

DIPUTACIÓ DE
VALÈNCIA



Protecció de Dades i Seguretat de la Informació



Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la
Informació de la Diputació Provincial de València

Butlletí N.º 36 | Juny 2023

**SISTEMES D'INTEL·LIGÈNCIA ARTIFICIAL (I.A.) I PROTECCIÓ DE
DADES PERSONALS**



Í N D E X



SISTEMES D'INTEL·LIGÈNCIA ARTIFICIAL (IA) I PROTECCIÓ DE DADES PERSONALS

	Pàgina
Introducció	2
Sistema vs. Tractament IA	3
Principi d'exactitud en els tractaments IA	6
Intel·ligència Artificial i les decisions automatitzades	8
Protecció de dades i la dimensió ètica	10
Notices i material complementari	12



Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpto. de Protecció de Dades i
Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre
Butlletí informatiu accedeix al
següent [enllaç](#)



INTRODUCCIÓ

Actualment la protecció de les dades personals es veu desafiada pel ràpid desenvolupament i el veloç desplegament de la Intel·ligència Artificial (d'ara en avant, "IA"), perquè la seua utilització implica necessàriament el tractament de dades massives, dins dels quals s'inclouen diferents categories de dades personals.

La majoria de les aplicacions de IA requereixen grans volums de dades per a aprendre i prendre decisions intel·ligents. En aqueix sentit, les dades són necessàries no sols perquè la IA aconseguisca el seu màxim potencial, sinó també perquè aquesta puga evitar biaixos o errors al moment de realitzar un tractament.

El ràpid avanç de la tecnologia i les eines de IA han portat canvis que possibiliten el processament de milions de dades en diferents parts del món i per diferents actors a una velocitat inimaginable. Però tenim respostes per a tots els reptes que suposen en privacitat l'ús d'aquests sistemes?

Cal preguntar-se quins són els escenaris en els quals la IA puga generar un risc al titular de dades personals. En el present Butlletí tractarem de donar resposta a algunes qüestions suscitées a propòsit de l'afectació d'aquesta mena de sistemes de IA i les diferents implicacions que tenen. Així, ens preguntem si els sistemes de IA podrien ser un mitjà seleccionat per un responsable per a implementar operacions de dades personals en un tractament, però no constituir un tractament en si mateix? i que important és el principi d'exactitud en la recollida de dades i el seu posterior processament?, així com quines implicacions té en les decisions automatitzades en aquesta mena de sistemes?

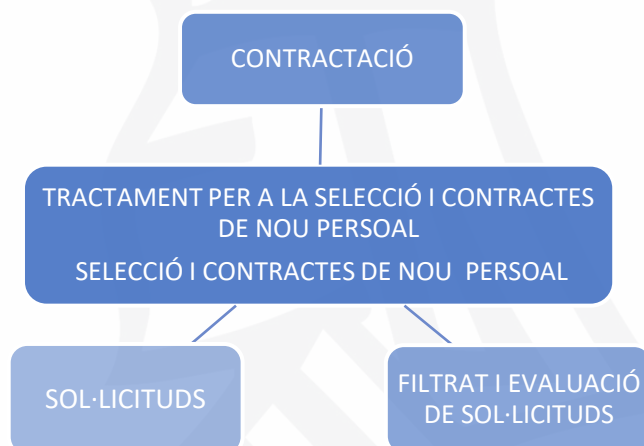


SISTEMA VS. TRACTAMENT IA

Un sistema d'Intel·ligència Artificial (IA), o diversos sistemes de IA, podria ser un mitjà seleccionat per una organització per a implementar operacions de dades personals en un tractament, però no constitueix un tractament en si mateix. És important entendre que la finalitat última d'un tractament és diferent dels mitjans seleccionats per a implementar-lo. Serà el responsable qui determine si els resultats d'un sistema de IA implicarien una decisió automàtica o determinarà que s'inclouga una supervisió humana que prenga la decisió final. Per això, tal com disposa l'AEPD en alguna de les seues publicacions, les decisions automatitzades no estan en la naturalesa del sistema de IA, sinó que són una opció triada pel responsable.

Tenint en compte la premissa, sobre que un sistema de IA en si mateix és només un mitjà per al tractament de dades personals i no un fi últim, posem com a exemple el marc d'un tractament de dades amb finalitats de selecció de personal d'una borsa d'ocupació.

Amb l'exemple seleccionat, el tractament es defineix per la seua finalitat (reclutament), abast (dades d'empleats potencials afectats, duració del procés de selecció, etc.), context (regulació laboral, situació social, estatus d'aquest treball en la societat, etc.) i naturalesa (com s'implementarà el tractament).



Després de decidir la implementació del tractament de dades, el responsable abordarà el disseny del conjunt d'operacions necessàries per a la consecució de la seua finalitat, algunes de la quals requeriran processar dades i altres no. Entre aquestes operacions poden figurar les següents:

- publicar l'oferta laboral,
- disposar d'un procediment per a orientar i recollir les sol·licituds,
- filtrar i seleccionar les sol·licituds que compleixen amb els requisits,
- fer i publicar la selecció final,
- contractar el finalment triat.

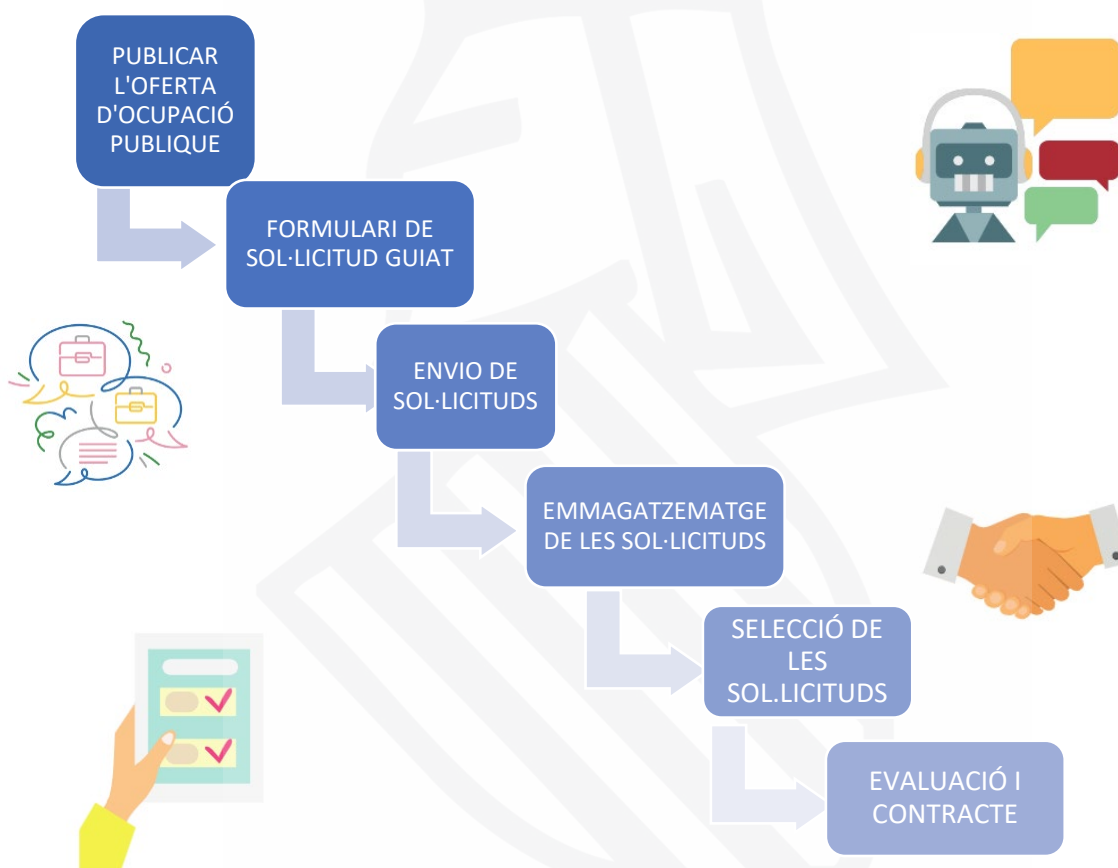
Serà el responsable l'Administració Pública oportuna- qui determine el mitjà d'implementació de les diferents operacions. Aquests podran ser automatitzats o manuals, en les propies instal·lacions o en la nube, per sistemes mòbils, mediante la externalizació de algunes operacions a los encargados, etc.

En aquest marc, l'AEPD posa diversos exemples de com el responsable pot decidir implementar les diferents operacions del tractament proposat.

Així, assenyalava la possibilitat que el responsable decidisca que el procediment per a guiar als candidats a completar el formulari de sol·licitud on inclourien els requisits a implementar s'implemente mitjançant un chatbot (un sistema de IA) dins de la pròpia web de l'Administració; que decidisca utilitzar un sistema de IA per a la selecció automàtica de les sol·licituds que si compleixen les condicions de l'oferta, d'acord amb els criteris necessaris per al desenvolupament del lloc determinats pel responsable (l'Administració), qui també decidirà si aquesta selecció serà supervisada per un humà o no, i per tant si aquesta operació es configura com una presa de decisions automatitzada.

El responsable també podria implementar l'avaluació dels candidats mitjançant un altre sistema de IA que realitze i avalue les proves per als candidats prèviament seleccionats i fins i tot decidir que la selecció final dels candidats es realitze pels resultats del sistema de IA o que hi haguera una supervisió humana d'aquesta avaluació.

En conseqüència, l'AEPD sosté que el responsable té a la seua mà la determinació de configurar una operació com una presa de decisions automatitzada, i l'il·lustra de la següent manera en l'exemple proposat:





Por tant, en aquest exemple, el responsable decideix utilitzar fins a tres sistemes de IA diferents en el marc d'una mateixa activitat de tractament, però cadascun d'aquests sistemes constitueix un mitjà per a implementar diferents operacions i no un tractament en si mateix.

Així, entenem que són operacions dins d'un tractament, perquè cada operació aïllada no podria legitimar-se si no s'inclou en un tractament ampli amb una finalitat última i legítima.

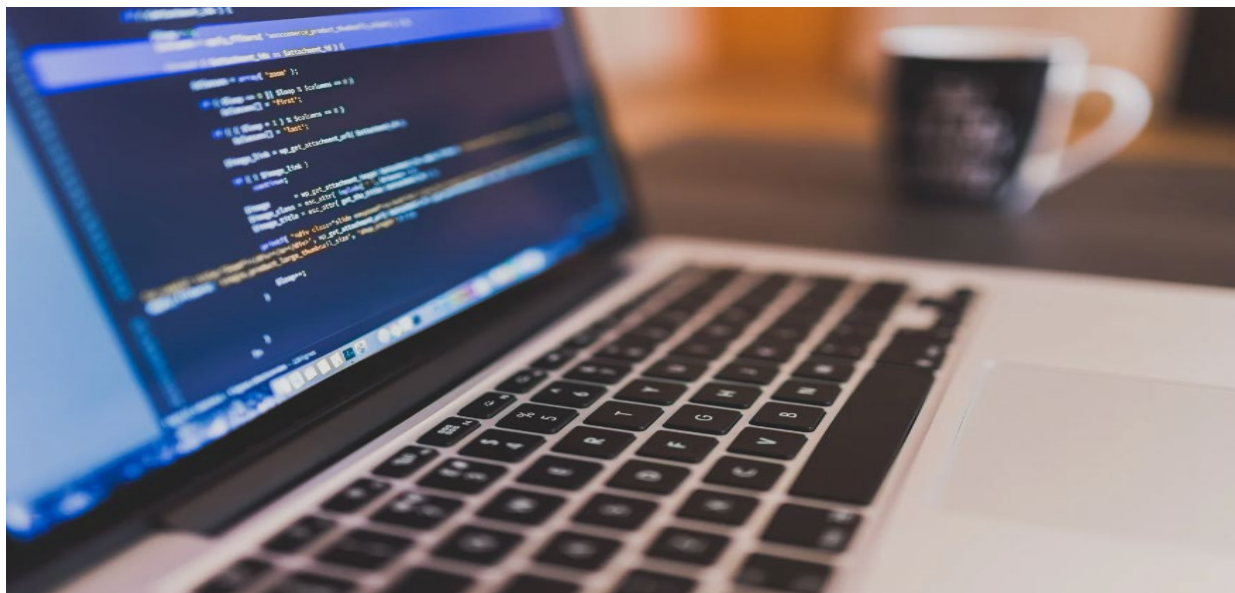
En estudiar aquest procés la conclusió que aconseguim és que és una decisió del responsable sobre l'ús dels sistemes de IA puga conduir a la presa de decisions automatitzades. En conseqüència, el fet que la presa de decisions siga automatitzada no és una característica del sistema IA en si. A l'hora de dissenyar el tractament, és el responsable qui determinarà si inclou una operació addicional de supervisió humana sobre els resultats produïts pel sistema IA.

Finalment, i tenint en compte l'assenyalat per l'AEPD trobem que un tractament de dades personals podria ser implementat per diferents sistemes de IA simultàniament, i també, aquests sistemes de IA podrien implementar-se en local o en el núvol, podrien involucrar encarregats del tractament, etc.

Els sistemes IA formaran part de la naturalesa del tractament quan hagen sigut inclosos en algunes de les operacions necessàries per a dur a terme el tractament amb la seua finalitat explícita. En tal cas, es podrien generar riscos específics per als drets i llibertats dels interessats que han de ser avaluats i gestionats.

“EN CONSEQÜÈNCIA, EL FET QUE LA PRESA DE DECISIONS SIGA AUTOMATITZADA NO ÉS UNA CARACTERÍSTICA DEL SISTEMA IA EN SI. A L'HORA DE DISSENYA EL TRACTAMENT, ÉS EL RESPONSABLE QUI DETERMINA SI INCLOU UNA OPERACIÓ ADDICIONAL DE SUPERVISIÓ HUMANA SOBRE ELS RESULTATS PRODUÏTS PEL SISTEMA IA”.

PRINCIPI D'EXACTITUD EN ELS TRACTAMENTS IA



En un tractament de dades que incorpora un sistema de IA resulta necessari avaluar l'exactitud de les dades que es tractaran. Com que a vegades el comportament d'un algorisme pot veure's compromés per la inexactitud de les dades d'execució d'aquest, no sols per les dades utilitzades en el seu desenvolupament.

Es fa necessari avaluar la fidelitat de les dades d'entrada, ja que els mateixos podrien introduir biaixos resultant compromesos no sols el rendiment de l'algorisme, sinó tot el tractament de dades. Amb això deu s'ha de procurar introduir salvaguardes que s'ocupen d'evitar les possibles inexactituds de les dades d'entrada i protegir así del seu possible impacte; amb estratègies "des del disseny" en l'execució del tractament.

Respecte al principi d'exactitud, podem identificar diversos punts clau derivats d'aquest exemple des del punt de vista del RGPD:

- La falta de definició de les dades d'entrada a un algorisme podria donar lloc a errors o biaixos que no formen part de l'algorisme en sí.
- El principi d'exactitud ha d'aplicar-se tant en les dades d'entrada, com d'eixida i fins i tot en les dades intermèdies de tot tractament.
- Ha d'establir-se una definició precisa de cada dada d'entrada (semàntica) "per disseny" i documentar-se adequadament.
- L'impacte de cada dada d'entrada en el resultat final ha d'avaluar-se "per disseny", per a cada fi específic, mitjançant la realització d'una anàlisi de l'algorisme implementat, mitjançant les proves de verificació dels requisits i mitjançant les proves de validació en el context de l'operació.
- De recopilar-se de manera manual les dades d'entrada els interessats (i els que recopilen dades) han de conèixer i comprendre la semàntica de les dades i l'impacte de la seua resposta.
- Hi ha la possibilitat que les dades d'entrada d'un algorisme es recopilen de fonts diferents, ja siguen bases de dades, sensors com a càmeres, lectors d'empremtes dactilars. Des de l'etapa de



recopilació fins a l'execució de l'algorisme, Les dades poden patir diverses transformacions que també formen part del tractament. Totes aqueixes operacions formen part del tractament, juntament amb l'algorisme.

- Finalment, “S'adoptaran totes les mesures raonables perquè se suprimisquen o rectifiquen sense dilació les dades personals que siguen inexactes respecte als fins per als quals es tracten” (article 5.1.d) del RGPD), és a dir, per a cada fi específic i durant el funcionament del tractament.

En conclusió, cal tindre en compte que fins i tot l'algorisme més precís pot fallar perquè un altre element del tractament no funciona correctament, i en canvi un algorisme menys precís pot funcionar prou bé si durant el disseny s'inclouen les garanties adequades per a evitar gestionar possibles errors.

“PODEM CONCLUDEURE QUE UNA IMPLEMENTACIÓ ADEQUADA DEL PRINCIPI D'EXACTITUD (ARTICLE 5.1.D) DEL RGPD) ÉS ESSENCIAL EN L'EXECUCIÓ DE L'ALGORISME I EN L'ACOMPLIMENT DE TOT EL TRACTAMENT.”

INTEL·LIGÈNCIA ARTIFICIAL I LES DECISIONS AUTOMATITZADES



El Reglament General de Protecció de Dades (article 22.1) garanteix als interessats, el dret a no ser objecte de decisions individuals automatitzades, inclosa l'elaboració de perfils, que produïska en ells efectes jurídics o els afecten significativament. A més, preveu la intervenció o supervisió humana sobre la decisió automàtica per a salvaguardar els drets, els llibertats i els interessos legítims dels interessats.

Deixar clar que, aquest dret s'aplica exclusivament a la presa de decisions totalment automatitzades i que produïska efectes jurídics o, en el seu cas, afecten significativament els titulars de les dades tractades; és a dir, que afecte els seus drets o a la seua esfera jurídica, com, per exemple, la denegació de subvencions públiques o d'entrada a un país, o la cancel·lació d'un contracte o afecte significativament a qualsevol d'aquests.

Més exemples sobre aquest tema, serien a desestimació en un procés de selecció, la denegació d'un crèdit o segur, o l'aplicació de preus diferents a un mateix col·lectiu. No és necessari que afecte un gran nombre de persones. D'acord amb l'anterior, veiem que la casuística pot ser molt diversa:

- Cap tractament automatitzat de dades sense elaboració de perfils
- Elaboració de perfils com a suport a processos de decisió automatitzada
- Elaboració de perfils com a base de processos de decisió completament automatitzada
- Processos de decisió automatitzada amb o sense elaboració de perfils prèvia.

Doncs bé, hem d'esmentar la imminent entrada en vigor del Reglament del Parlament Europeu i del Consell pel qual s'estableixen normes harmonitzades en matèria d'Intel·ligència Artificial (d'ara en avant, RUEIA) el qual planteja criteris de coherència normativa en la interpretació d'aquest article 22 RGPD. Els articles 5 i 14 RUEIA estableixen, respectivament, la prohibició de la IA només en uns certs casos i la supervisió humana únicament en supòsits de sistemes de IA d'alt risc. En la resta dels usos de la IA no es preveu ni reserva d'humanitat ni supervisió humana.

En el desé punt de l'Exposició de Motius de la citada norma s'indica que els Estats membres han d'estar facultats per a especificar l'aplicació de les disposicions a través de la seua pròpia normativa nacional, per a això el Reglament concedeix als Estats un marge de maniobra en la concreció d'aquesta normativa interna, fins i tot en el tractament de dades personals.

En relació amb la legislació espanyola sobre IA i la presa de decisions administratives, cal fer esment de l'article 23 de la Llei 15/2022, de 12 de juliol, integral per a la igualtat de tracte y la no discriminació, que estableix els principis de bona administració i diligència deguda com a límits de les decisions administratives automatitzades.

De conformitat amb aquest estàndard jurídic, les Administracions públiques hauran de tindre en compte criteris de minimització de biaixos, transparència i rendició de comptes, i, seguint les recomanacions de l'O.E., promouran "l'ús d'una IA ètica, de confiança i respectuosa amb els drets



fonamentals". Amb tot, les operacions d'elaboració de perfils realitzades per les autoritats públiques haurien de ser legals, proporcionades i necessàries respecte als fins d'aquestes operacions.

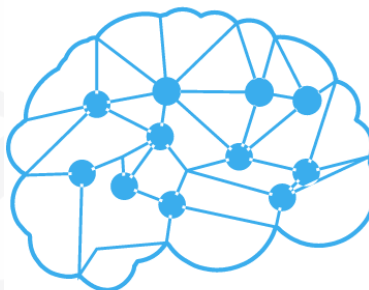
L'esment a la necessitat de continuar avançant en la rendició de comptes dels sistemes de IA amb presa de decisions algorítmiques resulta oportuna, en nom de la protecció dels drets i llibertats dels ciutadans. Com que, malgrat els innegables avantatges de l'ús de sistemes de decisions automatitzades basades en algorismes en termes d'eficàcia i economia, no poden defugir-se els riscos que comporten aquestes decisions per als drets i interessos de la ciutadania.



PROTECCIÓ DE DADES I LA DIMENSIÓ ÈTICA

La perspectiva ètica de la IA, com una part de la “ètica digital”, és un dels aspectes que més inquietud desperta. Cal ser vigilants tant sobre la legitimitat ètica dels tractaments com dels efectes inesperats d'aquests. Així mateix, ha de considerar-se el possible impacte col·lateral d'aquests tractaments en un entorn social, més enllà de les limitacions concebudes inicialment de propòsit, de duració en el temps i d'extensió.

És a dir, cal analitzar la solució IA per se, però també en el marc del tractament en el qual s'integra, i les relacions d'aquest tractament amb l'entorn en diversos aspectes:



- En l'aspecte cultural, amb la seua escala de valors.
- En el context en el qual es desplega el servei, amb els seus requisits de qualitat.
- En els aspectes que es deriven de la interconnexió massiva de components en la societat de la informació.

Els sistemes algorítmics requereixen avaluacions adequades de l'impacte en la privacitat, que incloguen també consideracions socials i ètiques de la seua utilització i una ocupació innovadora de l'enfocament de privacitat des de l'etapa de concepció. Els actors de la IA han d'assumir la responsabilitat de la concepció i l'aplicació dels sistemes de IA de manera que es garantisca la protecció de la informació personal durant tot el cicle de vida del sistema de IA.

Un aspecte crític dels sistemes de IA és el de la possible existència de biaixos (“bias” en anglés). Els biaixos són particularment greus quan, per exemple, deriven en discriminacions d'un d'un grup en favor d'un altre. Però, existeix un altre tipus de biaix que pot ser encara més preocupant i que és el del biaix en la interpretació dels resultats de la IA.

Aquest biaix humà consisteix a acceptar, sense esperit crític, els resultats d'una IA com a certs i inamovibles.

Com ja esmentem en l'epígraf anterior, pot ocórrer que, en algunes ocasions, els éssers humans decidisquen dependre dels sistemes de IA per raons d'eficàcia. Però, la decisió de cedir el control en contextos limitats continuarà recaient en els éssers humans, ja que aquests poden recórrer als sistemes de IA en l'adopció de decisions i en l'execució de tasques. No obstant això, un sistema de IA mai podrà reemplaçar la responsabilitat final dels éssers humans i la seua obligació de rendir comptes. Per regla general, les decisions de vida o mort no haurien de cedir-se als sistemes.

Són diferents problemàtiques les que hauran d'abordar-se de cara a disposar d'una protecció homogènia sobre l'ús dels sistemes de IA. Actualment, aquestes són algunes de les qüestions que els Estats membres hauran de resoldre:

1. Que siga possible atribuir la responsabilitat ètica i jurídica, en qualsevol etapa del cicle de vida dels sistemes de IA, així com en els casos de recurs relacionats amb sistemes de IA, a persones físiques o a entitats jurídiques existents.
2. Haurien d'establir marcs d'avaluació de l'impacte, com a avaluacions de l'impacte ètic, per a determinar i analitzar els beneficis, els problemes i els riscos dels sistemes de IA, així com



mesures adequades de prevenció, atenuació i seguiment dels riscos, entre altres mecanismes de garantia.

3. Vetlar perquè els mecanismes de governança de la IA siguen inclusius, transparents, multidisciplinaris i multilaterals.
4. Procurar elaborar estratègies de governança de dades que garantisquen l'avaluació contínua de la qualitat de les dades d'entrenament per als sistemes de IA, en particular la idoneïtat dels processos de recopilació i selecció de dades, i que prevegen mesures adequades de seguretat i protecció de les dades, així com mecanismes de retroalimentació per a aprendre dels errors i compartir les millors pràctiques entre tots els actors de la IA.





MATERIAL COMPLEMENTARI

- Reglament (UE) 2022/868 del Parlament Europeu i del Consell de 30 de maig de 2022 relatiu a la governança europea de dades i pel qual es modifica el Reglament (UE) 2018/1724 (Reglament de Governança de Dades). Consulta la Directiva en [aquest enllaç](#).
- Publicació guia de l'AEPD sobre "Adequació al RGPD de tractaments que incorporen Intel·ligència Artificial. Una introducció. Consulta la Publicació en [aquest enllaç](#).
- Publicació de l'AEPD, sobre "Mapa de referència per a tractaments que inclouen Intel·ligència Artificial". Consulta [aquest enllaç](#).
- Proposta de reglament del parlament europeu i del consell pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial (Llei d'intel·ligència artificial) i es modifiquen determinats actes legislatius de la unió. Consulta [aquest enllaç](#).
- Carta dels drets fonamentals de la Unió Europea. Consulta [aquest enllaç](#).
- Tractat de funcionament de la Unió Europea. Consulta [aquest enllaç](#).
- Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). Consulta [aquest enllaç](#).

NOTICIES

▪ Les autoritats de la Xarxa Iberoamericana de Protecció de Dades Personals inicien una acció coordinada en relació amb el servei ChatGPT

La Xarxa Iberoamericana de Protecció de Dades (RIPD), fòrum constituït per 16 autoritats de protecció de dades de 12 països de la regió l'objectiu de la qual és promoure i garantir el dret fonamental a la protecció de dades personals i la secretaria permanent de les quals ostenta a l'Agència Espanyola de Protecció de Dades, coordinarà una acció sobre el servei ChatGPT

Consulta la publicació en [aquest enllaç](#).

▪ L'AEPD inicia d'ofici actuacions d'investigació a OpenAI, propietària de ChatGPT

L'Agència Espanyola de Protecció de Dades (AEPD) va iniciar d'ofici actuacions prèvies d'investigació a l'empresa estatunidenca OpenAI, propietària del servei ChatGPT, per un possible incompliment de la normativa

Consulta la publicació en [aquest enllaç](#).

▪ L'autoritat de control de protecció de dades d'Itàlia bloqueja ChatGPT. Recopilació il·legal de dades personals. Absència de sistemes de verificació de l'edat dels menors.

El Garant per la Protezione dei Dati Personali per la protecció de dades personals va ordenar, amb efecte immediat, la limitació temporal el tractament de dades d'usuaris italians. Alemanya, França i Irlanda han sol·licitat informació al Garant per si també pren aquestes mesures.

Consulta la publicació en [aquest enllaç](#).