiu principal del RIA és millorar el funcionament del mercat interior i promoure l'adopció d'una IA centrada en l'ésser humà i fiable i garantir, alhora, un elevat nivell de protecció de la salut, la seguretat i els drets fonamentals consagrats a la Carta de drets fonamentals de la Unió Europea, inclosos la democràcia i l'estat de Dret (considerants 1, 2, 6, 7, 27 i 28; i art. 40.3 RIA). A més, el RIA es concep com una norma oberta i dinàmica, dissenyada per adaptar-se als avenços tecnològics i als nous reptes que pugui plantejar l'ús de la IA. Amb aquesta finalitat, inclou múltiples elements subjectes a desenvolupaments futurs i preveu facultats de modificació per a la Comissió Europea; d'aquesta manera, n'assegura la flexibilitat i capacitat d'adaptació a l'evolució del sector i a les necessitats reguladores emergents. Tot i que inicialment semblaria que aquestes modificacions es podien fer sense control parlamentari, els articles 97.8 i 112.1 del RIA clarifiquen que només entraran en vigor si el Parlament Europeu i el Consell no hi formulen objeccions en un termini de tres mesos, garantint així un cert control legislatiu.

D'altra banda, és important destacar que el RIA no exhaureix la regulació de la IA, sinó que forma part d'un marc normatiu més ampli. Per aquest motiu, l'aplicació ha de ser integrada amb altres normatives del dret digital europeu (com ara l'RGPD, l'RSD, l'RMD o l'NIS2) i, també, amb les normatives sectorials específiques que siguin rellevants, com les que afecten el sector financer o els dispositius mèdics (Barrio Andrés 2024). En aquest context, la protecció de les dades personals, com a dret fonamental, adquireix un paper central al

y la seguridad pública y económica o la difusión de contenidos ilícitos, falsos o discriminatorios" (considerant 110 RIA). És important destacar que aquests riscos sistèmics s'intensifiquen a mesura que augmenta la capacitat i l'abast dels models, i poden manifestar-se al llarg de tot el seu cicle de vida.

[3] Els sistemes d'IA que presenten un risc mínim o nul no estan regulats, però els proveïdors i els responsables de desplegament poden adherir-se a codis de conducta voluntaris.

llarg de totes les fases de desenvolupament i ús dels sistemes d'IA que, en molts casos, utilitzen dades personals.[4]

Per això, no és estrany que les autoritats de protecció de dades assumeixin un paper central dins del nou marc regulador establert pel RIA. Aquestes entitats, que ja exercien una funció clau en la supervisió del tractament de dades personals sota l'RGPD,[5] ara amplien les seves responsabilitats per incloure'n de noves sota el RIA. Tenint en compte aquest escenari, aquest treball es proposa analitzar:

- El rol de les autoritats de protecció de dades dins del RIA, examinant si les competències assignades suposen una ampliació de les seves competències o si, per contra, constitueixen una evolució natural de les atribucions ja establertes per l'RGPD.
- La seva designació com a autoritats de protecció de drets fonamentals, amb les implicacions que això comporta en la protecció dels drets individuals en el context de la IA.

En resum, es pretén comprendre millor els mecanismes de governança establerts pel RIA i el paper central que hi juguen les autoritats de protecció de dades. Això sense entrar a considerar altres funcions o competències que puguin ser assumides en el cas que, d'acord amb l'esquema de governança previst al RIA, es pugui ser designat com AVM.

[4] Un dels principals reptes és la prevenció de riscos, com ara els atacs d'inversió de models o la identificació indeguda de persones, que poden produir-se tant durant la recopilació inicial de les dades com en les fases d'aprenentatge i desplegament dels sistemes d'IA (Keber 2024). Per això, resulta fonamental assegurar que els sistemes compleixin els principis de l'RGPD i que hi hagi una autoritat competent que avaluï factors com el cost de la identificació, el temps necessari per dur-la a terme i els avenços tecnològics que puguin facilitar la reidentificació de dades personals, fins i tot si inicialment semblen anonimitzades.

[5] Les autoritats de protecció de dades han estat actives durant molt de temps i col·laboren en fòrums internacionals en matèries relacionades amb els sistemes d'IA (Assemblea Global de Privacitat, Grup Internacional sobre Protecció de Dades en Tecnologies, etc.).
EDPB. *Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial*. Juliol 2024. Disponible a: edpb_statement_202403_dpasroleaiact_es.pdf

2. El rol de les autoritats de protecció de dades dins del RIA

Tatiana Bianca Vulpe

En el context de l'adopció creixent de sistemes d'IA a la Unió Europea, el RIA estableix un marc normatiu que cerca equilibrar el desenvolupament tecnològic amb la protecció dels drets fonamentals, un dels quals és la protecció de dades. En aquest marc, tal com s'apuntava a la introducció, les autoritats de protecció de dades hi juguen un paper essencial per assegurar que l'ús de les tecnologies que incorporin IA respectin plenament les normes vigents en matèria de protecció de dades personals.

En aquesta línia, és important analitzar com el RIA amplia i concreta les funcions d'aquestes autoritats per abordar els reptes específics que planteja la implementació d'aquestes tecnologies emergents, alhora que en manté la independència i competències; així, garanteix la preservació dels drets dels ciutadans en un entorn cada vegada més digitalitzat i global.

Els considerants 10, 45, 69 i 157 del RIA proporcionen un context inicial per interpretar aquest reglament en matèria de protecció de dades, així com per comprendre el paper de les autoritats de protecció de dades. En particular, durant tota l'anàlisi cal tenir en compte els aspectes següents:

- El RIA no pretén afectar l'aplicació del Dret de la Unió vigent que regula el tractament de dades personals, incloses les funcions i atribucions de les autoritats competents. Tampoc afecta les obligacions dels proveïdors i els responsables de desplegament de sistemes d'IA, en el seu rol de responsables o encarregats del tractament, en la mesura que el disseny, el desenvolupament o l'ús de sistemes d'IA impliquin el tractament de dades personals. A més, els interessats continuen mantenint tots els drets i garanties previstes a l'RGPD (considerant 10).

- El RIA no ha d'afectar les pràctiques prohibides pel Dret de la Unió, inclòs el Dret de la Unió en matèria de protecció de dades (considerant 45). Això significa que qualsevol ús de sistemes d'IA ha de respectar les lleis europees vigents, especialment pel que fa a la protecció de les dades personals i la privacitat dels ciutadans.

- El dret a la protecció de dades personals s'ha de garantir al llarg de tot el cicle de vida del sistema d'IA. En aquest sentit, els principis de minimització de dades i de protecció de dades des del disseny i per defecte, establerts en el Dret de la Unió en matèria de protecció de dades, són aplicables quan es tracten dades personals (considerant 69).

- A més, el RIA s'entén sens perjudici de les competències, funcions, poders i independència de les autoritats de protecció de dades (considerant 157). Això assegura que aquestes autoritats continuïn exercint plenament les seves responsabilitats sense interferències, per garantir que els drets dels individus en matèria de protecció de dades es preservin en tot moment, fins i tot amb la implementació de noves tecnologies d'IA.

- Quan sigui necessari per al seu mandat, les autoritats de protecció de dades també han de tenir accés a qualsevol documentació creada en virtut del present Reglament (157). Aquest és un punt important, perquè els operadors hauran de facilitar la

documentació creada en virtut d'aquest Reglament a les autoritats de protecció de dades quan aquestes actuïn en relació amb l'RGPD.

En aquesta línia, el CEPD ha subratllat que, sempre que un model o sistema d'IA impliqui el tractament de dades personals, entraria en l'àmbit de supervisió de les autoritats nacionals de protecció de dades pertinents.[6] En aquest sentit, es important tenir clar el concepte de dades personals en contraposició al concepte de dades anònimes.

A més, cal tenir en compte que l'existència i l'ús de sistemes d'IA és prèvia al RIA, i que les autoritats de protecció de dades ja havien abordat aquesta matèria en relació amb l'RGPD. L'APDCAT, per exemple, ja s'ha pronunciat en aquest àmbit fent èmfasi en obligacions com la protecció de dades des del disseny, l'aplicació dels principis de protecció de dades o les avaluacions d'impacte.[7] Per altra banda, en el desenvolupament dels models amb intel·ligència artificial, aquesta autoritat també ha recomanat que s'apliquin mecanismes d'aprenentatge federat "de manera que les persones que tenen les dades (individus, entitats, etc.) poden entrenar el model de forma distribuïda, sense que hagin de cedir les dades a una entitat que centralitza l'entrenament."[8]

Per abordar adequadament l'anàlisi normatiu, resulta imprescindible precisar primer el concepte de *sistema d'IA*. L'article 3.1 del RIA defineix un sistema d'IA com "un 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."

Aquest article s'ha de relacionar amb el considerant 12 del RIA. Segons aquest considerant, podem dir que un sistema d'IA és un programari que es distingeix dels enfocaments tradicionals basats en regles predefinides per humans. A diferència d'aquests, un sistema d'IA està dissenyat per operar amb diversos nivells d'autonomia i té una capacitat d'inferència que li permet assolir objectius, tant de manera explícita com implícita. A més, el sistema ha de disposar de capacitat d'autoaprenentatge, la qual cosa implica la possibilitat de modificar-ne el comportament mentre s'utilitza, d'acord amb la lògica aplicada, el coneixement adquirit i les estratègies prèviament establertes. Aquesta característica és fonamental, ja que permet als sistemes d'IA evolucionar i adaptar-se a noves situacions, cosa que els diferencia clarament dels sistemes de programació estàtica basats en normes fixes.

---

[6] EDPB. *Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial.* Juliol 2024. Disponible a: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_es

[7] Autoritat Catalana de Protecció de Dades (APDCAT). *Intel·ligència artificial. Decisions automatitzades a Catalunya.* 2020. Disponible a: https://apdcat.gencat.cat/web/.content/03-documentacio/intelligencia_artificial/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf

[8] Autoritat Catalana de Protecció de Dades (APDCAT). *La privacitat des del disseny i la privacitat per defecte. Guia per a desenvolupadors*. Juny 2024. Disponible a: https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD.pdf

És especialment rellevant tenir en compte aquesta definició, ja que els sistemes que no compleixin aquestes característiques essencials quedarien, en principi, fora de l'àmbit d'aplicació del RIA. Dit d'una altra manera: si parlem de sistemes automatitzats sustentats exclusivament en normes preestablertes per persones, sense capacitat d'inferència o d'aprenentatge autònom, no estaríem davant d'un sistema d'IA en el sentit estricte del RIA; per tant, el seu ús s'escaparia de l'abast regulador d'aquest marc jurídic (Fernández Hernández 2024).

Així doncs, als apartats següents s'analitzen les diverses mencions que fa el RIA sobre les autoritats de protecció de dades, ja sigui en termes d'habilitacions o d'exigències. A més, a fi d'adquirir el context necessari, es recomana llegir l'annex d'aquest treball, que tracta sobre la identificació biomètrica remota.

2.1. Recepció de notificacions sobre l'ús de sistemes d'identificació biomètrica remota *en temps real* (art. 5.4 i considerants 36 i 38 RIA)

"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." (art. 5.4 RIA)

Aplicable a partir del 2 de febrer de 2025.

El considerant 36 del RIA disposa que cada ús d'un sistema d'identificació biomètrica remota en temps real s'ha de notificar a l'autoritat de vigilància del mercat pertinent, així com a l'autoritat nacional de protecció de dades. L'article 5.4 del RIA detalla aquesta notificació i estipula que, sense perjudici del que es disposa a l'apartat 3 del mateix article, qualsevol ús d'un sistema d'identificació biomètrica remota en temps real en espais d'accés públic, amb finalitats de garantia del compliment del Dret, s'ha de notificar a l'autoritat de vigilància del mercat pertinent i a l'autoritat nacional de protecció de dades; la notificació ha d'incloure com a mínim la informació especificada a l'apartat 6 i excloure dades operatives sensibles. Tenint en compte que els estats membres no estan obligats a nomenar una autoritat nacional de vigilància del mercat abans del 2 d'agost de 2025, s'entén que en el període comprès entre el 2 de febrer de 2025 i aquesta data (o si ho fan en termini) només hi ha l'obligació de notificar-hi a les autoritats de protecció de dades.

A l'Estat hi ha diverses autoritats de protecció de dades: l'Agència Espanyola de Protecció de Dades (AEPD), l'Autoritat Catalana de Protecció de Dades (APDCAT), l'Agència Basca de Protecció de Dades i el Consell de Transparència i Protecció de Dades d'Andalusia. Per tant, es podria considerar raonable que la notificació s'efectués directament a l'autoritat de protecció de dades competent, segons qui desplegui el sistema d'identificació biomètrica. Per exemple, l'àmbit d'actuació de l'APDCAT, tal com es disposa a l'article 3 de la Llei

32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, comprèn els fitxers i tractaments efectuats per les institucions públiques, l'Administració de la Generalitat i els ens locals, entre d'altres. Així, si un sistema és utilitzat per forces de seguretat de Catalunya, la notificació s'hauria de presentar davant l'APDCAT.

Queda clar que cada autoritat ha de disposar de la informació necessària per exercir les seves funcions dins del seu àmbit competencial. No obstant això, per evitar duplicitats o buits en la supervisió, especialment en situacions en què no sigui clar a qui s'ha de notificar (per exemple, en casos de col·laboració entre els cossos i forces de seguretat de diversos territoris), seria recomanable disposar de mecanismes de coherència entre les diferents autoritats. Aquesta coherència garantiria que la informació sobre l'ús d'aquests sistemes sigui accessible per a totes les parts pertinents i que, indirectament, els drets de les persones es protegissin de manera coherent.

És important tenir present que aquesta notificació s'emmarca en el context d'excepcions a pràctiques prohibides, regulades a l'article 5 del RIA. Qualsevol ús, entès en un sentit ampli, de sistemes d'identificació biomètrica remota en temps real que requereixi notificació s'emmarca dins d'un context d'excepcionalitat, regit per criteris de necessitat, proporcionalitat i respecte als drets fonamentals.

Les pràctiques prohibides no s'han d'entendre com una llista tancada, ja que l'article 112 del RIA exigeix que, cada any, la Comissió Europea revisi "la necesidad de modificar la lista del anexo III y la lista de prácticas de IA prohibidas previstas en el artículo 5." A més, d'acord amb l'article 96.1.*b* del RIA, la Comissió, com ja ho ha fet recentment, ha d'aprovar directrius sobre la implementació de les pràctiques prohibides per l'article 5 del RIA. Aquestes directrius no només han de servir per ajudar els proveïdors i responsables del desplegament a l'hora de garantir el compliment del RIA, sinó que també han de funcionar com una guia per orientar les autoritats competents en virtut del RIA.[9]

En aquest context analitzat, la notificació a les autoritats de protecció de dades proporciona de manera indirecta una garantia addicional per assegurar que aquestes pràctiques compleixen les normes de protecció de dades. Encara que el RIA no detalla una actuació posterior d'aquestes autoritats, la notificació permet un seguiment exhaustiu i una intervenció efectiva, en cas d'indicis d'irregularitats sobre les competències que aquestes autoritats ja tenien atribuïdes en el marc de l'RGPD; no es pot oblidar que la biometria ja era una qüestió que tractaven les autoritats de protecció de dades[10] o el Comitè Europeu de Protecció de dades (CEPD), integrat per totes les autoritats de control nacionals europees.

Concretament, com a text rellevant que convé esmentar, el CEPD va aprovar les Directrius 5/2022, sobre l'ús de la tecnologia de reconeixement facial, adoptades en data 26 de maig de 2023, després de la consulta pública. A l'apartat 12, diuen: "Aunque las dos funciones (autenticación e identificación) son distintas, ambas se refieren al tratamiento de datos

[9] No s'ha de perdre de vista que aquestes directrius no són vinculants i que, per tant, qualsevol interpretació del Reglament ha de passar pel Tribunal de Justícia de la Unió Europea (TJUE).

[10] Com per exemple l'APDCAT, en el dictamen emès a la consulta 21/2020, o en l'informe 1/2022.

biométricos relacionados con una persona física identificada o identificable y, por lo tanto, constituyen un tratamiento de datos personales y, más concretamente, un tratamiento de categorías especiales de datos personales."

En darrer terme, la identificació mitjançant sistemes d'IA no és possible sense una base de dades de referència que contingui dades biomètriques a efectes de comparació. La utilització de la IA fa possible un tractament més sofisticat de les dades biomètriques, la qual cosa permet no només la identificació, sinó també obtenir inferències sobre determinats aspectes o patrons de comportament de la persona, amb els consegüents riscos per als seus drets. Aquest punt és especialment rellevant perquè estem davant de categories especials de dades, tal com s'estableix a l'article 9.1 del Reglament (UE) 2016/679, l'article 10 de la Directiva (UE) 2016/680 i l'article 10.1 del Reglament (UE) 2018/1725. Així, el tractament de dades biomètriques encaminades a identificar de manera unívoca una persona física està subjecte al règim específic de l'RGPD en categories especials de dades.

Amb tot, seria desitjable més claredat sobre alguns aspectes clau d'aquesta notificació, a fi de garantir una aplicació coherent i eficaç de la normativa. En primer lloc, tot i que l'article fa referència al fet que la notificació ha d'excloure dades operatives sensibles, no s'aporten detalls concrets sobre quins elements són imprescindibles, més enllà d'una remissió. Per exemple, seria important definir si cal incloure-hi informació sobre els objectius de l'ús, l'abast temporal, geogràfic i personal o les mesures de seguretat implementades. Aquesta manca de claredat pot generar inconsistències a la pràctica. En segon lloc, també cal aclarir els terminis en què s'ha d'efectuar aquesta notificació. El RIA no determina si s'ha de presentar abans de l'ús del sistema, immediatament després d'utilitzar-lo o si hi ha un període específic per presentar-la. Sí que ho preveuen directrius recents [11] relatives a pràctiques prohibides, on es concreta el següent: la notificació s'ha de fer després de cada ús, per poder informar sobre el nombre d'autoritzacions i el seu resultat. Encara que proporciona més concreció, no tenim una definició precisa, cosa que pot resultar problemàtica, especialment en contextos on el temps és crític, en situacions d'urgència o en casos excepcionals. L'establiment de terminis clars contribuiria a garantir una coherència efectiva entre les autoritats implicades i asseguraria que la supervisió es faci en temps real o en un període raonable.

2.2. Presentació d'informes anuals a la Comissió, en relació amb les notificacions sobre l'ús de sistemes d'identificació en temps real (art. 5.6 RIA i considerant 36)

"Las autoridades nacionales de vigilancia del mercado y l**as 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

[11] Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

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." (art. 5.6 RIA)

Aplicable a partir del 2 de febrer de 2025.

Vinculat amb el que s'ha desenvolupat al punt anterior d'aquest treball, les autoritats nacionals de protecció de dades dels estats membres que rebin notificacions sobre l'ús de sistemes d'identificació biomètrica remota en temps real, en espais d'accés públic, amb finalitats de garantia del compliment del Dret, tenen l'obligació de presentar informes anuals a la Comissió Europea, que han d'incloure informació sobre el nombre de decisions adoptades. Aquest sistema planteja diversos reptes pràctics i conceptuals.

Un aspecte a esmentar és que, en aquest apartat, el RIA fa ús del plural ('les autoritats nacionals de protecció de dades') quan es refereix a les autoritats de protecció de dades, mentre que en el context de la recepció de la notificació empra el singular ('l'autoritat nacional de protecció de dades'). En principi, l'ús del singular o del plural en el RIA no té per què tenir una implicació jurídica significativa, ja que podria tractar-se simplement d'una qüestió de redacció sense intenció d'introduir diferències pràctiques. No obstant això, tenint en compte el context de l'Estat espanyol, on coexisteixen diferents autoritats, aquesta diferència terminològica podria obrir la porta a interpretacions més àmplies. Així, cal entendre que totes les autoritats competents segons el territori o l'àmbit material afectat pel sistema d'identificació biomètrica— han de redactar l'informe corresponent. No obstant això, resta pendent de concretar com es vehicularia la tramesa formal dels informes a la Comissió Europea.

Així mateix, el fet que cada autoritat que ha rebut notificacions presenti un informe en el marc de l'article 5.6 del RIA genera dubtes sobre les possibles duplicitats en els informes. Per exemple, si diverses autoritats (autoritats de vigilància de mercat i autoritats de protecció de dades) reben notificacions sobre el mateix ús, caldrà definir si cadascuna d'elles ha de presentar un informe independent a la Comissió, o si es concentraran en una única autoritat per facilitar-ne una presentació unificada. La falta de claredat en aquest punt podria generar una duplicitat de dades o una càrrega administrativa innecessària, dificultant l'objectiu de supervisió efectiva. A més, com ja s'apunta a les directrius de la Comissió respecte de les pràctiques prohibides, de moment les autoritats nacionals de vigilància del mercat i les autoritats nacionals de protecció de dades són lliures de decidir si volen presentar informes individuals o bé un informe conjunt per estat membre.

L'informe que preveu l'article 5.6 del RIA representa una novetat dins del nou marc regulador per a les autoritats de protecció de dades i es diferencia significativament de l'informe regulat per l'article 59 de l'RGPD. Mentre que aquest últim té un caràcter públic i el contingut està clarament definit, l'informe del RIA a què ens referim encara no té un desenvolupament concret. A més, la redacció d'aquests informes anuals depèn de la disponibilitat de directrius i models establerts per la Comissió Europea; això limita l'acció de les autoritats, ja que el marc regulador encara no està completament definit, tot i que l'article 5 del RIA ja és vigent. D'altra banda, només l'informe de les autoritats nacionals de protecció

de dades cobriria el període comprès entre el 2 de febrer de 2025 i el 2 d'agost de 2025, ja que el RIA no exigeix als estats membres que designin una autoritat nacional de vigilància del mercat abans d'aquesta data.

Aquest sistema d'aplicació progressiva es pot justificar per la complexitat i l'evolució constant de la intel·ligència artificial. Com apunta Quadra-Salcedo (2024), és pràcticament impossible regular amb precisió des de l'inici tot l'abast, les possibilitats i els riscos que planteja aquesta tecnologia. Per tant, sembla raonable establir unes bases inicials, que es puguin ajustar i desenvolupar a mesura que es consolidi i s'entengui millor la tecnologia. Això permetrà abordar nous reptes i adaptar les normes a les circumstàncies canviants. No obstant això, aquesta aproximació progressiva també planteja incerteses. Quan la Comissió estableixi el contingut específic dels informes, encara quedarà oberta la possibilitat d'ampliar o modificar la informació exacta que s'hi haurà d'incloure, i això podria requerir ajustar les pràctiques de notificació i els informes respectius de manera contínua.

2.3. Accés a documentació sobre l'ús de sistemes d'identificació biomètrica remota en diferit, documentada a l'expedient policial pertinent (art. 26.10 RIA).

"No obstante lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación cuya finalidad sea la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello, el responsable del despliegue de un sistema de IA de alto riego de identificación biométrica remota en diferido solicitará, ex ante o sin demora indebida y a más tardar en un plazo de cuarenta y ocho horas, a una autoridad judicial o administrativa cuyas decisiones sean vinculantes y estén sujetas a revisión judicial, una autorización para utilizar ese sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso sobre la base de hechos objetivos y verificables vinculados directamente al delito. Cada utilización deberá limitarse a lo que resulte estrictamente necesario para investigar un delito concreto.

(...)

Con independencia de la finalidad o del responsable del despliegue, **se documentará toda utilización de tales sistemas de IA de alto riesgo en el expediente policial pertinente y se pondrá a disposición, previa solicitud,** de la autoridad de vigilancia del mercado pertinente y **de la autoridad nacional de protección de datos, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho.** El presente párrafo se entenderá sin perjuicio de los poderes conferidas por la Directiva (UE) 2016/680 a las autoridades de control.

(...)" (art. 26.10 RIA)

Aplicable a partir del 2 d'agost de 2026.

L'article 26 del RIA recull les obligacions dels responsables de desplegament de sistemes d'IA d'alt risc. Aquest responsable es defineix com una persona física o jurídica, o una

autoritat pública, organisme o entitat, que utilitzi un sistema d'IA sota la seva pròpia autoritat, excepte quan el seu ús s'emmarqui en una activitat personal de caràcter no professional (art. 3.4 RIA).

Abans d'entrar en l'anàlisi, és important fer dues consideracions prèvies. En primer lloc, cal destacar que les obligacions recollides a l'article 26 no són les úniques que recauen sobre els responsables del desplegament, ja que també n'hi ha d'altres de rellevants fora d'aquest article. Per exemple, l'article 27, que es va introduir en una fase avançada del procés legislatiu, imposa a certs responsables del desplegament de sistemes d'IA d'alt risc l'obligació de fer una avaluació de l'impacte que l'ús d'aquests sistemes pot tenir sobre els drets fonamentals.

D'altra banda, el RIA no altera les obligacions que altres normatives de la Unió Europea o de legislacions nacionals imposin als responsables del desplegament, com queda explícit a l'article 26.2 del RIA. Per exemple, i com ja s'ha esmentat prèviament, si l'ús de sistemes d'IA implica el tractament de dades personals, el responsable del desplegament també ha d'assumir el rol de responsable o encarregat del tractament i complir les normatives aplicables en matèria de protecció de dades personals (considerant 10).

En concret, l'article 26.10 del RIA aborda les obligacions de documentació i supervisió d'usos de sistemes d'IA d'alt risc per a la identificació biomètrica remota en diferit. Qualsevol utilització d'aquests sistemes ha de quedar registrada als expedients policials pertinents, amb la finalitat de garantir una traçabilitat adequada i possibilitar la supervisió per part de les autoritats competents. Aquesta documentació ha d'estar disponible, prèvia sol·licitud, per a l'autoritat de vigilància del mercat pertinent i l'autoritat nacional de protecció de dades, exclosa explícitament la divulgació de dades operatives sensibles relacionades amb la garantia del compliment del Dret.

El RIA distingeix entre els sistemes d'identificació biomètrica remota en temps real i en diferit, en funció de si la captura de dades biomètriques, la comparació i la identificació es produeixen amb un retard significatiu o sense, tal com s'explica en apartats previs.[12]

Atès el caràcter altament intrusiu dels sistemes d'identificació biomètrica, convé tenir present que, a part del RIA, aquests sistemes estan sotmesos a una sèrie de garanties imposades pel Dret de la Unió en matèria de protecció de dades i que el legislador europeu del RIA ha volgut establir de manera expressa una sèrie de garanties addicionals, per evitar que el desplegament dels sistemes d'identificació biomètrica remota en diferit pugui donar lloc a una vigilància indiscriminada (considerant 95).

En aquest sentit, cal destacar que l'article 26.10 del RIA presenta nombroses similituds amb la regulació dels sistemes d'identificació biomètrica remota en temps real, establerta als articles 5.2 a 5.7 (desenvolupats als apartats 2.1 i 2.2 d'aquest treball). Així, des d'una perspectiva sistemàtica, la regulació de l'ús policial dels sistemes d'identificació biomètrica en diferit s'ha elevat a l'article 26, ja que, tot i que el legislador europeu vol limitar-ne l'ús i

[12] A l'annex d'aquest article s'exposa breument aquesta diferència.

impedir-ne l'aplicació indiscriminada, no ha optat per convertir aquesta pràctica en una prohibició absoluta, sinó que la sotmet a condicions i requisits estrictes (López 2024).

No obstant això, cap dels dos supòsits defineix de manera prou precisa el contingut exacte dels informes o registres que cal mantenir o facilitar. Aquesta manca de concreció genera un buit normatiu, que pot donar lloc a interpretacions divergents i a dificultats pràctiques en l'aplicació efectiva del RIA, fins que la Comissió publiqui les directrius corresponents.

L'única referència (indirecta) que en tenim és al considerant 93 del RIA, sobre la informació que ha de constatar el responsable del desplegament en relació amb els interessats:

- Els responsables del desplegament de sistemes d'IA d'alt risc inclosos a l'annex III, que prenguin o ajudin a prendre decisions relacionades amb persones físiques, estan obligats a informar els afectats que estan exposats a l'ús de sistemes d'IA d'alt risc. Aquesta informació ha d'incloure la finalitat prevista i el tipus de decisions que es prenen, així com garantir el dret de la persona afectada a una explicació d'acord amb el RIA. Per tant, se'n podria extreure que seria convenient acreditar als expedients el contingut d'aquesta informació, i com s'ha fet efectiva.

- Pel que fa als sistemes d'IA d'alt risc utilitzats amb finalitats d'aplicació del Dret, s'aplica l'article 13 de la Directiva (UE) 2016/680. Aquest precepte estableix que s'ha de posar a disposició de l'interessat informació addicional o facilitar-li, en cas de tractament de dades personals per part de les autoritats competents en matèria de prevenció, investigació, detecció o enjudiciament d'infraccions penals, així com en l'execució de sancions penals.[13] Per tant, seria convenient deixar també constància als expedients d'aquesta informació addicional.

Així doncs, un dels principals reptes identificats és l'absència de directrius específiques sobre el contingut que hauria d'incloure la documentació als expedients policials. Aquesta manca de precisió no només pot dificultar la tasca de supervisió de les autoritats, sinó que també podria portar a una aplicació inconsistent entre estats membres, o fins i tot entre autoritats dins d'un mateix estat.

Tal com succeeix amb els sistemes en temps real, analitzats als apartats 2.1 i 2.2 d'aquest treball, a l'article 26.10 no queda clar com s'ha de gestionar la coherència entre les diverses autoritats implicades, com ara les autoritats nacionals de protecció de dades i les autoritats de vigilància del mercat.

[13] A Espanya, s'ha de considerar l'article 21 de l'LO 7/2021.

2.4. Recepció d'informes anuals sobre l'ús de sistemes d'identificació biomètrica remota en diferit (art. 26.10 RIA)

"No obstante lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación cuya finalidad sea la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello, el responsable del despliegue de un sistema de IA de alto riego de identificación biométrica remota en diferido solicitará, ex ante o sin demora indebida y a más tardar en un plazo de cuarenta y ocho horas, a una autoridad judicial o administrativa cuyas decisiones sean vinculantes y estén sujetas a revisión judicial, una autorización para utilizar ese sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso sobre la base de hechos objetivos y verificables vinculados directamente al delito. Cada utilización deberá limitarse a lo que resulte estrictamente necesario para investigar un delito concreto.

(...)

Los responsables del despliegue presentarán informes anuales a la autoridad de vigilancia del mercado pertinente y **a la autoridad nacional de protección de datos sobre el uso que han hecho de los sistemas de identificación biométrica remota en diferido**, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. Los informes podrán agregarse de modo que cubran más de un despliegue.

(...)" (art. 26.10 RIA)

Aplicable a partir del 2 d'agost de 2026.

Els responsables del desplegament han de presentar informes anuals a l'autoritat de vigilància del mercat pertinent i a l'autoritat nacional de protecció de dades, sobre l'ús que hagin fet dels sistemes d'identificació biomètrica remota en diferit, excloent-ne la divulgació de dades operatives sensibles relacionades amb la garantia del compliment del Dret.

L'obligació que els responsables del desplegament presentin informes anuals a les autoritats de vigilància del mercat i de protecció de dades es podria considerar com a mesura essencial per garantir la transparència i la supervisió adequada de l'ús dels sistemes d'identificació biomètrica remota en diferit. Aquesta mesura permet a les autoritats competents, com l'APDCAT, supervisar com s'utilitzen aquests sistemes, assegurar que es compleixin les normatives establertes i detectar possibles irregularitats, a l'hora d'implementar-los o fer-ne ús.

Un aspecte rellevant d'aquesta obligació és que els informes poden ser agregats per cobrir més d'un desplegament. Aquesta opció pot facilitar la gestió administrativa als responsables del desplegament, especialment si han fet múltiples usos dels sistemes en diferents contextos. Al mateix temps, l'agregació podria simplificar el procés de revisió de les autoritats de vigilància i protecció de dades, oferint una visió més global de l'ús d'aquests sistemes en un període determinat. No obstant això, l'agregació també planteja reptes: és crucial que no comprometi la capacitat de supervisió de les autoritats, assegurant que els

informes agregats siguin prou detallats per identificar possibles abusos o desviacions de la normativa. Seria recomanable que els informes agregats incloguessin dades clau sobre cada desplegament, com ara la finalitat específica, l'abast geogràfic, les condicions d'ús i les mesures de control implementades.

En tot cas, la presentació d'informes anuals esdevé una eina clau per reforçar la responsabilitat dels responsables del desplegament, així com garantir que els sistemes d'identificació biomètrica remota en diferit no s'utilitzen de manera abusiva ni vulneren els drets fonamentals. A més, aquests informes anuals podrien ser útils per analitzar l'impacte acumulat d'aquests sistemes, detectar tendències en l'ús i ajustar les actuacions futures segons les necessitats i els riscos identificats.

2.5. Participació en espais controlats de proves per a la IA (art. 57.10 RIA)

"Las autoridades nacionales competentes velarán por que, **en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes que proporcionen o respalden el acceso a los datos, las autoridades nacionales de protección de datos** y las demás autoridades nacionales o competentes **estén ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y competencias**." (art. 57.10 RIA)

Aplicable a partir del 2 d'agost de 2026.

L'article 57 del RIA estableix la creació d'espais controlats de proves per a la IA (o *sandboxes*), amb l'objectiu de fomentar la innovació i facilitar el desenvolupament, entrenament, prova i validació de sistemes d'IA innovadors, abans d'introduir-los al mercat. Els estats membres hauran d'establir, com a mínim, un espai controlat de proves operatiu abans del 2 d'agost de 2026, sota la supervisió de les autoritats competents nacionals.

Tot i que els *sandboxes* inicialment van sorgir com a entorns regulats d'experimentació centrats principalment en el sector d'empreses de tecnologies financeres (*fintech*), recentment han començat a aparèixer espais similars dissenyats específicament per a la IA en diferents parts del món (Arellano Toledo 2024). Un exemple proper és 'l'entorn controlat de proves' establert pel Govern de l'Estat amb el Reial decret 817/2023, de 8 de novembre. Aquest decret regula un espai de proves dedicat a garantir que la proposta del RIA es compleix. En aquesta línia, es pot constatar que el Govern de l'Estat espanyol s'ha avançat a les exigències de l'article 57 del RIA. Tot i que aparentment això pugui semblar positiu, pot provocar una manca de coherència entre els requisits que estableix el RIA i els que preveu l'RD. Un exemple n'és que l'article 3.2 de l'RD fa referència tant als proveïdors com als usuaris, mentre que el RIA (tal com s'observa als considerants 138 i 139 i a l'article 57) es limita a esmentar els proveïdors i els proveïdors potencials, deixant al marge els usuaris (equivalència responsables del desplegament, segons el RIA). A més, l'article 3.8 de l'RD

distingeix entre dos tipus d'usuaris (sol·licitants i participants) i, a l'article 3.7, entre proveïdors sol·licitants i participants.

Així, pel que fa als anomenats *sandbox*, s'estableixen quatre categories diferents que no apareixen exactament de la mateixa manera al RIA. Aquestes divergències, juntament amb altres qüestions, com ara les diferències en els tipus de sistemes d'IA regulats, podrien fer necessària una revisió o modificació dels marcs legals nacionals, per garantir-ne l'harmonització i adequació a la normativa comunitària (Arellano Toledo, 2024). Això, sense comptar amb la possibilitat que la Comissió, mitjançant els seus actes executius, estableixi disposicions més precises sobre els tipus i el nombre de participants que poden fer ús dels espais de proves.

Per altra banda, a les guies i recomanacions elaborades fins ara per l'AEPD[14] i la CNMC,[15] així com per altres autoritats, també es posa de manifest una actitud favorable respecte de la implementació d'aquest tipus de projectes, que es consideren una oportunitat per promoure la innovació, mentre es redueixen els possibles impactes de la IA sobre la ciutadania.[16] Aquest enfocament hauria d'assegurar que l'assignació de competències es formalitzés mitjançant normes amb valor legal i que es despleguin mesures de protecció adequades. A més, té especial importància respectar principis com la limitació en el tractament de dades i la transparència, restringint l'abast dels projectes a objectius específics, explícits i legítims (Arellano Toledo 2024).

Un dels punts més delicats, vinculats amb la interacció amb l'RGPD, és la limitació de finalitats, que exigeix una avaluació més precisa de l'ús de sistemes d'IA destinats a objectius concrets. Això té com a objectiu evitar que l'entrenament o el disseny inicial d'un sistema interfereixi amb el seu ús posterior, per a finalitats diferents o incompatibles. Aquest mateix principi s'aplica als sistemes d'IA que, tot i ser utilitzats per a objectius compatibles, necessiten identificar clarament la base legal que sustenta el tractament i dur a terme les accions necessàries per validar-lo, si cal (Arellano 2024).

Pel que fa a les autoritats de protecció de dades, l'article 57.10 les esmenta directament en indicar que, en la mesura que els sistemes innovadors d'IA impliquin el tractament de dades personals (o estiguin sota la supervisió d'altres autoritats nacionals o competents que proporcionin o donin suport a l'accés a les dades), aquestes autoritats han d'estar lligades al funcionament de l'espai controlat de proves per a la IA i involucrades en la supervisió d'aquests aspectes, segons les seves funcions i competències. Això és un indicador del

---

[14] AEPD. *Requisitos para Auditorías de Tratamientos que incluyan IA,* 2021.
AEPD. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020.
AEPD. *Tratamientos que incluyen Inteligencia Artificial (IA). Mapa de referencia,* 2022.

[15] CNMC. Informe sobre el proyecto de Real Decreto que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial, 2023.

[16] Aquestes guies presenten exemples d'usos raonables de sistemes d'intel·ligència artificial, justificats per l'interès públic, com ara projectes de ciutats intel·ligents (*smartcities*) o el control de fronteres.

paper actiu que tenen les autoritats de protecció de dades en aquests entorns. Però, quin és l'abast real d'aquesta vinculació al funcionament de l'espai? No queda clar.

L'article 57 del RIA no torna a referir-se explícitament a les autoritats de protecció de dades, sinó que fa servir el terme genèric *autoritats competents* per regular el funcionament de l'entorn de proves. Aquesta formulació podria generar inseguretat jurídica i requerir futurs aclariments sobre si *autoritats competents* és el mateix que *autoritats nacionals competents*.

Independentment de si es consideren o no autoritats competents en aquest context, en qualsevol cas les autoritats de protecció de dades han d'estar vinculades al funcionament de l'espai controlat de proves per a la IA i participar en la supervisió d'aquests aspectes, tal com s'apunta anteriorment.

Segons l'enfocament adoptat, el llistat següent podria comportar noves funcions per a les autoritats de protecció de dades o, com a mínim, una millor inferència/definició del que hauria d'implicar la seva vinculació al funcionament i supervisió:

- En primer lloc, dins de l'espai controlat de proves les autoritats competents han de proporcionar orientació, supervisió i suport per determinar els riscos, especialment per als drets fonamentals, la salut i la seguretat. Això inclou avaluar les proves i les mesures de mitigació, així com la seva eficàcia en relació amb les obligacions i requisits del RIA i, quan escaigui, d'altres disposicions del Dret de la Unió i nacional supervisades a l'espai controlat de proves (art. 57.6 RIA).

- En segon lloc, les autoritats competents han de proporcionar als proveïdors i potencials proveïdors orientacions sobre les expectatives en matèria de regulació i la manera de complir els requisits i obligacions establerts al RIA. Si el proveïdor o potencial proveïdor del sistema d'IA ho sol·licita, l'autoritat competent també ha d'aportar una prova escrita de les activitats realitzades amb èxit a l'espai controlat de proves, així com un informe de sortida que detalli les activitats realitzades i els resultats i aprenentatges corresponents. Els proveïdors poden utilitzar aquesta documentació per demostrar que compleixen el RIA, mitjançant el procés d'avaluació de la conformitat o les activitats de vigilància del mercat pertinents (art. 57.7 RIA).

- En tercer lloc, els espais controlats de proves per a la IA no afecten les facultats de supervisió o correctores de les autoritats competents que els supervisen, ni tan sols a escala regional o local. Qualsevol risc considerable per a la salut, la seguretat i els drets fonamentals detectat durant el procés de desenvolupament i prova d'aquests sistemes d'IA requerirà una mitigació adequada. Si no és possible mitigar-los, les autoritats nacionals competents estan facultades per suspendre temporalment o permanentment el procés de prova, o la participació a l'espai controlat de proves, i han d'informar l'Oficina d'IA d'aquesta decisió. Amb l'objectiu de donar suport a la innovació en matèria d'IA a la Unió, aquestes autoritats exerceixen les seves facultats de supervisió dins dels límits del dret pertinent i utilitzen la seva potestat discrecional per aplicar disposicions jurídiques relacionades amb un projecte específic d'espai controlat de proves per a la IA (art. 57.11 RIA).

Altres apartats indiquen que els espais controlats de proves per a la IA s'han de dissenyar i implementar de manera que, quan escaigui, facilitin la cooperació transfronterera entre les autoritats nacionals competents. Aquestes autoritats han de coordinar les seves activitats i cooperar en el marc del Consell de IA, informant sobre l'establiment d'un espai controlat de proves l'Oficina de IA i el Consell de IA, als quals poden sol·licitar suport i orientació. A més, han de presentar informes anuals que proporcionin informació sobre el progrés i els resultats de la implementació d'aquests espais, incloent-hi millors pràctiques, incidents, ensenyaments extrets i recomanacions sobre la seva configuració i, si escau, sobre l'aplicació i possible revisió del Reglament.

No obstant això, l'apartat que cal analitzar amb més detall és el número 12, especialment tenint en compte que el RIA no hauria d'interferir en les competències sancionadores de les autoritats de protecció de dades. Aquest apartat estableix que, segons el Dret de la Unió i nacional en matèria de responsabilitat, els proveïdors i potencials proveïdors que participin a l'espai controlat de proves per a la IA són responsables de qualsevol dany infligit a tercers, com a resultat de l'experimentació duta a terme a l'espai. Tanmateix, sempre que els proveïdors potencials respectin el pla específic i les condicions de la seva participació, i segueixin de bona fe les orientacions proporcionades per l'autoritat nacional competent, les autoritats no imposaran multes administratives per infraccions del RIA. En els casos en què altres autoritats competents responsables d'altres disposicions del Dret de la Unió i nacional hagin participat activament en la supervisió del sistema d'IA i hagin proporcionat orientacions per complir-les, tampoc s'imposaran multes administratives en relació amb aquestes disposicions.

Segons l'RGPD, les autoritats de protecció de dades tenen la potestat d'imposar sancions administratives en cas d'incompliment de la normativa de protecció de dades. Si el RIA estableix una possible exempció de sancions administratives, aquesta hauria de ser interpretada amb cautela per tal de no contradir les atribucions legals d'aquestes autoritats. En particular, l'article 57.12 del RIA genera dubtes, ja que podria ser interpretat com una limitació o interferència en les funcions de les autoritats de protecció de dades. Tot i això, aquesta interpretació no és inequívoca i caldria valorar-la cas per cas.

És important remarcar que el fet que es formuli una recomanació genèrica en el marc d'un espai controlat de proves no pot ser entès com una exempció automàtica de responsabilitat o sanció. Caldrà analitzar cada situació concreta per determinar fins a quin punt aquestes recomanacions s'han aplicat de manera efectiva i adequada al cas en qüestió. Aquest extrem és especialment rellevant quan l'autoritat que investigui una possible infracció no coincideixi amb la que ha participat en l'espai de proves, i es pugui veure eventualment condicionada pel criteri d'aquesta última.

En qualsevol cas, convé recordar els principis de no interferència en les competències, funcions, poders i independència de les autoritats de protecció de dades (considerants 10, 45, 69 i 157 del RIA), tal com ja s'ha exposat a la introducció d'aquest apartat.

2.6. Designació com a autoritat de vigilància del mercat (art. 74.8 RIA)

"En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III del presente Reglamento, punto 1, en la medida en que los sistemas se utilicen a los efectos de la garantía del cumplimiento del Derecho, la gestión de fronteras y la justicia y la democracia, y **en el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, puntos 6, 7 y 8, del presente Reglamento, los Estados miembros designarán como autoridades de vigilancia del mercado** a efectos del presente Reglamento bien **a las autoridades de control encargadas de la protección de datos competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680**, bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la independencia de las autoridades judiciales ni interferirán de otro modo en sus actividades en el ejercicio de su función judicial."

Aplicable a partir del 2 d'agost de 2026.

A la definició 26 de l'article 3, el RIA defineix les autoritats de vigilància de mercat amb una remissió al Reglament 2019/1020: "la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020." A més, tal com disposa el considerant 156 del RIA, aquestes autoritats han de disposar de tots els poders d'execució establerts al RIA i a l'RVM.

Segons l'article 3.4 del Reglament 2019/1020, l'autoritat de vigilància del mercat es defineix com "la autoridad designada por un Estado miembro, de conformidad con el artículo 10, responsable de efectuar la vigilancia del mercado en el territorio de ese Estado miembro." Al mateix article 3, la vigilància del mercat es defineix com les activitats i mesures adoptades per aquestes autoritats per garantir que els productes compleixin els requisits de la legislació d'harmonització de la Unió i vetllin per la protecció de l'interès públic emparat per aquesta legislació. Aquesta concepció contrasta amb la naturalesa de les autoritats de control de protecció de dades, que, segons l'article 51 de l'RGPD, supervisen l'aplicació del Reglament per salvaguardar els drets i llibertats fonamentals en relació amb el tractament de dades i facilitar la lliure circulació d'aquestes dades dins la UE.

A priori, doncs, encara que sembli que les autoritats de vigilància del mercat i les autoritats de protecció de dades responen a lògiques diferents, no es pot perdre de vista l'estreta relació entre IA i dades personals. Per tant, l'article 74.8 del RIA, que insta (o obliga) els estats membres a designar com a autoritats de vigilància del mercat d'IA les autoritats de protecció de dades o altres òrgans que compleixin unes condicions determinades, sembla un encert. A més, el Comitè Europeu de Protecció de Dades, a la "Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial", posa de manifest l'adequació d'aquesta designació, atès que les autoritats de protecció de dades ja tenen experiència i coneixements especialitzats. Aquesta designació

ha de venir acompanyada dels recursos econòmics i humans necessaris per assegurar una implementació efectiva.[17]

Encara que no s'analitzarà en aquest treball, s'ha de tenir present que el RIA confereix a les AVM una sèrie de poders i funcions que es podrien assimilar als recollits a l'RGPD, ja que, encara que no es categoritzin d'aquesta manera, s'hi poden identificar poders d'investigació, poders correctors i poders d'autorització i consultius. A mode d'exemple, en relació amb els poders d'investigació, el RIA (i l'RVM) regula diferents tipus d'accessos a informació i documentació determinada. Algunes exemples concrets relatius a possibles sol·licituds d'accessos a informació o documentació que tindran les AVM[18] són els següents:

- Declaració UE de conformitat (art. 18.1.*e* i art. 47 RIA).[19]
- Informació i documentació segons l'RVM (art. 14.4 RVM).
- Informació i documentació de sistemes d'IA d'alt risc (art. 18.1.*a*, art. 21, art. 22.3.*c*, art. 23.6, art. 26.6, art 74.13 i art 75.3 RIA).
- Documentació de les autoritats garants de compliment del Dret, d'immigració o d'asil, quan siguin proveïdores de sistemes d'IA d'alt risc (art. 78.2 i 3 RIA).
- Informació de sistemes d'IA d'ús general (art. 53.1.*a*, art. 54.3.*b* RIA i art. 75.3 RIA).
- Documentació del sistema de gestió de la qualitat (art. 18.1.*b* i art. 17 RIA).
- Modificacions i decisions d'organismes notificats (art. 18.1.*c* i art 18.1.*d* RIA).
- Base de dades de la UE (art. 49.4 RIA).

És important destacar que, en virtut de l'article 58.1.*e* de l'RGPD, les autoritats de protecció de dades ja disposen del poder d'obtenir del responsable i de l'encarregat del tractament l'accés a totes les dades personals i a la informació necessària per exercir les seves funcions de supervisió i control.

---

[17] En aquest sentit, és interessant esmentar l'article 15 de l'RVM, que dictamina que els estats membres poden autoritzar les AVM a reclamar als operadors econòmics pertinents la totalitat dels costos de les seves activitats, en relació amb casos d'incompliments.

[18] Aquest llistat no comprèn tots els accessos i només és il·lustratiu.

[19] L'annex V del RIA estableix els elements que ha de contenir, com a mínim, la declaració UE de conformitat: (i) Les dades identificatives del sistema d'IA: nom, tipus i qualsevol referència unívoca que permeti traçar el producte; (ii) El nom i l'adreça del proveïdor o del seu representant autoritzat; (iii) L'afirmació que la DUEC s'expedeix sota la responsabilitat exclusiva del proveïdor; (iv) La declaració de conformitat amb el RIA i, si escau, amb la resta de normativa d'harmonització de la Unió; (v) Quan el sistema d'IA impliqui tractament de dades personals, la declaració de conformitat amb la normativa de protecció de dades (RGPD, etc.); (vi) Les referències a les normes harmonitzades aplicades o a l'especificació comuna pertinent; (vii) El nom i el número d'identificació de l'organisme notificat que hagi expedit el certificat, si n'hi ha, i la descripció del procediment d'avaluació de la conformitat seguit; i (viii) El lloc i la data d'expedició, el nom, el càrrec i la signatura de la persona que expedeix la declaració en representació del proveïdor.

Una conclusió que es pot extreure del fet que una autoritat de protecció de dades sigui designada com a AVM és que les principals novetats no es troben tant en l'accés a la informació —ja previst en el RGPD i reforçat pel considerant 157 del RIA—, sinó en la possibilitat d'imposar sancions en virtut del RIA i d'organitzar espais de proves (sandboxes) en el sentit de l'article 57 del mateix reglament, amb les conseqüències específiques que això comporta.

Pel que fa a l'accés a la informació, la qüestió rellevant no és tant si poden accedir-hi, sinó amb quin fonament jurídic legitimen la seva sol·licitud d'accés en cada cas concret o amb quina finalitat accedeixen (per exemple, investigació/sanció segons el RIA o segons l'RGPD).

2.7. Altres consideracions

"Los importadores proporcionarán a las **autoridades competentes pertinentes**, previa solicitud motivada, toda la información y la documentación, incluidas las referidas en el apartado 5, que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2 en una lengua que estas puedan entender fácilmente. A tal efecto, velarán asimismo por que la documentación técnica pueda ponerse a disposición de esas autoridades." (art. 23.6 RIA)

"Los importadores cooperarán con las **autoridades competentes pertinentes** en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo introducido en el mercado por los importadores, en particular para reducir y mitigar los riesgos que este presente." (art. 23.7 RIA)

"Previa solicitud motivada de una **autoridad competente pertinente**, los distribuidores de un sistema de IA de alto riesgo proporcionarán a esa autoridad toda la información y la documentación relativas a sus actuaciones con arreglo a los apartados 1 a 4 que sean necesarias para demostrar que dicho sistema cumple los requisitos establecidos en la sección 2." (art. 24.5 RIA)

"Los distribuidores cooperarán con las **autoridades competentes pertinentes** en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo comercializado por los distribuidores, en particular para reducir o mitigar los riesgos que este presente." (art. 24.6 RIA)

"Los responsables del despliegue cooperarán con las **autoridades competentes pertinentes** en cualquier medida que estas adopten en relación con el sistema de IA de alto riesgo con el objetivo de aplicar el presente Reglamento." (art. 26 12 RIA)

Convé entendre el concepte autoritats competents pertinents (relevant competent authorities, en la versió en anglès). Aquest concepte pot generar confusió (o fins i tot inseguretat jurídica), a causa del qualificatiu competent utilitzat per referir-se a diferents autoritats. El RIA esmenta: 'autoridades competentes', de manera aïllada; i, posteriorment, de manera concreta en relació amb altres qualificatius com ara nacional, judicials, pertinents, públiques, etc. (per exemple, 'autoridades nacionales competentes'; autoridades judiciales competentes'; 'autoridades de vigilancia del mercado competentes'; 'autoridades competentes pertinentes'; 'autoridades competentes responsables de otras disposiciones del Derecho de la Unión y nacional'; 'autoridades públicas competentes'; 'autoridades nacionales competentes pertinentes').

En primer lloc, convé matisar que és possible que, quan el RIA esmenti l'autoritat competent pertinent, no es refereixi a l'autoritat nacional competent definida a l'article 3.48 del RIA com: "una autoridad notificante o una autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a autoridades de vigilancia del mercado se interpretarán como referencias al Supervisor Europeo de Protección de Datos".

	Anglès	Espanyol
Considerant 139 RIA	To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the AI regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. AI regulatory sandboxes established under this Regulation should be without prejudice to other law allowing for the establishment of other sandboxes aiming to ensure compliance with law other than this Regulation. Where appropriate, **relevant competent authorities** in charge of those other regulatory sandboxes should consider the benefits of using those sandboxes also for the purpose of ensuring compliance of AI systems with this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world conditions may also be operated and supervised in the framework of the AI regulatory sandbox.	Para garantizar una aplicación uniforme en toda la Unión y conseguir economías de escala, resulta oportuno establecer normas comunes para la creación de espacios controlados de pruebas para la IA, así como un marco para la cooperación entre las autoridades pertinentes implicadas en la supervisión de dichos espacios. Los espacios controlados de pruebas para la IA establecidos en virtud del presente Reglamento deben entenderse sin perjuicio de otros actos legislativos que permitan el establecimiento de otros espacios controlados de pruebas encaminados a garantizar el cumplimiento de actos legislativos distintos del presente Reglamento. Cuando proceda, las **autoridades competentes pertinentes** encargadas de esos otros espacios controlados de pruebas deben ponderar las ventajas de utilizarlos también con el fin de garantizar el cumplimiento del presente Reglamento por parte de los sistemas de IA. Previo acuerdo entre las autoridades nacionales competentes y los participantes en el espacio controlado de pruebas para la IA, las pruebas en condiciones reales también podrán gestionarse y supervisarse en el marco del espacio controlado de pruebas para la IA.
Art. 57.10 RIA	***National competent authorities*** shall ensure that, to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data, the national data protection authorities and those **other national or competent authorities** are associated with	Las **autoridades nacionales competentes** velarán por que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes que proporcionen o respalden el acceso a los datos, las autoridades nacionales de protección de datos y las **demás autoridades**

	the operation of the AI regulatory sandbox and involved in the supervision of those aspects to the extent of their respective tasks and powers.	**nacionales o competentes** estén ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y competencias.

A partir de la comparació entre els diferents preceptes del RIA, es pot observar que el concepte d'*autoritat nacional competent* està definit específicament a l'article 3.48 del RIA, mentre que el terme d'*autoritat competent pertinent* apareix en altres apartats del RIA, com ara el considerant 139, sense una definició clara i tancada. Aquesta distinció és fonamental per comprendre'n l'àmbit d'aplicació i les possibles implicacions jurídiques.

L'article 3.48 delimita el concepte d'autoritat nacional competent com una autoritat notificadora o una autoritat de vigilància del mercat; en canvi, en el cas dels sistemes d'IA utilitzats per institucions, òrgans i organismes de la Unió, fa referència al Supervisor Europeu de Protecció de Dades. Això suggereix que aquest tipus d'autoritat té un àmbit clarament delimitat i vinculat, principalment, a la supervisió del mercat i a la notificació de sistemes d'IA.

D'altra banda, el considerant 139 introdueix el concepte d'autoritat competent pertinent i indica que aquest tipus d'autoritat està implicada en la supervisió dels espais controlats de proves per a IA. Aquest considerant també fa referència a la cooperació entre diferents autoritats en la supervisió d'aquests espais, incloses les que puguin tenir competències en altres normatives més enllà del RIA. Això podria indicar que les autoritats competents pertinents tenen un abast més ampli i poden incloure organismes amb funcions de supervisió en altres àmbits normatius, com ara la protecció de dades, la seguretat o els drets fonamentals; o, simplement, en referència a altres normatives harmonitzades que regulen altres productes relacionats amb la vigilància de mercat.

Per exemple, en referència a l'article 26, els responsables del desplegament tenen l'obligació de cooperar amb les autoritats competents pertinents, en qualsevol mesura relacionada amb l'ús dels sistemes d'IA d'alt risc, amb l'objectiu de garantir l'aplicació del RIA. L'article 26 no esmenta explícitament les autoritats de protecció de dades com a 'competents pertinents' a aquest efecte; tanmateix, a partir del que s'ha exposat prèviament a l'apartat 2.4 d'aquest treball i respecte del contingut general de la norma, una hipòtesi/conclusió preliminar a la qual es pot arribar és que aquestes autoritats també en podrien formar part, especialment en relació amb l'ús de sistemes d'identificació biomètrica remota en diferit, atès el seu paper clau en la supervisió d'aquest tipus de tractaments (com s'ha analitzat en els apartats previs).

Aquesta obligació de cooperació no figurava a la proposta original de la Comissió, sinó que apareix per primera vegada a la versió del Consell i posteriorment, amb algunes modificacions, a les esmenes introduïdes pel Parlament. No obstant això, l'article 26.12 no detalla en què ha de consistir exactament aquesta cooperació. Es poden considerar diverses possibilitats, com ara l'obligació de facilitar a les autoritats competents pertinents l'accés als registres generats automàticament pels sistemes d'IA d'alt risc (d'acord amb el que preveu, per exemple, l'article 21.2 del RIA, que utilitza el concepte d'autoritat competent en lloc d'autoritat nacional competent), o bé de subministrar qualsevol altra informació sota el seu control.

Si les autoritats de protecció de dades es consideren com a autoritats competents pertinents, com s'apuntava prèviament, aquesta nova obligació s'alinea amb les estipulacions de l'RGPD, on ja s'exigeix que els responsables i encarregats del tractament cooperin amb les autoritats de control. Així, es consolida un marc de supervisió i col·laboració essencial per abordar els reptes i riscos associats als sistemes d'IA d'alt risc. Tal com es disposa a l'article 31 de l'RGPD, el responsable i l'encarregat del tractament, i si escau els seus representants, han de cooperar en l'acompliment de les funcions de l'autoritat de control que ho sol·liciti, i aquesta és una qüestió valorable en un procediment sancionador (art. 83.2.*f*. RGPD i 99 RIA).

3. El nou rol de les autoritats de protecció de dades com a autoritats de drets fonamentals

Daniel Duro Millan

Quan parlem de protecció de dades, no només parlem de riscos i beneficis, sinó també de drets fonamentals, i el dret a la protecció de dades és sens dubte un dels més afectats per la intel·ligència artificial. Prova d'això és la designació del Supervisor Europeu de Protecció de Dades com a supervisor del RIA, així com les diverses guies, recomanacions i plans d'acció publicats en els darrers anys per diverses autoritats de protecció de dades (APD), com ara l'APDCAT, l'AEPD, la CNIL o l'ICO, entre d'altres, en què ja s'alertava sobre els riscos que podia arribar a comportar la IA.[20]

Consegüentment, a l'hora de publicar el llistat d'autoritats encarregades de protegir els drets fonamentals (APDF), en virtut de l'obligació imposada a l'article 77.2 del RIA, l'Estat espanyol ha designat, entre un llarg llistat, a tres APD:[21] l'Agència Espanyola de Protecció de Dades, l'Autoritat Catalana de Protecció de Dades i el Consell de Transparència i de Protecció de Dades d'Andalusia. No obstant això, sorprèn l'absència de l'Autoritat Basca de Protecció de Dades en aquest llistat, especialment tenint en compte que s'hi han inclòs les altres dues autoritats autonòmiques existents.[22]

La designació de les APDF efectuada en molts estats membres, inclòs l'Estat espanyol, no ha cobert de manera exhaustiva i concreta tots els drets fonamentals esmentats al RIA. És a dir, no es preveu la designació d'organismes *ad hoc* per a la protecció de certs drets fonamentals. Un exemple destacat és el dret a la no discriminació que, tot i que l'article 77.1 del RIA el cita explícitament i que compta amb organismes per protegir-lo,[23] a la llista de nomenaments no hi apareix cap organisme que el supervisi. Això contrasta amb altres drets

---

[20] Autoritat Catalana de Protecció de Dades (APDCAT). *Intel·ligència artificial. Decisions automatitzades a Catalunya.* 2020. [en línia] Disponible a: https://apdcat.gencat.cat/web/.content/03-documentacio/intelligencia_artificial/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf

Agència Espanyola de Protecció de Dades (AEPD). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción,* 2020. [en línia] Disponible a: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf

Commission Nationale de l'Informatique et des Libertés (CNIL). *Artificial intelligence: the action plan of the CNIL,* 2023. [en línia] Disponible a: https://www.cnil.fr/en/artificial-intelligence-action-plan-cnil

Information Comissioner's Office (ICO). *Guidance on AI and Data Protection,* Actualitzat a maig de 2023. [en línia] Disponible a: ico.org.uk/media2/ga4lfb5d/guidance-on-ai-and-data-protection-all-2-0-38.pdf

[21] Secretaria d'Estat de Digitalització i Intel·ligència Artificial. *Authorities protecting fundamental rights | Spain.* 2024. [en línia] Disponible a: https://digital.gob.es/dam/es/portalmtdfp/DigitalizacionIA/AuthoritiesFundamentalRights-Spain.pdf

[22] L'Autoritat Basca de Protecció de Dades no es troba nomenada com APDF a la data de publicació d'aquest treball.

[23] Com a Catalunya, l'Oficina d'Igualtat de Tracte i No-discriminació.

fonamentals, com el de la protecció de dades personals que, com s'ha apuntat, té assignades tres de les quatre autoritats existents a l'Estat espanyol.

En aquest context, en què diverses APD han estat designades com a APDF, és fonamental entendre què implica aquesta designació. No es tracta exclusivament d'un canvi nominal, sinó també de l'adquisició de noves competències, poders i responsabilitats.

Des del moment de designació com a APDF, el treball proactiu ha de permetre que, un cop arribat el 2 d'agost de 2026, en què el RIA serà aplicable,[24] les autoritats de protecció de dades com l'APDCAT hagin pogut adaptar internament les seves estructures, formar el seu personal i establir els protocols interns necessaris per exercir òptimament, des d'un bon inici, les competències derivades dels articles 73.7, 77, 79.2 i 82.1 del RIA.

Un exemple d'aquest treball proactiu és el model pioner a Europa que l'APDCAT ha publicat recentment, per a l'avaluació d'impacte sobre els drets fonamentals en l'ús d'intel·ligència artificial (AIDF).[25] Citant el mateix document, es tracta d'un model que aspira a esdevenir una eina eficaç per desenvolupar solucions d'IA fiables i centrades en l'ésser humà, dissenyada per concretar les noves obligacions establertes pel RIA. Aquesta iniciativa difereix d'altres metodologies aprovades darrerament, com és el cas d'HUDERIA,[26] publicada a finals de 2024 per Consell d'Europa, ja que la proposta catalana concreta la implementació de les variables, la gestió dels paràmetres i, explora l'aplicació pràctica del model mitjançant quatre casos d'ús reals.

Així doncs, als apartats següents s'analitzen les principals competències que el RIA atorga a les APD nomenades com a APDF, prestant especial atenció a la convergència d'aquestes competències amb les que tenen atribuïdes en virtut de l'RGPD.

3.1. Accés a documentació creada o conservada de conformitat amb el RIA, necessària per complir-ne el mandat (art. 77.1 RIA)

"Las autoridades u organismos públicos nacionales encargados de supervisar o hacer respetar las obligaciones contempladas en el Derecho de la Unión en materia de protección de los derechos fundamentales, incluido el derecho a la no discriminación, con respecto al uso de sistemas de IA de alto riesgo mencionados en el anexo III tendrán la facultad de solicitar cualquier documentación creada o conservada con arreglo al presente Reglamento y de acceder a ella, en un lenguaje y formato accesibles, cuando el acceso a dicha

[24] No obstant això, l'article 6.1 i les obligacions corresponents del RIA són aplicables a partir del 2 d'agost del 2027 (art. 113.*c* RIA).

[25] APDCAT. *Model per a l'AIDF: guia i casos d'ús. Metodologia aplicada de l'avaluació d'impacte sobre els drets fonamentals en el disseny i desenvolupament de la IA.* 2025. [en línia] Disponible a: https://apdcat.gencat.cat/ca/documentacio/intelligencia_artificial/

[26] Consell d'Europa, *Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (HUDERIA METHODOLOGY)* 2024. [en línia] Disponible a: https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f

documentación sea necesario para el cumplimiento efectivo de sus mandatos, dentro de los límites de su jurisdicción (...)."

Aplicable a partir del 2 d'agost de 2026.

L'article 77.1 del RIA estableix la facultat a les APDF de: (i) sol·licitar l'accés a qualsevol documentació creada o conservada d'acord amb el RIA; (ii) relativa als sistemes d'IA enumerats a l'annex III; i (iii) quan aquest accés sigui necessari per complir el mandat de l'autoritat, dins de la seva jurisdicció. Per tant, perquè una APDF pugui sol·licitar documentació cal complir tres requisits.

En primer lloc, la documentació que es podrà sol·licitar serà la "creada o conservada con arreglo al presente Reglamento". Això implica que les APDF poden sol·licitar tota la documentació que el RIA preveu que els operadors han de crear o conservar, per permetre un seguiment adient dels SIA d'alt risc enumerats a l'annex III. Alguns exemples són els articles 11, 12 i 13 del RIA.

En segon lloc, la documentació que se sol·licita ha de ser relativa a sistemes d'IA d'alt risc recollits a l'annex III. Cal destacar que, segons l'article 6 del RIA, els sistemes inclosos a l'annex III no són els únics que el RIA reconeix com d'alt risc. Per tant, les APDF només poden sol·licitar documentació relativa a un nombre concret de sistemes d'IA d'alt risc. Tanmateix, cal tenir en compte que quan una APD sigui alhora APDF, en haver estat nomenada com a tal en virtut de l'article 77.2 del RIA, pot accedir a qualsevol documentació necessària per assegurar que es compleix l'RGPD, d'acord amb el considerant 157 del RIA i l'article 58.1 de l'RGPD. Així, les APD poden accedir a qualsevol documentació per exercir les seves funcions d'acord amb l'RGPD quan un SIA, tot i no estar inclòs a l'annex III, comporti el tractament de dades personals. Per tant, la circumscripció d'accés a la documentació emmarcada a l'annex III afectarà les APDF que no tinguin una via alternativa d'accés a documentació, més enllà de l'habilitació de l'article 77.1 del RIA.

En qualsevol cas, pel que fa als SIA sobre els quals les APDF poden sol·licitar documentació en virtut de l'article 77.1 del RIA, l'article 6 estableix les normes generals per classificar els sistemes d'IA com a sistemes d'alt risc; per la seva banda, l'annex III enumera àmbits i casos d'usos específics de sistemes d'IA que han de ser considerats d'alt risc, amb diferents excepcions associades. Aquesta classificació ha estat objecte de nombrosos debats i negociacions durant la tramitació del projecte normatiu, fins a la versió final (Muñoz Vela 2024).

Els sistemes d'IA d'alt risc recollits a l'annex III inclouen aplicacions en àmbits especialment sensibles, com ara la biometria (identificació, categorització o reconeixement d'emocions), infraestructures crítiques, educació, ocupació, accés a serveis essencials, compliment normatiu, migració i control fronterer i administració de justícia i processos democràtics.

La confecció de la llista de sistemes d'IA d'alt risc inclosos a l'annex III, més enllà de la classificació general que fa l'article 6 del RIA per determinar quan un SIA ha de ser considerat d'alt risc, respon a un treball de la Comissió basat en la determinació de quins SIA generaven un alt risc per a la salut, la seguretat o els drets fonamentals de les persones

(Muñoz Vela 2024). Així es recull al considerant 46 de l'articulat final del RIA i es justifica al considerant 157, en establir la necessitat d'un procediment de salvaguarda específic per garantir una execució adequada i oportuna enfront de SIA que presentin un risc per a la salut, la seguretat o els drets fonamentals.

Per l'afectació que pot implicar a les competències de les APDF, escau assenyalar que, d'acord amb els articles 7 i 97 del RIA, la Comissió té la facultat d'adoptar actes delegats per modificar o afegir casos d'ús de SIA a l'annex III. En atenció a això, la llista de SIA sobre els quals les APDF poden sol·licitar documentació, així com sobre els quals poden sol·licitar motivadament l'organització de proves, com es veurà a l'apartat 3.3 d'aquest treball, podria variar en el futur.

Aquesta decisió de deixar oberta la possibilitat de modificar o desenvolupar contingut de l'articulat del RIA no és exclusiva per a l'annex III, sinó que, d'acord amb l'article 96 del RIA, es preveu que la Comissió elabori directrius sobre l'aplicació pràctica del RIA, com ha fet recentment amb les directrius relatives a SIA prohibits.[27] Aquesta fórmula ha de permetre que, en un àmbit tant canviant com la IA, en la mesura del possible es pugui regular a la velocitat a què evoluciona la tecnologia.

L'exemple més paradigmàtic, esmentat a la introducció d'aquest informe, és la incorporació del concepte de models i sistemes d'IA d'ús general arran de l'aparició de ChatGPT, que van suposar l'adaptació del projecte d'articulat del RIA per encabir la regulació específica d'aquests SIA dins del reglament.

L'últim requisit a complir perquè les APDF puguin exercir la facultat reconeguda a l'article 77.1 del RIA és la fonamentació de la sol·licitud d'accés a documentació en el "cumplimiento efectivo de sus mandatos" Això implica que cada organisme designat com a APDF per un estat membre de la UE pot sol·licitar documentació relativa a SIA que suposin un risc per al dret o els drets fonamentals que protegeixen amb relació a l'annex III. En aquest cas, és evident que les APD, com l'APDCAT, s'emmarquen en la protecció del dret fonamental a la protecció de dades personals, i del conjunt de drets i llibertats que es puguin veure afectats pels tractaments de dades.

En relació amb el paper de les APD en el marc del RIA, com s'ha advertit a l'apartat 2.7 d'aquest treball, el Reglament preveu a l'article 74.8 que les APD esdevinguin AVM en relació amb els SIA recollits a l'annex III. En aquest sentit, a la "Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial", el Comitè Europeu de Protecció de Dades s'ha pronunciat positivament respecte d'aquesta possibilitat, posant en relleu el paper de les autoritats de protecció de dades en la supervisió d'aquests sistemes. Aquesta qüestió resulta especialment rellevant —com s'observarà als apartats següents d'aquest treball—, ja que les funcions i poders assignats a

[27] European Comission. *Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).* 2025. [en línia] Disponible a: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

les APDF, principalment orientats a l'anàlisi documental en el marc de la potestat d'investigació i avaluació, estan estretament vinculats a les facultats executives atorgades a les AVM.

En aquest context, tot i que ja es coneixen els organismes que l'Estat espanyol ha designat com a APDF, encara manca el pronunciament oficial sobre quin o quins ho seran com a AVM.[28] Aquesta designació, a diferència de les APDF, no és preceptiva fins el 2 d'agost de 2025. Conseqüentment, cal tenir present la possibilitat que les APD puguin assumir simultàniament els rols d'APDF i AVM.

Tornant a l'article 77.1 del RIA, com a deure dels operadors s'especifica que la documentació a què poden sol·licitar accés les APDF s'ha de transmetre en un llenguatge i format accessibles per als subjectes requerits. Aquesta exigència respon a un dels principals reptes de fiscalització de la IA: poder comprendre els processos que generen els resultats, així com les dades que s'han utilitzat, com a element essencial de transparència. En aquest mateix sentit ja es pronunciava un informe de l'Agència Europea de Drets Fonamentals (FRA) de l'any 2021, que analitzava els principals esdeveniments en l'àmbit dels drets fonamentals dins de la UE i destacava tant els progressos realitzats com les dificultats que encara persistien.[29] Concretament, el dictamen 6.4 de l'informe de la FRA tracta de la possible introducció d'eines d'IA dins de la UE, per millorar les decisions en assumptes de fronteres, asil i immigració, i assenyala que la falta de transparència en relació amb les dades utilitzades podria dificultar que les persones afectades poguessin refutar els resultats obtinguts per aquestes eines.

Finalment, en analitzar l'article 77.1 del RIA des de l'òptica de la protecció de dades personals, s'evidencia la semblança amb l'article 58.1.*a* de l'RGPD, quan preveu per a les autoritats de protecció de dades el poder "de ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones." Tanmateix, s'observen tres diferències entre ambdós articles.

- En primer lloc, l'article 58.1.*a* de l'RGPD especifica clarament els subjectes a qui pot adreçar-se l'autoritat de protecció de dades per sol·licitar informació; en canvi, el RIA només preveu la possibilitat de sol·licitar documentació, sense indicar si els destinataris podrien ser tots els subjectes que l'article 3.8 del RIA cataloga com a operadors. No obstant això, la lògica fa pensar que les APDF podran sol·licitar documentació a qualsevol operador del RIA que posseeixi la documentació necessària per al compliment efectiu del seu mandat, dins dels límits de la seva jurisdicció.

[28] El març de 2025 s'ha presentat l'Avantprojecte de llei per al bon ús i la governança de la intel·ligència artificial, que ha de concretar aquesta qüestió; tot i això, fins que se'n publiqui el text final no es coneixerà amb certesa el llistat d'autoritats designades.

[29] Agència de la Unió Europea pels Drets Fonamentals (FRA). Informe sobre los derechos fundamentales, 2021. [en línia] Disponible a: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-fundamental-rights-report-2021-opinions_es.pdf

- En segon lloc, i com s'analitzarà a l'apartat següent, mentre que les autoritats de control de protecció de dades no han de comunicar les seves peticions d'informació a cap altre organisme, les APDF estan obligades a notificar les seves sol·licituds d'accés a documentació a les AVM.

- En darrer lloc, les APD poden sol·licitar qualsevol informació requerida per complir les seves funcions. Per contra, la documentació que poden sol·licitar les APDF s'ha de circumscriure a SIA d'alt risc enumerats a l'annex III.

Aquestes tres diferències no s'aprecien si, en comptes de comparar l'article 58.1.*a* de l'RGPD amb l'article 77.1 del RIA, se substitueix aquest darrer per l'article 14.4.*a* de l'RVM, que recull el poder de les AVM d'exigir documentació als operadors. Així, les AVM poden exigir qualsevol documentació, sense haver-ho de notificar a cap altra autoritat i sense limitar els productes respecte dels quals poden exercir aquest poder.

Aquesta comparativa evidencia la diferència entre els poders d'investigació amb què compten les APD en virtut del RIA i l'RGPD, en el marc de les seves respectives competències i rols, en comparació amb els de les AVM. Aquesta diferència s'accentua si es comparen els poders executius amb els de les APDF i AVM, com s'exposa als apartats següents d'aquest treball.

En aquest context, i com es reitera al llarg del document, és important tenir en compte que els poders que el RIA atorga a les APDF són independents dels que ja disposen les APD en virtut de l'RGPD. Això comporta que les competències adquirides com a APDF no puguin limitar les que ja s'exerceixen d'acord amb l'RGPD, tal com estableix l'article 2.7 del RIA.

3.2. Informar a l'autoritat de vigilància del mercat de sol·licituds de documentació creada o conservada de conformitat amb el RIA, necessària per complir-ne el mandat (art. 77.1 RIA)

"(...) La autoridad u organismo público pertinente informará sobre cualquier solicitud de este tipo a la autoridad de vigilancia del mercado del Estado miembro que corresponda."

Aplicable a partir del 2 d'agost de 2026.

En compliment de l'article 77.1 *in fine,* en exercici de la facultat d'accés a documentació que es desenvolupa a l'apartat 3.1 d'aquest treball, les APDF han d'informar les AVM de l'estat membre corresponent de les sol·licituds d'accés a documentació que s'hagin efectuat als operadors.

De l'articulat del precepte es desprèn que el deure d'informar no suposa que calgui la validació de l'AVM per accedir a la documentació sol·licitada. A més, no s'especifica l'ús o servei que aquesta notificació pot suposar per a l'AVM. Un escenari raonable seria emmarcar-ho dins de la previsió de l'article 11.3 de l'RVM, que estipula que, a l'hora de fer comprovacions de productes, les AVM han d'aplicar un enfocament basat en el risc en què, entre altres factors, cal tenir en compte la informació provinent d'altres autoritats. En aquest context, es tractaria d'un mecanisme que ajudaria les AVM a determinar quins SIA podrien

suposar un risc per als DF i mereixen ser avaluats. Aquesta previsió també es podria connectar amb l'article 79.2 del RIA, que estipula que, quan les AVM tinguin motius suficients per considerar que un SIA presenta un risc, d'acord amb la definició de l'article 3.19 de l'RVM, cal avaluar-lo.

Addicionalment, la redacció final del RIA deixa sense concretar altres aspectes d'aquest deure, com ara l'absència d'un termini específic per efectuar la notificació a l'AVM, o l'AVM a notificar, en cas que hi hagi més d'una autoritat que podria ser considerada competent. En relació amb això, el RIA no determina si sempre s'ha de notificar a una AVM del mateix estat, o bé, quan l'operador tingui l'establiment principal en un altre estat membre, a l'AVM d'aquell estat.

En contrast, el considerant 36 de l'RGPD delimita el concepte d'establiment principal del responsable i encarregat de tractament, que després s'usa a l'article 56 per determinar la competència de l'autoritat de control principal. A més, el dictamen 4/2024 del CEPD[30] delimita exhaustivament el concepte d'establiment principal d'un responsable del tractament, d'acord amb l'RGPD.

Addicionalment, convé esmentar que al capítol VII de l'RGPD es recull el mecanisme de coherència per a la cooperació entre autoritats de protecció de dades. Queda pendent, per tant, desenvolupar el RIA en aquest àmbit, perquè proporcioni la mateixa seguretat jurídica que ofereix l'RGPD.

3.3. Sol·licitud de proves dels sistemes d'IA d'alt risc i col·laboració en l'organització de les proves (art. 77.3 RIA)

"Cuando la documentación mencionada en el apartado 1 no baste para determinar si se ha producido un incumplimiento de las obligaciones previstas en el Derecho de la Unión en materia de protección de los derechos fundamentales, la autoridad u organismo público a que se refiere el apartado 1 podrá presentar una solicitud motivada a la autoridad de vigilancia del mercado para organizar pruebas del sistema de IA de alto riesgo a través de medios técnicos. La autoridad de vigilancia del mercado organizará las pruebas con la estrecha colaboración de la autoridad u organismo público solicitante en un plazo razonable tras la presentación de la solicitud."

Aplicable a partir del 2 d'agost de 2026.

[30] EDPB. *Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR*. 13 de febrer de 2024. [en línia] Disponible a: https://www.edpb.europa.eu/system/files/2024-02/edpb_opinion_202404_mainestablishment_en.pdf#:~:text=The%20French%20Supervisory%20Authority%20requested%20the%20European%20Data,mechanism%2C%20in%20particular%20regarding%20the%20notion%20of%20controll

El considerant 139 del RIA desenvolupa el concepte d'espai controlat de proves de sistemes d'IA. Aquest recull el deure de cooperació entre les autoritats nacionals competents que estableixin espais controlats de proves d'IA, amb altres autoritats, com les APDF ("cooperar con otras autoridades pertinentes, incluidas las que supervisan la protección de los derechos fundamentales").

En aquest context, i tenint en compte que al RIA no es recull cap altre situació en què les APDF poden participar a l'espai controlat de proves, l'anàlisi d'aquest article parteix de la premissa que, quan l'article 77.3 del RIA estableix que les APDF poden presentar una sol·licitud motivada a l'AVM per organitzar proves de SIA d'alt risc a través de mitjans tècnics, es pot entendre que es refereix a l'organització de proves en un espai controlat de proves. No obstant això, no es pot descartar que el legislador del RIA, en referir-se a "organizar pruebas del sistema de IA de alto riesgo a través de medios técnicos", no estigui fent referència als espais controlats de proves d'IA.

Feta aquesta consideració prèvia, l'article 77.3 del RIA exposa que si, amb la documentació sol·licitada en virtut de l'article 77.1 del RIA, una APDF no pot determinar si s'ha produït un possible incompliment del Dret de la Unió en matèria de protecció dels drets fonamentals, es preveu un segon mecanisme de verificació d'adequació: la sol·licitud motivada a l'AVM per organitzar proves del sistema d'IA objecte d'investigació. Tot i no trobar-se explícitament estipulat, es dedueix que l'AVM tindrà la potestat d'acceptar o denegar l'organització de les proves. En aquest sentit, manca concreció en relació amb els motius o requisits que ha de complir la sol·licitud, per poder ser acceptada o denegada.

Una qüestió que el precepte no concreta és l'abast del concepte *estrecha colaboración* amb què les AVM i les APDF han d'organitzar les proves. Així, si bé queda clar que l'APDF és qui sol·licita l'organització de proves de sistemes a l'AVM, no s'especifica com s'ha de materialitzar la col·laboració a l'hora d'organitzar-les. En qualsevol cas, queda clar que l'objectiu és completar la investigació iniciada per l'APDF en virtut de l'article 77.1 del RIA, quan amb la documentació sol·licitada no s'hagi pogut determinar si s'ha produït un incompliment de les obligacions de la UE en matèria de protecció dels DF. Així mateix, pot ser que l'accés a la documentació regulat a l'article 77.1, i la posterior organització de proves, sigui relativa a un SIA que, a part de ser d'alt risc de l'annex III, suposi un risc d'acord amb l'article 79.1 del RIA. En aquest supòsit, l'organització de les proves es podria vincular amb l'avaluació de SIA que regula l'article 79.2.

Addicionalment, l'article afegeix que l'organització de proves s'ha de produir en un termini raonable des que es va presentar la sol·licitud. S'infereix que el legislador no concreta el termini, ja que es busca dotar de flexibilitat les autoritats tenint en compte variables com la magnitud i complexitat de la prova que s'hagi d'organitzar, així com els recursos que s'hi hagin d'invertir. Tanmateix, com a mínim queda pendent establir un termini màxim per assegurar la viabilitat de les investigacions de les APD, en el marc de les seves competències atribuïdes per l'RGPD.

En aquest punt, escau esmentar l'article 57.10 del RIA, desenvolupat a l'apartat 2.6 d'aquest treball, relatiu al rol de les APD als espais de proves. D'acord amb aquest article, les APD

han d'estar lligades al funcionament dels espais controlats de proves per als SIA que tractin dades personals, així com involucrades en la seva supervisió.

Això implica que el RIA preveu que les APD, pel simple fet de ser-ho, tenen potestat per actuar en la supervisió dels espais controlats de prova de sistemes d'IA, tot i que l'articulat del RIA tampoc concreta aquesta actuació. Així doncs, el valor afegit que s'atorga amb el nomenament com a APDF és la facultat de presentar sol·licituds motivades a les AVM, per organitzar proves en els casos en què l'APDF ho consideri necessari, d'acord amb el que preveu l'article 77.3.

Aquest últim matís és rellevant ja que aquesta extensió no és aplicable als SIA sobre els quals es pot sol·licitar l'organització de proves, tot i que a l'apartat 3.1 d'aquest treball s'explica que, per les competències que els atorga l'RGPD, les APDF que siguin alhora APD poden accedir a qualsevol documentació, i no només a la relativa a SIA inclosos a l'annex III. Això és així perquè l'article 77.3 disposa que les APDF poden sol·licitar l'organització de proves respecte dels SIA a què poden sol·licitar documentació en virtut de l'article 77.1 del RIA. És a dir, respecte dels SIA d'alt risc enumerats a l'annex III i no de qualsevol SIA que tracti dades personals.

Finalment, encara que no s'analitzarà, convé esmentar que el tercer apartat de l'article 57 del RIA atorga al Supervisor Europeu de Protecció de Dades, que és alhora Supervisor del RIA, la potestat d'establir un espai controlat de proves per les institucions, òrgans i organismes de la UE; també, que pot exercir les mateixes funcions que les autoritats nacionals competents en aquesta matèria.

3.4. Ser informades de la recepció de notificacions a l'AVM sobre incidents greus a què es refereix l'article 3.49.*c* del RIA (art. 73.7 RIA)

"Tras la recepción de una notificación relativa a un incidente grave a que se refiere el artículo 3, punto 49, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo. Dichas orientaciones se publicarán a más tardar el 2 de agosto de 2025 y se evaluarán periódicamente."

Aplicable a partir del 2 d'agost de 2026.

L'article 3.49.*c* del RIA defineix l'incident greu com aquell incident o defecte de funcionament d'un sistema d'IA que, directament o indirectament, tingui com a conseqüència l'incompliment d'obligacions en virtut del Dret de la Unió destinades a protegir els drets fonamentals. Si es produeix un incident greu d'aquestes característiques, l'article 73.7 del RIA estableix que l'AVM l'ha de notificar a l'APDF corresponent.

Tot i que l'article 73.7 del RIA no especifica quin ús han de fer les APDF de les notificacions d'incidents greus, es pot interpretar que aquesta notificació està vinculada a les potestats que tenen reconegudes a l'article 77.1 del RIA per complir el seu mandat i vinculades a la

seva jurisdicció. Aquest enllaç permetria a les APDF que són APD exercir les seves funcions per investigar i garantir la protecció dels drets fonamentals afectats per l'incident (concretament, el dret a la protecció de dades), així com obrir una investigació contra l'operador (quan també actuï com responsable o encarregat del tractament), en cas de manca de notificació de violació de seguretat, si aquest hi està obligat per l'RGPD.

Des de la perspectiva de protecció de dades, les notificacions d'incidents greus previstes al RIA segueixen una estructura semblant a les notificacions de violació de seguretat (NVS) regulades als articles 33 i següents de l'RGPD. Així, en ambdós casos es tracta d'una notificació d'un responsable del tractament o operador a l'autoritat de control o vigilància pertinent, per comunicar unes circumstàncies que provoquen l'incompliment de l'RGPD o del RIA.

En aquest context, es pot donar el cas que un proveïdor de SIA, que també sigui responsable del tractament segons l'RGPD, pateixi un incident de seguretat que derivi d'un defecte del SIA; incident que, al seu torn, comporti un risc per al dret fonamental a la protecció de dades personals. En aquest cas, l'APD podria rebre la notificació per duplicat:

- En primer lloc, del proveïdor, en virtut de l'article 33 de l'RGPD.

- En segon lloc, de l'AVM, d'acord amb l'article 73.7 del RIA, un cop el proveïdor del sistema d'IA li hagués notificat, d'acord amb l'obligació que li imposa l'article 73.1 del RIA.

Respecte d'això, hi ha acadèmics que consideren que els organismes que entrin en l'àmbit d'aplicació de més d'una norma de la UE poden patir una sobrecàrrega de notificacions. Per evitar-ho, s'han plantejat possibles alternatives.

Una possibilitat és l'exigència a les APDF, que en qualitat d'APD reben NVS d'acord amb l'RGPD, de notificar la violació de seguretat a les AVM, quan sigui conseqüència d'un SIA d'alt risc (Karathanasis 2024). Així doncs, aplicant aquesta proposta, quan les APDF siguin alhora APD sota l'RGPD, les AVM no els notificarien els incidents previstos a l'article 3.49.*c* del RIA, com preveu l'article 73.7 del RIA, sinó que les mateixes APD remetrien a les AVM qualsevol NVS relativa a sistemes d'IA que pugui suposar un incident greu. Aquest sistema de notificació es justifica en raó de la probabilitat superior que siguin les APD les primeres a assabentar-se de les violacions de seguretat, des del punt de vista de la normativa de protecció de dades, i d'incidents greus, en el sentit de l'article 3.49.*c*, per al dret fonamental a la protecció de dades, des del punt de vista del RIA.

Si bé, la justificació d'aquesta proposta no es troba desenvolupada, es podria deure als terminis que tant l'RGPD com el RIA preveuen per a les notificacions respectives. Així, mentre que l'RGPD preveu que el responsable del tractament notifiqui l'NVS en un termini màxim de 72 hores, des que en té constància (art. 33.1), el RIA preveu un termini no superior a 15 dies perquè els proveïdors facin la notificació a les AVM (art. 73.2), i no preveu el termini en què, després, l'AVM l'ha de notificar a l'APDF (art. 73.7). Per tant, en cas que un operador, alhora responsable del tractament, tingués coneixement d'una vulneració del dret fonamental a la protecció de dades i ho notifiqués per les dues vies esmentades,

sembla raonable pensar que l'APD ho conegués abans. Això no obstant, el fet que el RIA i l'RGPD supervisin matèries tan diferents pot comportar que, quan un SIA pateixi un incident greu, que impliqui la vulneració de la normativa de protecció de dades, els proveïdors notifiquin a les AVM l'incident greu, però no l'NVS a les APD. En aquest sentit, juntament amb la disparitat en el termini de notificació, cal tenir en compte que, si bé ambdues notificacions segueixen un esquema similar, consistent a notificar a l'autoritat pertinent una situació que vulnera el seu respectiu reglament, hi ha altres diferències cabdals en la seva naturalesa i finalitat.

La notificació d'incident greu s'efectua quan un proveïdor que introdueix un SIA al mercat de la Unió constati un incident greu, d'acord amb la definició que en fa l'article 3.49 del RIA. Així, aquest article preveu quatre conseqüències del mal funcionament d'un SIA que deriven en incident greu: a) la mort o perjudici greu per a la salut d'una persona; b) l'alteració greu i irreversible de la gestió o funcionament d'infraestructures crítiques; c) l'incompliment de les obligacions en virtut del dret de la Unió destinades a protegir els DF; i d) danys greus a la propietat o el medi ambient. Quan es produeix una d'aquestes situacions, el proveïdor ho notifica a l'AVM en el termini màxim de 15 dies en general. A més, si l'incident deriva del cas *c*, addicionalment l'AVM l'ha de notificar a l'APDF en un termini no establert al RIA.

D'acord amb l'article 73.8 del RIA, una de les principals conseqüències derivada de la notificació de l'incident greu és que, en un termini no superior a 7 dies des de la recepció de la notificació, les AVM han d'adoptar les mesures recollides a l'article 19 de l'RVM. Aquestes són la facultat de recuperar o retirar el producte, entre d'altres que evitin la comercialització de productes que suposin un risc greu. Per la seva banda, l'NVS s'efectua quan un responsable del tractament constata una violació de seguretat en un tractament de dades personals, d'acord amb la definició de l'article 4.12 de l'RGPD. Aquesta notificació compleix diferents funcions per a les APD a les quals es notifica. Per exemple, permet analitzar l'impacte en els drets i llibertats dels ciutadans afectats, investigar si l'organisme que ha patit la violació de seguretat compleix la normativa i disposa de les mesures adequades per intentar evitar-lo, així com sol·licitar o imposar mesures correctores per mitigar l'esdeveniment i altres possibles conseqüències.

Per tant, en el context en què una violació de seguretat en matèria de protecció de dades provingui d'un SIA, és possible que el proveïdor notifiqui l'incident a l'AVM que supervisa el producte que el proveïdor pretén comercialitzar (un SIA); però pot ser que no sigui conseqüent amb el seu rol de responsable del tractament i no notifiqui la violació de seguretat, per exemple perquè no ha adoptat un sistema de governança integral del compliment normatiu. Per tant, en els supòsits en què una violació de seguretat provingui d'un SIA, és possible que la notificació prevista a l'article 73.7 del RIA sigui l'únic mecanisme de què disposin les APD per tenir-ne coneixement.

En un altre sentit, el termini de 7 dies que recull l'article 73.8 del RIA dificulta que, en trobar-nos amb un incident greu derivat del supòsit de l'article 3.49.*c* del RIA, les APDF disposin de prou temps per avaluar el perjudici de l'incident per als DF i cooperar amb les AVM per determinar les mesures més adients a adoptar. Val a dir que els apartats 3 i 4 de l'article 73 del RIA estableixen dos supòsits en què els terminis de notificació són més curts, però no comporten cap canvi significatiu a la problemàtica plantejada. En qualsevol cas, no s'ha

previst que la notificació de l'article 73.7 suposi l'avaluació conjunta de l'AVM i l'ADPF de l'incident, per determinar les mesures més adients a prendre en virtut de l'article 73.8 del RIA. Tanmateix, sembla raonable que, si l'incident greu ho és perquè provoca que s'incompleixin les obligacions en virtut de la UE destinades a protegir els DF, les autoritats encarregades de protegir aquests drets participin en la delimitació de l'abast i les mesures més adients per mitigar els efectes de l'incident.[31]

Finalment, considerant els terminis de notificació que preveu el RIA, si les APD s'assabenten d'una violació de seguretat de protecció de dades exclusivament per mitjà d'una notificació d'incident greu, sembla prudent pensar que, en la majoria de situacions, això comportarà una vulneració del termini previst a l'article 33 de l'RGPD.

En resum, si bé sembla força possible que la notificació recollida a l'article 73.7 del RIA produeixi situacions de duplicitat de notificacions, també és un escenari a considerar que, sense la notificació de les AVM a les APDF, aquestes darreres no s'assabentin de moltes situacions amb potencial perjudici per al dret fonamental a la protecció de dades, especialment en els primers anys d'aplicació del RIA.

3.5. Procediment aplicable als sistemes d'intel·ligència artificial que "presenten un risc"

"Los sistemas de IA que presentan un riesgo se entenderán como «productos que presentan un riesgo» tal como se definen en el artículo 3, punto 19, del Reglamento (UE) 2019/1020, en la medida en que presenten riesgos que afecten a la salud, la seguridad o los derechos fundamentales de las personas." (art. 79.1 RIA)

"Cuando la autoridad de vigilancia del mercado de un Estado miembro tenga motivos suficientes para considerar que un sistema de IA presenta un riesgo mencionado en el apartado 1 del presente artículo, efectuará una evaluación del sistema de IA de que se trate para verificar su cumplimiento de todos los requisitos y obligaciones establecidos en el presente Reglamento. Debe prestarse una especial atención a los sistemas de IA que presenten un riesgo para los colectivos vulnerables. Cuando se detecten riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 77, apartado 1, y cooperará plenamente con ellos. Los operadores pertinentes cooperarán en lo necesario con la autoridad de vigilancia del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1.

Cuando, en el transcurso de tal evaluación, la autoridad de vigilancia del mercado o, cuando proceda, la autoridad de vigilancia del mercado en cooperación con la autoridad nacional pública a que se refiere el artículo 77, apartado 1, constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora

[31] En altres punts de l'articulat del RIA, com l'article 79.2, sí que es regula la cooperació entre AVM i APDF quan un SIA pot suposar un risc per als DF.

indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad podrá determinar y, en cualquier caso, en un plazo de quince días hábiles a más tardar o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes según corresponda." (art 79.2 RIA)

(...)

"Si, tras efectuar una evaluación con arreglo a lo dispuesto en el artículo 79 y consultar a la autoridad pública nacional a que se refiere el artículo 77, apartado 1, la autoridad de vigilancia del mercado de un Estado miembro concluye que un sistema de IA de alto riesgo, a pesar de cumplir con el presente Reglamento, presenta sin embargo un riesgo para la salud o la seguridad de las personas, para los derechos fundamentales o para otros aspectos de protección del interés público, pedirá al operador interesado que adopte todas las medidas adecuadas para garantizar que el sistema de IA de que se trate ya no presente ese riesgo cuando se introduzca en el mercado o se ponga en servicio sin demora indebida, dentro de un plazo que dicha autoridad podrá determinar." (art. 82.1 RIA)

Aplicable a partir del 2 d'agost de 2026.

La tercera secció del capítol IX del RIA es dedica a la garantia del compliment del Reglament (articles 74-84). En el marc d'aquesta secció, es regulen diversos procediments interrelacionats[32], entre els quals, el procediment aplicable als SIA que presenten un risc. En aquest, hi intervenen les APDF tal i com s'explicarà seguidament.

Abans de res, cal tenir en compte que quan el procediment parla de sistema d'IA que presenta un risc, aquest s'ha d'entendre com "producto que presenta un riesgo", d'acord amb la definició de l'article 3.19 de l'RVM[33], en la mesura que presentin un risc per la salut, seguretat o els drets fonamentals (art. 79.1 RIA). En aquest sentit, l'article 3.19 de l'RVM estableix que s'entenen per productes que presenten un risc aquells que afecten negativament […] en un grau que va més enllà del que es considera raonable i acceptable en relació amb la seva finalitat prevista o en les condicions d'ús normals o raonablement previsibles del producte en qüestió, inclosa la duració de la seva utilització i, en el seu cas, els requisits de la seva posada en servei, instal·lació i manteniment. Per tant, quan en aquest apartat es parli de "presenta un risc", es farà tenint en compte aquesta definició específicament.

---

[32] Aquests procediments no s'apliquen als SIA associats a productes regulats pels actes legislatius d'harmonització de la Unió enumerats en l'annex 1, secció A, quan aquests actes legislatius ja prevegin procediments que garanteixin un nivell equivalent de protecció amb un mateix objectiu (art. 74.4 RIA).

[33] Article 3.19 de l'RVM: "Producto que puede afectar negativamente a la salud y la seguridad de las personas en general, a la salud y la seguridad en el trabajo, a la protección de los consumidores, al medio ambiente, a la seguridad pública o a otros intereses públicos protegidos por la legislación de armonización de la Unión aplicable, en un grado que vaya más allá de lo que se considere razonable y aceptable en relación con su finalidad prevista o en las condiciones de uso normales o razonablemente previsibles del producto en cuestión, incluida la duración de su utilización y, en su caso, los requisitos de su puesta en servicio, instalación y mantenimiento."

El procediment que s'inicia a l'article 79 indica que quan una AVM "tenga motivos suficientes"[34] per considerar que un SIA presenta un risc, l'AVM avaluarà el SIA per verificar si compleix els requisits i obligacions que li imposa el RIA (en funció de la seva categoria).[35] Així mateix, quan el risc que es detecti ho sigui pels drets fonamentals, l'AVM informarà l'APDF pertinent i cooperarà plenament amb ella en l'avaluació del SIA corresponent (art. 79.2 RIA)[36]. Aquesta avaluació pot tenir dos possibles resultats: (i) bé, que es constati que el SIA avaluat no compleix amb els requisits o obligacions del RIA, (ii) bé que es constati que sí que els compleix.

Quan de l'avaluació del SIA es detecti que aquest no compleix amb els requisits o obligacions del RIA, l'AVM exigirà a l'operador pertinent que, en un termini a determinar per l'AVM[37]:

- adopti les mesures correctores oportunes per adaptar el SIA als esmentats requisits i obligacions;
- el retiri del mercat[38]; o bé,
- el recuperi[39].

Segons l'apartat 4 de l'article 79, l'operador s'assegurarà de complir i aplicar les mesures en tota la UE.

En el cas que l'operador no adopti les mesures adients per complir amb els requisits o obligacions del RIA, se seguirà el procediment establert als apartats 5 i 9 de l'article 79 i l'article 81, tal com s'explica a l'Annex 2 d'aquest treball, i l'AVM adoptarà les mesures provisionals necessàries per evitar que el SIA pugui suposar un perjudici dins del mercat de la UE. Això obre la porta a que AVM diferents a la que va iniciar el procediment també adoptin mesures quan el SIA afecti al seu territori i, per tant, es preveu un procediment de salvaguarda de la Unió[40] perquè la comissió avaluï si les mesures adoptades son justificades o no. En cas de

---

[34] Poden derivar-se de: la conservació de registres d'esdeveniments (art. 12.2.*a* RIA); informació del responsable del desplegament (art. 26.5 RIA); avaluacions de conformitat (art. 43 RIA); recepció de notificacions d'incidents greus (art. 73.1 RIA); notificació de sol·licitud d'accés a informació per part d'una APDF (art. 77.1 RIA); i reclamacions presentades davant d'una AVM (art. 85 RIA), entre d'altres.

[35] Aquest procediment s'iniciarà quan el SIA presenti un risc, independentment de si es tracta d'un SIA prohibit, d'alt risc o de risc limitat. La seva categorització, això sí, es tindrà en compte a l'hora d'avaluar els seus respectius requisits i obligacions.

[36] Convé destacar que els operadors també hauran de cooperar amb les APDF en aquesta avaluació (art. 79.2 in fine).

[37] Inferior a 15 dies hàbils o en el termini que prevegin els actes legislatius d'harmonització de la UE quan escaigui. (art. 79.2)

[38] D'acord amb la definició de l'article 3.22 de l'RVM.

[39] D'acord amb la definició de l'article 3.23 de l'RVM.

[40] Regulat a l'article 81 del RIA.

considerar-se justificades, tots els EEMM hauran d'assegurar-se d'adoptar aquestes mesures i informar a la Comissió una vegada ho facin. Per contra, en cas de no ser considerades justificades, l'EM corresponent haurà de retirar la mesura i informar també a la Comissió.

D'altra banda, quan de l'avaluació del SIA que presenta un risc es conclou que aquest compleix els requisits i obligacions del RIA, s'obren dues noves possibilitats. En primer lloc, que es consideri que, determinada la conformitat del SIA al RIA, aquest no presenta un risc addicional que ha de ser mitigat; en aquest cas, finalitza el procediment. En segon lloc, que l'AVM, després de consultar l'APDF, conclogui que tot i que un SIA d'alt risc compleixi amb el RIA, aquest presenta igualment un risc addicional[41] per la salut, seguretat, drets fonamentals o per altres aspectes de protecció de l'interès públic. En aquest segon supòsit, l'AVM demanarà a l'operador pertinent que adopti les mesures necessàries perquè aquest risc no es trobi present quan aquest SIA s'introdueixi al mercat de la UE o es posi en servei sense demora indeguda (art. 82.1 RIA).

Desglossat aquest procediment, sorgeixen certs dubtes interpretatius sobre el seu abast que escau esmentar.

En primer lloc, pel que fa a la participació de les APDF en el procediment d'adopció de mesures un cop han cooperat amb les AVM en l'avaluació dels SIA que presenten un risc. Si bé l'article 79.2 del RIA no explicita que la cooperació s'estengui a l'exigència d'adopció de mesures correctores als operadors, seria raonable que hi participessin en relació a aquells SIA que incompleixen el RIA per presentar un risc pels drets fonamentals. En aquest punt, a més, cal assenyalar que, quan un sistema d'IA presenti un risc per al dret fonamental a la protecció de dades o per a qualsevol dret o llibertat que es vegi afectat pel tractament de dades, les APD, en virtut de les seves competències, poden prendre mesures cautelars d'acord amb l'article 66 de l'RGPD. Així, més enllà de les mesures que les AVM puguin exigir prendre als operadors, les APD ja tenen poders executius per protegir el dret fonamental a la protecció de dades personals,[42] sense necessitat de recórrer a les potestats que el RIA li pugui atorgar en condició d'APDF; o d'haver de dependre d'una mesura executiva de l'AVM. Aquesta potestat atorgada a les APD té una certa semblança amb la prevista a l'article 79.7 del RIA per a les AVM.

En segon lloc, pel que fa a l'article 82.1 del RIA, sembla que el legislador ha volgut establir un mecanisme de salvaguarda per a les situacions en què, tot i que es compleixin les

[41] En aquest context s'utilitza el terme "risc addicional" per diferenciar-lo del risc que recull l'article 79.1 del RIA

[42] Preneu com a exemple la mesura cautelar adoptada per l'AEPD envers Tools for Humanity Corporation, per la qual exigia que cessés en la recollida i el tractament de les dades personals que s'estava efectuant a Espanya, en virtut del seu projecte World Coin. AEPD, *La Agencia ordena una medida cautelar que impide a Worldcoin seguir tratando datos personales en España.* 2024 [en línia] Disponible a: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-ordena-medida-cautelar-que-impide-a-worldcoin-seguir-tratando-datos-personales-en-espana

obligacions que estableix el RIA (perquè un SIA d'alt risc pugui ser conforme al reglament[43]), es detecti un risc per a la salut, la seguretat, els drets fonamentals o altres aspectes de protecció de l'interès públic, que hagi de ser mitigat. En aquest context, d'acord amb l'article 82.3 del RIA, quan els estats membres es trobin en una situació d'aquestes característiques també n'han d'informar la Comissió i aportar una sèrie de detalls relatius al SIA en qüestió. Doncs bé, aquesta obligació d'informar-la pot vincular-se amb l'atribució que té atorgada la Comissió per adoptar actes delegats, en virtut de l'article 97 del RIA, per modificar l'annex III, la llista de SIA prohibits i, també, ajustar les obligacions i requisits que ha de complir un SIA perquè el seu risc es circumscrigui als llindars de tolerància del dret de la UE. Així, aquesta notificació pot esdevenir una eina perquè, amb l'aprovació del Parlament Europeu, la Comissió pugui adaptar el RIA a aquestes situacions, a mesura que les AVM les vagin identificant.

També en relació amb l'article 82.1 del RIA, escau valorar si la consulta a l'APDF atorga una competència addicional que no s'emmarqui dins el deure d'informar i cooperar plenament amb l'APDF que té l'AVM quan el risc que presenti un SIA ho sigui pels drets fonamentals. En aquest sentit, de la lectura literal de l'article 82.1 del RIA s'infereix que la consulta a l'APDF és un requisit perquè l'AVM pugui demanar a l'operador interessat que adopti les mesures adequades quan de l'avaluació del SIA es constati: i) que és un SIA d'alt risc; ii) que és conforme als requisits i obligacions del RIA; i iii) que presenta un risc per la salut, seguretat, drets fonamentals o altres aspectes de protecció de l'interès públic. Així, sense efectuar aquesta consulta, l'AVM podria demanar a l'operador l'adopció de mesures correctores pels SIA que no siguin conformes al RIA, però no ho podria fer pels SIA que encaixin en el context de l'article 82.

En tercer lloc, pel que fa a la interrelació entre els diferents procediments de la secció 3 del capítol IX del RIA que s'han enunciat en aquest apartat, l'"Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)" evidencia que el legislador del RIA va concebre aquests procediments separats en l'articulat com un procediment únic. Així, el punt 54 de l'Annex[44] disposa, pel cas concret de les pràctiques prohibides, que el procediment que s'inicia a l'article 79 del RIA s'enllaça amb el de salvaguarda de la Unió regulat a l'article 81.

---

[43] Per exemple, la implantació, documentació i manteniment d'un sistema de gestió del risc (art. 9 RIA) i la realització d'una avaluació d'impacte en els drets fonamentals (art. 27 RIA), entre d'altres.

[44] "The procedure in the AI Act to deal with AI systems presenting a risk at national level is particularly relevant in the context of enforcing the prohibitions. Where there are cross-border implications beyond the territory of the market surveillance authority, the authority of the Member State concerned must inform the Commission and the market surveillance authorities of other Member States. All market surveillance authorities should follow a Union safeguard procedure with a decision taken by the Commission determining whether the AI system constitutes a prohibited practice. That procedure aims to ensure that the prohibitions are applied uniformly across all Member States, so as to provide legal certainty to both providers and deployers of AI systems. To ensure the uniform application of the AI Act, national market surveillance authorities should also strive for a harmonized application of the prohibitions for comparable cases that do not cross the Member State's territory by drawing inspiration from these Guidelines and cooperating within the AI Board."

En darrer lloc, l'article 80 del RIA, també inclòs a la tercera secció del capítol IX, regula el procediment aplicable als sistemes d'IA classificats pel proveïdor com no d'alt risc en aplicació de l'Annex III. En aquest cas, es regula un procediment per aquells supòsits en què l'AVM "tenga motivos suficientes" per considerar que un SIA no classificat com d'alt risc pel proveïdor, d'acord amb l'article 6.3 del RIA, sí que ho és. En el cas que es detecti aquesta situació, l'AVM demanarà al proveïdor que adopti les mesures necessàries perquè el SIA s'adapti als requisits i obligacions previstos al RIA pels SIA d'alt risc. En aquest punt, sorgeix el dubte de si aquest procediment podria afectar negativament a les competències de les APDF. En concret, en el cas que una AVM "tenga motivos suficientes" per sospitar que un proveïdor ha classificat un SIA com no d'alt risc i alhora aquest presenti un risc pels drets fonamentals, si es prioritzés el procediment regulat a l'article 80, en atenció a la seva especialitat, això suposaria l'exclusió de la participació de les APDF, que no es troba prevista en aquest darrer procediment.

En qualsevol cas, més enllà dels dubtes interpretatius que s'han esmentat, quan un SIA presenti un risc pels drets fonamentals, l'AVM n'informarà l'APDF pertinent i cooperarà plenament amb ella en l'avaluació del SIA corresponent.

4. Conclusions

Tatiana Bianca Vulpe i Daniel Duro Millan

Aquest treball s'ha elaborat amb la intenció de recollir i clarificar els principals reptes que les autoritats de protecció de dades (com l'APDCAT) hauran d'afrontar a causa de l'inici d'aplicabilitat del RIA: per la seva consideració com a APD, el nomenament com a APDF i la propera i probable designació com a AVM per a alguns sistemes d'IA.[45] A continuació, se'n presenten les principals conclusions.

Primera. Falta de concreció de qüestions referents a les funcions de les diferents autoritats

El RIA busca millorar el funcionament del mercat interior, però deixa moltes qüestions obertes respecte dels poders i les funcions de les diferents autoritats previstes a l'articulat, que sembla que no s'aclariran fins que cada estat membre ho reguli internament, amb el perill d'arribar a conclusions molt diverses. A més, encara que més endavant la Comissió aprovi directrius o recomanacions per omplir buits, aquests no són textos vinculants; per tant, pot succeir que cada estat membre legisli abans o que aquesta legislació presenti contradiccions. Ens trobem, per tant, en un escenari força incert i inconcret, que dificulta la seguretat jurídica en l'àmbit europeu.

Algunes de les qüestions que demanen més concreció són la interrelació entre agents/organismes (notificacions, informes, sol·licituds...), així com els termes *cooperació* i *col·laboració*; també, els conceptes jurídics indeterminats de l'article 57.10 del RIA, que estableix que les autoritats nacionals de protecció de dades han d'estar lligades al funcionament de l'espai controlat de proves per a la IA i involucrades en la supervisió d'aquests aspectes. Genera força dubtes com aquests conceptes es concretaran en accions/actuacions específiques, però considerem que el paper ha de ser actiu atès que els sistemes d'IA funcionen gràcies a dades que, en molts casos, són personals.

En contraposició, encara que provoquin incertesa o inseguretat jurídica, les qüestions que el RIA no concreta també reflecteixen la naturalesa dinàmica i en constant evolució del camp regulat. No s'ha d'oblidar que ens trobem en les primeres etapes de l'aplicació del reglament, el qual incorpora diferents terminis d'aplicabilitat. El RIA funciona actualment com un anunci del que ha de venir, atorgant temps per preparar-se adequadament per a les futures adaptacions i donant flexibilitat a la Comissió per concretar qüestions a mida que es donen a conèixer nous avanços tecnològics. Caldrà veure si aquesta flexibilitat és positiva o negativa.

[45] Tenint en compte el contingut de l'article 74.8 del RIA, així com l'Avantprojecte de llei per al bon ús i la governança de la intel·ligència artificial, presentat al març de 2025.

Segona. El RIA té molt present el paper de les autoritats de protecció de dades en relació amb els sistemes d'identificació biomètrica remota

El RIA estableix disposicions específiques que involucren les autoritats de protecció de dades en relació amb els sistemes d'identificació biomètrica remota, tant en temps real com en diferit. Si bé no necessàriament atorga nous poders explícits a aquestes autoritats, més enllà dels ja establerts a l'RGPD, sí que els confereix un paper significatiu en la supervisió de l'aplicació del RIA en aquest àmbit (rebre notificacions, accedir a documentació d'expedients policials sota sol·licitud i elaborar i rebre informes).

Tot i que el RIA opera sense perjudici de l'RGPD (amb excepcions tal com s'estableix a l'article 2.7 del RIA), el marc establert sembla reforçar la capacitat de les autoritats de protecció de dades per supervisar el tractament de dades personals en aquest context i aplicar, si escau, sancions per incompliment de l'RGPD. És a dir, l'articulat comporta que les autoritats de protecció de dades puguin estar assabentades dels usos que es facin de sistemes d'identificació biomètrica remota, sense preveure una actuació més enllà de tenir-ne coneixement (possiblement, perquè el legislador europeu considera que no cal, tenint en compte les competències que ja tenen gràcies a l'RGPD). Per tant, el RIA consolida el paper supervisor de les autoritats de protecció de dades en l'àmbit específic de la identificació biomètrica remota i les dota de mecanismes per ampliar l'abast de coneixement.

Tercera. Les APDF tenen un impacte significatiu en la categorització dels SIA

El RIA fa referències constants a la protecció dels drets fonamentals ("garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta").[46] En aquest sentit, incorpora les APDF al procés de supervisió del RIA, per exemple mitjançant:

(i) La sol·licitud d'accés a documentació dels SIA enumerats a l'annex III i la posterior sol·licitud motivada a les AVM, per organitzar proves sobre aquests SIA, si amb la sol·licitud de documentació no n'hi ha prou per determinar si incompleix el RIA.

(ii) La recepció d'informació provinent de les AVM, quan es produeixi un incident greu per incompliment de les obligacions de la UE en matèria de DF.

(iii) La recepció d'informació provinent de les AVM relativa a qualsevol SIA que pugui suposar un risc per als DF, per avaluar-los conjuntament i, posteriorment, categoritzar-los en alguna de les quatre categories que preveu el RIA (segons el risc) perquè, finalment, les AVM exigeixin als operadors que adoptin les mesures adients per assegurar la conformitat amb el RIA.

Aquestes competències són més àmplies en els casos en què addicionalment les APDF tenen atribuïts poders en virtut d'una altra norma de la UE. En el cas de les APD designades APDF, el RIA és explícit a l'hora d'afirmar que no afecta l'RGPD. Per tant, els poders que

[46] Considerants 1 i 176 i article 1 del RIA.

l'RGPD atorga a les APD per garantir els drets i llibertats fonamentals de les persones, pel que fa al tractament de les seves dades personals, es mantenen intactes. En aquest context, si bé el RIA circumscriu la documentació a què poden tenir accés les APDF als SIA d'alt risc de l'annex III (art. 77 RIA), aquesta limitació no afecta les APD, que hi poden accedir per les competències atorgades per l'RGPD. Addicionalment, quan es notifiqui o informi a l'APDF un incident greu relatiu al dret fonamental a la protecció de dades, o bé que un SIA pugui suposar un risc per a aquest dret, les APD poden adoptar mesures cautelars correctores en virtut de l'RPGD, tot i que com a APDF no tinguin atorgada aquesta potestat.

Per tant, en relació amb aquestes competències, l'RGPD atorga més facultats a les APD per protegir el dret fonamental a la protecció de dades que el mateix RIA. Tanmateix, hi ha altres competències que el RIA atorga a les APDF que sí que suposen acréixer les eines amb què les APD poden protegir les dades personals:

- En primer lloc, si bé les APD poden 'participar' en els espais controlats de proves pel simple fet de ser-ho (art. 57.10 RIA), les APDF poden sol·licitar motivadament a les AVM que organitzin proves de SIA d'alt risc de l'annex III, quan amb la sol·licitud de documentació les APDF no puguin determinar si el SIA analitzat incompleix el RIA (art. 77.3 RIA).

- En segon lloc, les AVM han de notificar a les APDF els incidents greus en SIA que puguin suposar riscos per als DF (art. 73.7 RIA). Com es desenvolupa a l'apartat 3.4, es valora la possibilitat que, per la diferent naturalesa de notificació que suposa una NVS i la notificació d'un incident greu, en algunes circumstàncies, a la pràctica, aquesta darrera pugui esdevenir l'únic mecanisme a l'abast de les APD per assabentar-se d'una violació de seguretat de dades personals en el context dels SIA.

- En tercer lloc, les AVM han d'informar les APDF de qualsevol SIA que presenti un risc per als DF, perquè en cooperació l'avaluïn i, en conseqüència, es categoritzi el SIA segons el seu risc (prohibit, d'alt risc, amb obligacions de transparència/risc limitat, o bé de risc mínim o nul). Això resulta especialment rellevant, ja que el RIA imposa obligacions d'acord amb la categorització dels SIA.

Quarta. L'adaptació de les autoritats de protecció de dades requereix una preparació rigorosa i recursos adequats per afrontar els nous reptes amb eficàcia

Queda clar que les autoritats de protecció de dades necessitaran una preparació prèvia exhaustiva per respondre satisfactòriament a totes les noves responsabilitats. Per abordar aquests reptes de manera efectiva, és essencial que disposin dels recursos humans i financers adequats. L'augment de les responsabilitats derivades del RIA, el nomenament com a APDF i la probable designació com a AVM requereixen una dotació de personal qualificat i especialitzat en tecnologies emergents i en la regulació de la intel·ligència artificial.

És important subratllar que, tot i que aquest treball no ha analitzat l'increment de les denúncies que han rebut les autoritats de protecció de dades en aplicació de l'RGPD i l'LOPDGDD, aquest fenomen és un indicador addicional de la creixent demanda i consciència ciutadana respecte del dret a la protecció de dades personals. Per tant, és

essencial que les autoritats de protecció de dades no només estiguin preparades per respondre adequadament a les reclamacions actuals, sinó que també puguin anticipar i gestionar proactivament les noves que es puguin presentar, com succeeix en l'àmbit de la IA.

5. Bibliografia

ABBOU, Daniel; et al. Open letter to the representatives of the European Commission, the European Council and the European Parliament. Artificial Intelligence: Europe's chance to rejoin the technological avant-garde. 2023. Disponible a: https://uploads-ssl.webflow.com/6034e2e35a869ae02e67f55f/649eadd757bee709f4fe1f49_Brandbrief%20en-US%20(2).pdf

ACCIÓ Generalitat de Catalunya. La intel·ligència artificial a Catalunya. Informe tecnològic. [en línia]. Abril de 2024. [consulta: 17 de octubre de 2024]. https://www.accio.gencat.cat/web/.content/bancconeixement/documents/informes-tecnologics/ACCIO-ia-catalunya-informe-complet-2024.pdf#:~:text=Catalunya%20va%20assolir%20les%202.102%20startups%20startups%20el

Agència Espanyola de Protecció de Dades (AEPD). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción,* 2020. Disponible a: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf

Agència Espanyola de Protecció de Dades. *Construir correctamente el futuro. La inteligencia artificial y los derechos fundamentales. Resumen* [en línia]. Disponible a: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_es.pdf

Agència Espanyola de Protecció de Dades. *Requisitos para Auditorías de Tratamientos que incluyan IA.* 2021.

Agència Espanyola de Protecció de Dades. *Tratamientos que incluyen Inteligencia Artificial (IA). Mapa de referencia*. 2022.

Agència Espanyola de Protecció de Dades. *La Agencia ordena una medida cautelar que impide a Worldcoin seguir tratando datos personales en España.* 2024. Disponible a: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-ordena-medida-cautelar-que-impide-a-worldcoin-seguir-tratando-datos-personales-en-espana

Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

ARELLANO TOLEDO, Wilma. Artículo 57. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 594-603. ISBN 978-84-18662-88-1.

ARELLANO TOLEDO, Wilma. Artículo 58. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 603-608. ISBN 978-84-18662-88-1.

Autoritat Catalana de Protecció de Dades (APDCAT). *Intel·ligència artificial. Decisions automatitzades a Catalunya.* 2020. Disponible a: https://apdcat.gencat.cat/web/.content/03-documentacio/intelligencia_artificial/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf

Autoritat Catalana de Protecció de Dades (APDCAT). Model per a l'AIDF: guia i casos d'ús Metodologia aplicada de l'avaluació d'impacte sobre els drets fonamentals en el disseny i desenvolupament de la IA. 2025. Disponible a: https://apdcat.gencat.cat/ca/documentacio/intelligencia_artificial/

Autoritat Catalana de Protecció de dades (APDCAT). La privacitat des del disseny i la privacitat per defecte. Guia per a desenvolupadors. Juny 2024. Disponible a: https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD.pdf

BARRIO ANDRÉS, Moisés. Artículo 1. En: Barrio Andrés, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 135-147. ISBN 978-84-18662-88-1.

BARRIO ANDRÉS, Moisés. Capítulo I. Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial. En: Jiménez Serranía, Vanessa, et al. El *Reglamento Europeo de Inteligencia Artificial.* Valencia: Tirant lo Blanch, 2024. ISBN13 9788410713048.

BELANO GARÍN, Beatriz. Artículo 82. En: Barrio Andrés, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 750-752. ISBN 978-84-18662-88-1.

Consell d'Europa. *Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (huderia methodology)* 2024 [consulta: 12 de desembre de 2024] Disponible a: https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f

EAPC. Jornada sobre intel·ligència artificial i la protecció de dades personals (22/11/2024). [Vídeo en línia]. 2024 [consulta: 03 de desembre de 2024]. Disponible a: https://www.youtube.com/watch?v=wd6KauY0g8s&t=312s

CEPD. Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial. [en línia.] Juliol 2024. [consulta: 27 de febrer de 2024]. Disponible a: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_es

EDBP. *Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR.* 2024 [consulta: 27 de febrer de 2024]. Disponible a: https://www.edpb.europa.eu/system/files/2024-02/edpb_opinion_202404_mainestablishment_en.pdf#:~:text=The%20French%20Supervisory%20Authority%20requested%20the%20European%20Data,mechanism%2C%20in%20particular%20regarding%20the%20notion%20of%20controll

Agència dels Drets Fonamentals de la Unió Europea (FRA). *Informe sobre los derechos fundamentales*. 2021. [en línia] Disponible a: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-fundamental-rights-report-2021-opinions_es.pdf

FERNÁNDEZ HERNÁNDEZ, Carlos. Artículo 5. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 180-205. ISBN 978-84-18662-88-1.

GAMERO CASADO, Eduardo. Artículo 99. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 837-844. ISBN 978-84-18662-88-1.

HERNÁNDEZ LÓPEZ, José Miguel. R*eglamento de Inteligencia Artificial: Incluye introducción, notas, cronología, webgrafía, bibliografía e índice analítico* [online]. Barcelona, España: J. M. Bosch Editor, 2024. ISBN 9788410044063.

KARATHANASIS, Theodoros. *AI incident notification in the EU AI Act: How does it work and is it Effective?* [en línia] Disponible a: https://ai-regulation.com/ai-act-incident-notification/

KEBER, Tobias, et al. Discussion paper: Legal basis for data protection in the use of artificial intelligence. Stuttgart: The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg, 2024.

MIGUEZ MACHO, Luis y TORRES CARLOS, Marcos. Capítulo II. Sistemas de IA prohibidos y sistemas de IA de alto riesgo. En: JIMÉNEZ SERRANÍA, Vanessa, et al. El Reglamento Europeo de Inteligencia Artificial. Valencia: Tirant lo Blanch, 2024. ISBN13 9788410713048.

MUÑOZ GARCÍA, Carmen. Artículo 53. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 548-552. ISBN 978-84-18662-88-1.

MUÑOZ GARCÍA, Carmen. Capítulo III. Modelos de IA de uso general y sistemas de IA de riesgo limitado y mínimo. En: JIMÉNEZ SERRANÍA, Vanessa, et al. *El Reglamento Europeo de Inteligencia Artificial.* Valencia: Tirant lo Blanch, 2024. ISBN13 9788410713048.

MUÑOZ VELA, José Manuel. Anexo III. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 906-933. ISBN 978-84-18662-88-1.

PADÍN VIDAL, Alejandro. Artículo 83. En BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 753-756. ISBN 978-84-18662-88-1.

PERRIGO, Billy. Exclusive: OpenAI Lobbied the E.U. to Water Down AI Regulation. En: *Time Magazine.* [en línia]. 20 de juny de 2023 [Consulta: 17 de desembre de 2024]. Disponible a: https://time.com/6288245/openai-eu-lobbying-ai-act/

PRESNO LINERA, Miguel Ángel; MEUWESE, Anne. La regulación de la inteligencia artificial en Europa. Teoría y Realidad Constitucional. 2024, no. 54, s. 131-161. ISSN 1139-5583.

QUADRA-SALCEDO, Tomás. Estudio Preliminar: el Reglamento Europeo de Inteligencia Artificial y su regulación en condiciones de permanente adaptación a los riesgos y a la evolución de los modelos y sistemas de IA de uso general. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 23-47. ISBN 978-84-18662-88-1.

URIOS APARISI, Xavier. Què passa amb les dades biomètriques? Són dades especialment protegides sempre? [en línia]. EAPC - Gestió de la informació: transparència i protecció de dades. 2024 [consulta: 09 de desembre de 2024]. Disponible a: https://formacioooberta.eapc.gencat.cat/espaistematics/gestio-dades/que-passa-amb-les-dades-biometriques-son-dades-especialment-protegides-sempre.html

Annex I - Identificació biomètrica remota en temps real i en diferit

Tatiana Bianca Vulpe

Aquest annex té com a objectiu clarificar i diferenciar els sistemes d'identificació biomètrica remota en temps real i en diferit. Per assolir-ho, s'ofereix un resum de diverses consideracions extretes de l'Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) (d'ara endavant, directrius).

L'article 5.1.*h* del RIA prohibeix l'ús de sistemes d'identificació biomètrica remota en temps real en espais d'accés públic, amb finalitats de garantia del compliment del Dret,[47] excepte i en la mesura que aquest ús sigui estrictament necessari per assolir un o diversos dels objectius següents:

- La recerca selectiva de víctimes concretes de segrest, tràfic d'éssers humans o explotació sexual d'éssers humans, així com la recerca de persones desaparegudes.[48]
- La prevenció d'una amenaça específica, important[49] i imminent[50] per a la vida o la seguretat física de les persones físiques,[51] o d'una amenaça real i actual o real i previsible d'un atemptat terrorista.[52]
- La localització o identificació d'una persona sospitosa d'haver comès un delicte, amb la finalitat de dur a terme una investigació o un procediment penal o d'executar una

[47] Sense perjudici de l'article 9 del Reglament (UE) 2016/679 per al tractament de dades biomètriques amb finalitats diferents de les finalitats policials i judicials.

[48] Tal com estipula la Comissió Europa a les seves directrius, en alguns estats membres la cerca d'una persona desapareguda es pot dur a terme en el marc d'un procediment administratiu i no amb finalitats de garantia del compliment del Dret. Per exemple, quan una persona vulnerable desapareix, però no hi ha sospita de cap delicte ni estem davant d'una altra finalitat relacionada amb la garantia del compliment del Dret, l'ús de sistemes d'identificació biomètrica en temps real per trobar aquesta persona no s'integraria com a pràctica prohibida, i es regiria per les normes corresponents establertes per l'RGPD.

[49] Una amenaça important per a la seguretat física estaria relacionada amb lesions corporals greus.

[50] Una amenaça imminent a la vida o a la seguretat física és una amenaça que pot ocórrer en qualsevol moment i requereix prendre mesures immediates.

[51] Un exemple d'amenaça seria la interrupció greu i la destrucció d'infraestructures crítiques (per exemple, una central elèctrica, un subministrament d'aigua o un hospital).

[52] El nivell d'amenaça terrorista es defineix en l'àmbit nacional i varia d'un estat membre a un altre. No obstant això, el concepte d'amenaça real i actual o real i previsible, tal com s'utilitza a l'article 5.1.*h.ii*, és una noció autònoma del dret de la Unió. Per tant, en principi s'ha d'avaluar independentment de les definicions nacionals. L'amenaça no es refereix al terrorisme en general, sinó específicament a l'amenaça d'un atac terrorista.

sanció penal per algun dels delictes esmentats a l'annex II,[53] que a l'estat membre corresponent es castigui amb una pena o una mesura de seguretat privativa de llibertat amb una durada màxima de quatre anys.[54]

Per tant, a més de considerar les tres excepcions, cal complir diverses condicions acumulatives perquè s'apliqui la prohibició de l'article 5.1.*h* del RIA: (i) el sistema d'IA ha de ser un sistema d'identificació biomètrica; (ii) remota; (iii) en relació amb l'ús d'aquest sistema; (iv) en temps real; (v) en espais d'accés públic; i (vi) amb finalitats de garantia del compliment del Dret.

Sistema d'identificació biomètrica

El concepte de dades biomètriques s'ha d'interpretar en relació amb l'article 4.14 de l'RGPD i l'article 3.13 de la Directiva (UE) 2018/1725. En aquest sentit, les dades biomètriques són "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (art. 4.14 RGPD).

Les dades biomètriques poden permetre l'autenticació, la identificació, la categorització i el reconeixement de les emocions de les persones físiques; el referit a la identificació està prohibit.

La identificació biomètrica es defineix com "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico[55] para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos" (art. 3.35 RIA). Per la seva banda, un sistema d'identificació biomètrica remota es defineix de manera funcional com un sistema d'IA "destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia" (art. 3.17 RIA), amb independència de la tecnologia, els processos o els tipus de dades biomètriques concretes que s'utilitzin.

---

[53] Terrorisme, tràfic d'éssers humans, explotació sexual de menors i pornografia infantil, tràfic il·lícit d'estupefaents o substàncies psicotròpiques, tràfic il·lícit d'armes, municions o explosius, assassinat, lesions corporals greus, tràfic il·lícit d'òrgans o teixits humans, tràfic il·lícit de materials nuclears o radioactius, segrest, restricció il·legal o presa d'ostatges, delictes de la jurisdicció de la Cort Penal Internacional, confiscació il·legal d'aeronaus o vaixells, violació, delictes ambientals, robatori organitzat o a mà armada, sabotatge i participació en una organització criminal implicada en un o més dels delictes esmentats anteriorment.

[54] La policia no pot desplegar tecnologies de reconeixement facial en temps real de manera àmplia i no específica, és a dir, amb l'esperança de trobar delinqüents buscats i treure'ls dels carrers. En contraposició, si la policia rep una descripció física amb una fotografia d'un individu buscat, subjecte a una ordre de detenció europea per tràfic de drogues, i hi ha motius per creure que serà en un lloc concret, com ara un festival, el desplegament de tecnologies de reconeixement facial en temps real per identificar l'individu pot estar cobert per l'article 5.1.*h.iii* del RIA.

[55] Com per exemple la cara, el moviment ocular, la forma del cos, la veu, l'entonació, la manera de caminar, la postura, la freqüència cardíaca, la pressió arterial, l'olor o les característiques de les pulsacions de tecla (considerant 15 RIA).

Per tant, s'han de considerar diferents i en queden exclosos els sistemes d'IA destinats a la verificació biomètrica o l'autenticació, que tenen com a únic propòsit confirmar que una persona física concreta és la persona que diu ser; també, els destinats a confirmar la identitat d'una persona física amb la finalitat exclusiva que per exemple tingui accés a un servei, desbloquegi un dispositiu o tingui accés de seguretat a un local. Aquesta exclusió es justifica pel fet que probablement aquests sistemes tenen menys repercussió en els drets fonamentals de les persones físiques (considerant 17).

Remota

El concepte de *remota* també s'ha de clarificar i posar-lo en relació o contradicció amb el concepte de *participació activa*. Segons l'article 3.41 del RIA, el concepte de remota implica la capacitat dels sistemes biomètrics per identificar persones sense la seva participació activa, normalment a distància, comparant les dades biomètriques d'una persona amb les dades biomètriques contingudes en una base de dades de referència. Per a la participació activa, no n'hi ha prou que les persones estiguin informades de la presència de càmeres, sinó que han de posar-se activament i conscientment davant d'una càmera instal·lada, de manera que fomenti la participació activa. Per exemplificar el concepte, podríem utilitzar els següents supòsits pràctics extrets de les directrius:

- Els sistemes d'identificació biomètrica remota en temps real que s'utilitzen en càmeres instal·lades a les parets o al sostre de les estacions de metro, amb finalitats de vigilància. Aquest sistema compleix la condició de *remota*.

- Els sistemes que s'utilitzen per donar accés a l'estació de metro, com ara els bitllets biomètrics de metro, en què les persones hi participen activament i s'acosten conscientment al sensor biomètric per accedir-hi. Aquests sistemes no compleixen aquesta condició.

- En el cas de les càmeres corporals capaces d'identificació biomètrica remota en temps real utilitzades per agents individuals de les forces de l'ordre, la filmació no dirigida, per exemple, durant una manifestació amb centenars de participants. En aquest cas, es considera que compleix la condició de *remota*.

Utilització/ús (*the use*); cada ús (*each use*)

En primer lloc, convé matisar que a la versió castellana del RIA, per referir-se al *use* de la versió anglesa original s'utilitza indistintament *uso* i *utilización*.

També es rellevant remarcar que, en el cas dels sistemes d'identificació biomètrica remota en temps real, la prohibició es limita exclusivament a la seva utilització, a diferència dels altres supòsits de pràctiques prohibides de l'article 5 del RIA on, en general, se'n prohibeix la introducció, la posada en servei i l'ús.

El concepte d'*ús* no té una definició concreta a l'article 3 del RIA ni està explícitament definit en tot el text normatiu, a diferència de la introducció al mercat (art. 3.9 RIA), la comercialització (art. 3.10 RIA) i la posada en servei (art. 3.11 RIA). Tot i això, s'ha d'entendre de manera àmplia per cobrir l'ús o la implementació del sistema en qualsevol moment del seu cicle de vida, després d'haver estat comercialitzat o posat en servei tal com

s'explica a directrius de la Comissió. Per tant, la restricció de l'article 5.1.*h* del RIA no s'aplica a la introducció al mercat ni a la posada en servei, que continuen essent activitats permeses sota el règim dels sistemes d'IA d'alt risc regulat a l'article 6.2 i l'annex III, lletra *a*, del RIA. Això significa que aquests sistemes es poden desenvolupar, vendre i desplegar, però el seu ús efectiu està subjecte a una regulació molt més estricta.

D'altra banda, convé matisar que, d'acord amb l'article 5.3 del RIA, *cada uso* (*each use*, en la versió anglesa) d'un sistema d'identificació biomètrica remota en temps real requereix una autorització prèvia. Això podria implicar que la simple instal·lació del sistema no necessita cap aprovació específica segons el RIA, però cada vegada que es vulgui utilitzar en un cas concret cal obtenir una autorització individual d'una autoritat judicial o administrativa independent, a més de de la resta de consideracions necessàries, com ara elaborar una avaluació de l'impacte en els drets fonamentals (FRIA).[56] Aquest matís és essencial per garantir que la tecnologia no s'utilitzi de manera indiscriminada i que cada aplicació concreta estigui justificada i supervisada, de manera que es protegeixin els drets fonamentals.

Alguns exemples que permeten comprendre la distinció, segons les directrius, són:

- Instal·lació del sistema: la policia instal·la càmeres biomètriques de videovigilància a l'estació principal de tren d'una ciutat. Segons el RIA no es requereix cap autorització prèvia per a la instal·lació, però el sistema ha de complir els requisits dels sistemes d'alt risc.[57] Abans del primer ús, s'ha de fer una avaluació de l'impacte en els drets fonamentals.

- Ús específic del sistema: la policia té indicis concrets que un terrorista arribarà en tren a la ciutat i decideix utilitzar el sistema d'identificació biomètrica remota en temps real, per identificar-lo en temps real. Aquest ús requereix l'autorització prèvia d'una autoritat judicial o administrativa independent.

Així, el RIA estableix una distinció clau entre la presència del sistema i el seu ús concret, per garantir que cada aplicació individual d'aquestes tecnologies en contextos sensibles se sotmeti a un control rigorós per protegir els drets fonamentals i evitar abusos.

En temps real

Quan el RIA esmenta *en temps real*, vol dir que la recollida de les dades biomètriques, la comparació i la identificació es produeixen "de manera instantánea, casi instantánea o, en cualquier caso, sin una importante demora" (considerant 17 RIA). En aquest sentit, no hi ha d'haver la possibilitat que, generant demores mínimes, es puguin eludir les normes previstes al RIA en relació amb l'ús en temps real dels sistemes d'IA. En termes generals, un retard és

[56] Cal recordar que per dur a terme una AIPDF tenim a la mà la metodologia presentada per l'APDCAT per a l'avaluació d'impacte en els drets fonamentals en matèria d'intel·ligència artificial (AIDF), aplicada a casos concrets a Europa, disponible a: https://www.dpdenxarxa.cat/pluginfile.php/2468/mod_folder/content/0/FRIA_ca.pdf_.pdf

[57] Sens perjudici que l'estat membre estableixi una cosa diferent.

significatiu almenys quan és probable que la persona hagi abandonat el lloc on es van prendre les dades biomètriques. Quan el retard és significatiu entenem que la identificació es fa en diferit. Uns exemples extrets de les directrius per comprendre la diferència serien els següents:

- Identificació biomètrica remota en temps real: un sistema d'IA examina al moment tots els assistents a un concert.

- Identificació biomètrica remota en diferit: un sistema filma tots els assistents que entren a un concert. Es produeix un incident i, després del concert, s'empra el sistema per identificar el delinqüent.

La distinció no sempre serà del tot clara i caldrà una anàlisi cas per cas. Per exemple, quan una autoritat policial fotografia una persona amb un dispositiu mòbil i l'envia a una base de dades per a una cerca immediata, depenent de les circumstàncies això pot caure sota la prohibició de l'article 5.1.*h* del RIA, segons es determini si el retard és significatiu o no.

En definitiva, els sistemes d'identificació biomètrica en temps real permeten analitzar i comparar immediatament dades captades per càmeres o altres dispositius similars. Per exemple, quan una càmera situada en un aeroport escaneja els rostres de les persones que hi passen i, instantàniament, els compara amb una base de dades de persones buscades per la policia, estem davant d'un sistema en temps real. Si hi ha una coincidència, el sistema genera una alerta immediata perquè els agents puguin actuar a l'instant. En aquest cas, el processament de la informació és simultani a la captació, cosa que possibilita una resposta immediata.

En canvi, els sistemes en diferit funcionen amb una important demora entre la captació i el processament de les dades biomètriques. Això passa, per exemple, quan la policia investiga un delicte i analitza enregistraments de vídeo d'una càmera de seguretat, per identificar un sospitós. Les imatges ja han estat captades prèviament i la comparació es fa posteriorment, mitjançant un sistema d'IA. En aquest cas, no hi ha un processament immediat, sinó que es treballa amb material ja enregistrat, com imatges d'arxiu captades per càmeres de videovigilància o dispositius privats.

Així, la diferència fonamental entre aquests dos tipus de sistemes rau en el moment en què es produeix l'anàlisi i la comparació. Mentre que en els sistemes en temps real la identificació es fa en directe o quasi en directe, en els sistemes en diferit aquesta anàlisi és posterior, utilitzant informació ja existent.

Espais d'accés públic

Tal com es constata a les directrius, pel que fa al concepte d'espai públic és important tenir present que alguns espais poden tenir una doble funció. Per exemple, un aeroport es considera generalment un espai d'accés públic pel que fa a les seves zones comunes, però l'àrea dedicada al control fronterer (on hi ha els funcionaris de duanes i es fan els passaports o els controls d'identitat) queda exclosa de l'àmbit de la prohibició. Com s'aclareix al considerant 19 del RIA, l'avaluació de si un espai és accessible al públic s'ha de fer amb una anàlisi cas per cas.

Finalitats de garantia del compliment del Dret

També cal considerar que l'article 3.46 del RIA descriu la garantia del compliment del Dret com "las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas."[58] Per tant, quan es parla de garantia del compliment del Dret s'ha d'entendre realitzada per les autoritats garants de compliment directament, o en el seu nom.

Segons l'article 3.45 del RIA, les autoritats garants del compliment del Dret són "toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, o cualquier otro organismo 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 delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas."[59]

Per tant, convé fer èmfasi i entendre què implica l'actuació *en nom de les autoritats garants*. Alguns exemples de delegacions, extrets de les directrius, serien els següents:

- Empreses de transport públic requerides per les autoritats policials per garantir la seguretat a les xarxes de transport públic, sota les seves instruccions i supervisió.

- Federacions esportives requerides per les autoritats policials per actuar sota les seves instruccions i supervisió, per proporcionar seguretat en esdeveniments esportius.

- Entitats financeres que són requerides per les autoritats policials per dur a terme certes accions per prevenir la execució de determinats delictes en casos específics, sota les instruccions i supervisió de les autoritats policials.

Aquestes activitats entren dins de la definició *amb finalitats de garantia del compliment del Dret*, ja que aquestes entitats actuen *en nom de les autoritats policials*. En contraposició, si actuessin en nom propi a l'hora de detectar i combatre delictes (com ara el frau o el blanqueig de capitals), no es consideraria que entren dins de la prohibició establerta a l'article 5.1.*h* del RIA.

---

[58] Algunes activitats de les autoritats policials estan excloses de l'àmbit d'aplicació, com ara quan realitzen tasques administratives (com ara recursos humans); aquestes activitats es duen a terme fora del marc d'aplicació del Reglament. Estan sota l'RGPD. Vegeu el considerant 19 de l'RGPD.

[59] A l'Estat espanyol, és important posar en relació aquestes definicions amb la Llei orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a fins de prevenció, detecció, investigació i enjudiciament de infraccions penals i de execució de sancions penals, ja que en molts casos una autoritat competent segons la Llei 7/2021 també serà una autoritat garant del compliment del Dret segons el RIA.

Finalment, un altre aspecte que cal tenir en compte és l'exclusió de l'àmbit d'aplicació del RIA per a determinades matèries, com la seguretat nacional, la defensa i les finalitats militars, d'acord amb el que estableix l'article 2 del RIA. Aquesta exclusió no és absoluta, ja que si un sistema d'IA inicialment destinat a finalitats militars, de defensa o de seguretat nacional s'utilitza posteriorment o simultàniament (temporalment o permanentment) amb altres finalitats (com per exemple civils o humanitàries), passa a estar dins de l'àmbit d'aplicació del RIA i, per tant, subjecte als seus requisits normatius. Per exemple, si una agència de seguretat nacional utilitza un sistema d'identificació biomètrica remota en temps real, amb finalitats de seguretat nacional, aquest ús quedaria exclòs del RIA. Ara bé, si el mateix sistema es destinés a localitzar persones desaparegudes, llavors sí que estaríem davant un supòsit regulat pel Reglament.

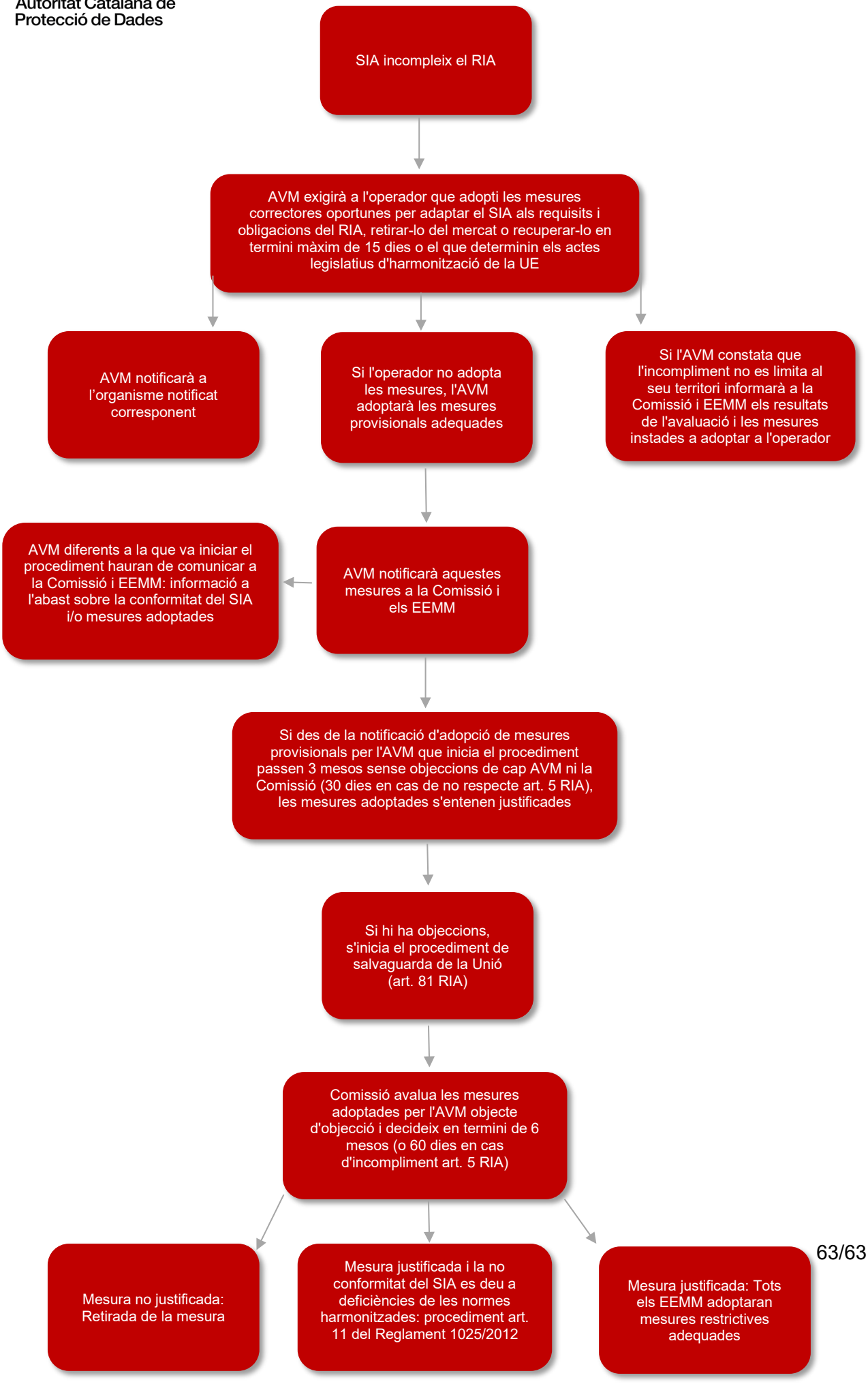
Aquesta diferenciació és especialment rellevant en relació amb les finalitats de garantia del compliment del Dret, tal com defineix l'article 3.46 del RIA. Aquest criteri és essencial per determinar quan un ús concret d'un sistema d'IA està exclòs, sotmès a la prohibició de l'article 5.1.*h* del RIA o quan es considera un ús permès, però classificat com a sistema d'alt risc. Per entendre aquesta diferència, es poden tenir presents els següents exemples extrets de les directrius:

- Una organització privada dedicada a la recerca de nens desapareguts decideix utilitzar un sistema d'identificació biomètrica remota en temps real. No té cap mandat per exercir l'autoritat i els poders públics, ni per prevenir delictes o tasques de prevenció d'amenaces a la seguretat pública. Aquest ús no entra dins de la prohibició establerta a l'article 5.1.*h* del RIA. No obstant això, aquest sistema es qualificarà d'alt risc (punt 1.*a* de l'annex III) i pot caldre fer una AIPD (art. 35 RGPD) i, si s'escau, una consulta prèvia a l'autoritat de protecció de dades, d'acord amb l'article 36 de l'RGPD.

- En canvi, si les autoritats policials sol·licitessin a la mateixa organització que actués en el seu nom per a la recerca de nens desapareguts, en un context policial i sota la supervisió i les instruccions de les autoritats policials competents, caldria una autorització prèvia d'acord amb l'article 5.3 del RIA.

Annex II – Procediment aplicable als sistemes d'IA que presenten un risc

Daniel Duro Millan


SIA incompleix el RIA
AVM exigirà a l'operador que adopti les mesures correctores oportunes per adaptar el SIA als requisits i obligacions del RIA, retirar-lo del mercat o recuperar-lo en termini màxim de 15 dies o el que determinin els actes legislatius d'harmonització de la UE
AVM notificarà a l'organisme notificat corresponent
Si l'operador no adopta les mesures, l'AVM adoptarà les mesures provisionals adequades
Si l'AVM constata que l'incompliment no es limita al seu territori informarà a la Comissió i EEMM els resultats de l'avaluació i les mesures instades a adoptar a l'operador
AVM diferents a la que va iniciar el procediment hauran de comunicar a la Comissió i EEMM: informació a l'abast sobre la conformitat del SIA i/o mesures adoptades
AVM notificarà aquestes mesures a la Comissió i els EEMM
Si des de la notificació d'adopció de mesures provisionals per l'AVM que inicia el procediment passen 3 mesos sense objeccions de cap AVM ni la Comissió (30 dies en cas de no respecte art. 5 RIA), les mesures adoptades s'entenen justificades
Si hi ha objeccions, s'inicia el procediment de salvaguarda de la Unió (art. 81 RIA)
Comissió avalua les mesures adoptades per l'AVM objecte d'objecció i decideix en termini de 6 mesos (o 60 dies en cas d'incompliment art. 5 RIA)
Mesura no justificada: Retirada de la mesura
Mesura justificada i la no conformitat del SIA es deu a deficiències de les normes harmonitzades: procediment art. 11 del Reglament 1025/2012
Mesura justificada: Tots els EEMM adoptaran mesures restrictives adequades