



El Model PIO (Principis, Indicadors i Observables) sobre *Obligacions i Drets*: Un enfocament d'autoavaluació per al compliment de la regulació en dades i sistemes d'intel·ligència artificial en el marc de la Unió Europea

Observatori d'Ètica en Intel·ligència Artificial de Catalunya (OEIAC)

El Model PIO (Principis, Indicadors i Observables) sobre *Obligacions i Drets*:
Un enfocament d'autoavaluació per al compliment de la regulació en dades i
sistemes d'intel·ligència artificial en el marc de la Unió Europea

CIP 681.3.01(IA) LIL

Lillo Campoy, Alexandra

El Model PIO (Principis, Indicadors i Observables) sobre
Obligacions i Drets : un enfocament d'autoavaluació per al
compliment de la regulació en dades i sistemes d'intel·ligència
artificial en el marc de la Unió Europea / redacció: Alexandra
Lillo Campoy, Arlet Brufau i Centelles i Albert Sabater Coll
(OEIAC). – Girona : Observatori d'Ètica en Intel·ligència
Artificial de Catalunya (OEIAC) : Universitat de Girona.
Oficina Edicions UdG, gener de 2025. – Girona : Observatori
d'Ètica en Intel·ligència Artificial de Catalunya (OEIAC) :
Universitat de Girona. Oficina Edicions UdG, gener de 2025.
Descripció del recurs: 16 gener 2025
ISBN 978-84-8458-711-8

I. Brufau i Centelles, Arlet, autor II. Sabater i Coll, Albert, autor
III. Observatori d'Ètica en Intel·ligència Artificial de Catalunya
1. Intel·ligència artificial – Aspectes ètics i morals 2. Llibres electrònics

CIP 681.3.01(IA) LIL



Aquesta obra es troba sota una llicència Creative Commons (Reconeixement – Compartir Igual).
Aquesta llicència permet l'ús, modificació i distribució d'aquesta obra amb qualsevol finalitat,
sempre i quan es reconegui als autors i, en el cas de que es realitzin modificacions o
desenvolupaments a partir de la mateixa, l'obra derivada es compartirà amb la mateixa llicència.

Observatori d'Ètica en Intel·ligència Artificial de Catalunya (OEIAC)

Carrer de la Universitat, 10 – Edifici Econòmiques

Universitat de Girona 17003 Girona

Girona, gener 2025

ISBN 978-84-8458-711-8 (Editor: Oficina Edicions UdG)

Agraïments: Alicia de Manuel Lozano, Amadeo Szpiga Montenegro i Arnau Serra Pòrtulas.

Contingut

Pròleg: La IA que ens cal	4
1. Introducció.....	6
2. Origen.....	9
3. Destinació: obligacions i drets	10
3.1. Un model d'obligacions.....	10
3.2. Un model basat en drets	14
4. Justificació.....	19
5. Instruccions.....	22
6. Les 10 preguntes inicials o bàsiques	28
7. Actualització del qüestionari	29
7.1. Preavaluació	30
7.1.1 Risc inacceptable.....	30
7.1.2. Qüestionari de classificació dels sistemes en funció dels riscos.....	32
7.2. Qüestionari.....	35
7.2.1. Principi 1: Transparència i explicabilitat.....	36
7.2.2. Principi 2: Justícia i equitat	49
7.2.3. Principi 3: Seguretat i no maleficència	62
7.2.4. Principi 4: Responsabilitat i retiment de comptes.....	73
7.2.5. Principi 5: Privacitat.....	84
7.2.6. Principi 6: Autonomia	98
7.2.7. Principi 7: Sostenibilitat.....	108
8. Guia per contractes en matèria d'IA.....	122
9. Bibliografia.....	132
ANNEX II: Navegació de la web Del Model Pio Obligacions i Drets.....	165
ANNEX III: Catàleg legal i de recomanacions.....	177
ANNEX IV: Catàleg d'exemples.....	196
ANNEX V: La AI Act.....	203
ANNEX VI: AI Liability Directive.....	209
ANNEX VII: Avaluació de conformitat.....	213
ANNEX VIII: Avaluació d'impacte sobre drets fonamentals.....	216
ANNEX IX: Obligacions de transparència.....	217
ANNEX X: Subjectes contemplats per la AI Act.....	221
ANNEX XI: 50 exemples de l'aplicació de la AI Act.....	222
ANNEX XII: Preguntes freqüents (FAQ).....	226

LA IA QUE ENS CAL

La intel·ligència artificial (IA) s'ha consolidat com una de les eines més transformadores del segle XXI. És, alhora, un motor de progrés i un gran repte col·lectiu de responsabilitat social.

En aquest context, el Govern de Catalunya assumeix el repte d'impulsar la implementació de la IA fent compatible la innovació digital amb un compromís ineludible amb la democràcia i els drets humans.

L'augment exponencial de l'ús de sistemes d'IA en tots els àmbits de la vida —des de la salut fins a la mobilitat, passant per l'educació, l'oci, o com ens relacionem amb les institucions públiques— exigeix solucions que garanteixin que la tecnologia es desenvolupi i utilitzi amb la perspectiva de millorar la vida de les persones i de respectar els principis ètics fonamentals.

Catalunya es troba avui en una posició privilegiada per esdevenir un referent internacional en la implementació d'una IA ètica i alhora competitiva. L'ecosistema d'IA català compta amb centres tecnològics i de recerca excel·lents, amb la capacitat de generar i atraure talent, amb mecanismes de transferència tecnològica per connectar la innovació amb les necessitats de la societat i les empreses, i amb una oferta de solucions basades amb IA per respondre a la demanda creixent d'adopció d'aquesta tecnologia. Vora 500 empreses a Catalunya es dediquen a la IA, gairebé el triple que fa cinc anys¹.

Des del Govern tenim la responsabilitat de facilitar que els diversos actors de l'ecosistema d'IA català tinguin molt en compte els principis ètics, l'impacte social i la legislació vigent. Exemplifica aquesta aposta el Model PIO (Principis, Indicadors i Observables), desenvolupat per l'Observatori d'Ètica en Intel·ligència Artificial de Catalunya (OEIAC) en el marc de l'Estratègia d'Intel·ligència Artificial de Catalunya (Catalonia.AI) que promou la Generalitat de Catalunya a través de la Secretaria de Polítiques Digitals.

El Model PIO és una eina d'autoavaluació per guiar les organitzacions públiques i privades en l'adopció de la IA. Aquesta eina incorpora, més enllà de recomanacions ètiques, tot el marc regulador que afecta la implementació d'IA, inclosa la regulació europea sobre IA (AI Act). És un recurs obert a tothom, disponible en català, castellà, anglès i francès, de moment, i permet la revisió pràctica de principis com la transparència, la seguretat i la responsabilitat, mitjançant indicadors clars i mesurables, així com exemples d'accions concretes.

És fonamental que qui demana, desenvolupa i utilitza solucions basades amb IA pugui prendre decisions informades i responsables. La innovació s'ha de desenvolupar dins d'un marc de confiança i seguretat. No es tracta només de complir amb la llei, sinó també de promoure la millora contínua d'acord amb els valors que ens defineixen com a societat. Volem i podem ser competitius fent les coses bé.

¹ ACCIÓ- Agència per la Competitivitat de l'Empresa en col·laboració amb el CIDAI. (2024) *La intel·ligència artificial a Catalunya*. (Informes tecnològics). Disponible a: <https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/la-intelligencia-artificial-a-catalunya> (consultada el 12 de desembre 2024).

Catalunya actualment presideix l'Aliança internacional DETA (*Disruptive and Emerging Technology Alliance*), una aliança de governs regionals d'arreu del món, representants de territoris capdavanters en la implementació de tecnologies digitals avançades i que aposten pel seu desplegament ètic. En aquest marc, el Govern ha liderat la redacció d'un manifest per promoure una IA fiable. El text fa un diagnòstic del context actual, dibuixa una visió i recull valors fonamentals i recomanacions. Així mateix, estableix cinc compromisos: desenvolupament ètic, governança transparent, innovació inclusiva, responsabilitat i retiment de comptes i desenvolupament sostenible. Cinc compromisos que són imprescindibles.

Totes les parts implicades —administracions, empreses, centres de recerca i tecnològics, societat civil organitzada i ciutadania— hem de sumar esforços per consolidar Catalunya com un referent on la IA serveixi per millorar la qualitat de vida de les persones, tot respectant i assegurant els seus drets. Aquesta és la IA que ens cal.

Treballem-hi.

Miquel Sàmper
 Conseller d'Empresa i Treball



1. INTRODUCCIÓ

És ben sabut que els desenvolupaments recents en intel·ligència artificial (IA) no són únicament tecnològics sinó ideològics i socials, ja que el seu impacte social és cada cop més ampli i els usos ètics no són suficients i requereixen d'una regulació. Aquesta evolució és normal després d'un període d'acceleració i laissez-faire en el que només alguns aspectes com els de seguretat i responsabilitat individual han estat els contemplats. No obstant, l'adopció de sistemes d'IA en la nostra vida quotidiana genera no tan sols una creixent demanda de consideracions ètiques i socials en el disseny i ús de sistemes d'IA, sinó que també és essencial identificar els aspectes clau d'aquestes consideracions i aplicar-los de manera pràctica per establir un procés continu de retiment de comptes sobre el disseny i ús de tecnologies d'IA.

Val a dir, però, que les consideracions ètiques no són suficients arribat aquest punt. En aquest context, la regulació és fonamental per garantir que els sistemes d'IA es desenvolupin i s'utilitzin de manera responsable i en benefici de la societat. Sense un marc normatiu clar, existeix el risc que els sistemes d'IA puguin ser explotats de maneres que violin els drets humans, amplifiquin desigualtats o generin danys socials i econòmics. La regulació també ajuda a establir estàndards de transparència, responsabilitat i seguretat que permeten garantir que la IA es dissenyi i s'implementi tenint en compte les persones al centre, així com els seus hàbitats i el medi ambient. És per això que calen accions i mesures que ajudin a avançar en aquesta direcció d'IA responsable i sostenible, assegurant que es preserven els valors fonamentals de la societat.

Evidentment, aquesta no és una tasca fàcil ja que una de les dificultats que sorgeixen és que moltes de les orientacions sobre ètica, regulació i IA són sovint massa complexes i tècniques, fent-les difícils d'entendre per a actors no acadèmics o especialistes. Això no només fa que siguin de difícil comprensió per part de sectors com l'administració, les empreses, els organismes professionals i les organitzacions de la societat civil, sinó que també en retarda la implementació. De fet, la manca d'un llenguatge accessible i d'indicadors fàcilment comprensibles endarrereix l'adopció de principis ètics i d'una regulació com a part fonamental de la innovació responsable.

En definitiva, per avançar cap a una IA responsable i sostenible, és necessari traduir els principis ètics en indicadors clars i mesurables, tant quantitius com qualitius, que permetin avaluar l'ús ètic de les dades i els sistemes d'IA en un marc regulador. Això no només facilitarà la seva adopció per part de la societat, sinó que també contribuirà a crear un entorn d'innovació més dinàmic i competitiu, on l'avaluació constant juga un paper crucial. Però això, requereix d'informació accessible i de capacitat tècnica en la mateixa avaluació així com anar més enllà de les recomanacions ètiques i d'uns determinats textos reguladors. Calen eines de verificació exhaustiva, però senzilles d'utilitzar que ens facin avançar cap a una aplicació molt més quotidiana i efectiva que inclogui, cada vegada més, aspectes d'alfabetització i normalització de l'avaluació dels usos ètics i del compliment de la regulació en dades i sistemes d'IA en el marc de la Unió Europea.

En aquest sentit, en el present informe presentem les principals modificacions realitzades al **Model PIO**, l'eina d'autoavaluació organitzativa sobre l'ús ètic de dades i sistemes d'intel·ligència artificial desenvolupada per l'Observatori d'Ètica en Intel·ligència Artificial de Catalunya (OEIAC).

En aquesta darrera interacció, que serà pròximament introduïda a la pàgina web de l'OEIAC (<https://OEIAC.cat/>), s'ha optat per seguir una doble estratègia que complementa la informació ja continguda al formulari original: il·lustrar l'origen, això és, les fonts que han nodrit el disseny del formulari; i fer referència la destinació de les preguntes, és a dir, quina serà la seva aplicació pràctica un cop entri en vigor la legislació que regula els sistemes d'IA.

Si bé l'objectiu inicial del **Model PIO** (versió beta) de l'OEIAC era desenvolupar una eina que permetés reduir la bretxa existent entre els principis d'alt nivell o abstractes i la seva aplicació de manera concreta o aplicada en qualsevol desenvolupament o implementació de la IA, amb aquesta actualització fem un pas més en aquesta direcció fomentant el compliment de la normativa sobre riscos de la IA mitjançant una verificació exhaustiva. Per tant, l'objectiu actual del nou **Model PIO** és facilitar tant l'aplicació dels usos ètics com promoure la normativa sobre IA i drets. Això sí, per facilitar el seu ús, ho fem de forma alineada amb els **7 principis** ètics que caracteritzen el **Model PIO** anterior i actual, ja que estan reconeguts com a estàndards internacionals en el disseny, implementació i ús de sistemes d'IA.

Aquests objectius parteixen d'un fet incontestable: la proliferació de productes i serveis que utilitzen sistemes d'IA. Davant d'aquesta realitat, creiem que és essencial garantir que els sistemes d'IA siguin justos, explicables i segurs, entre altres, i que les organitzacions que els desenvolupin o implementen actuïn de manera transparent i responsable. És obvi que si es vol fomentar la confiança del públic en aquestes tecnologies d'IA, és necessari anar molt més enllà del tecno-optimisme o confiança cega, així com passar pàgina en termes d'infal·libilitat i inevitabilitat tecnològica. No cal acceptar les tecnologies d'IA tal i com són i, en aquest sentit, al marge de l'autoavaluació constant, la regulació també exerceix un paper crucial per evitar que l'autoavaluació quedi limitada a accions voluntàries o simbòliques.

Mitjançant normatives clares i aplicables, podem garantir que les organitzacions assumeixin responsabilitats en el desenvolupament i ús de la IA, incloent-hi en casos d'errors o abusos. A més, un marc regulador ben definit facilita que les institucions supervisin i avaluin l'impacte social dels sistemes d'IA, establint mecanismes de control i sanció quan sigui necessari. Per tant, la regulació no només promou la confiança, sinó que també protegeix els drets de les persones usuàries i consumidors davant possibles abusos o mal ús d'aquestes tecnologies. En aquest context, el **Model PIO** és un pas endavant per integrar conjuntament els principis ètics bàsics de la IA en la pràctica i la normativa vigent referent a la IA i a drets, el que ajuda a garantir la responsabilitat a cada etapa del cicle de vida de les dades i sistemes d'IA. El nou model també es basa en la senzillesa i en una pregunta clau i recurrent ("Ho hem fet?"), però ofereix informació i indicacions de verificació per garantir que anem més enllà de la bona fe de les organitzacions per complir amb els estàndards ètics.

En resum, aquesta actualització del **Model PIO** cerca mostrar que els Principis, Indicadors i Observables inclosos, troben el seu origen en la literatura acadèmica especialitzada, en les recomanacions i els *checklists* i *toolkits* d'organismes i entitats que vetllen per l'ús ètic dels sistemes d'IA, i en la discussió constant sobre els usos ètics de la IA amb una, cada vegada, major representació de persones usuàries, destinatàries o afectades pels propis sistemes d'IA.

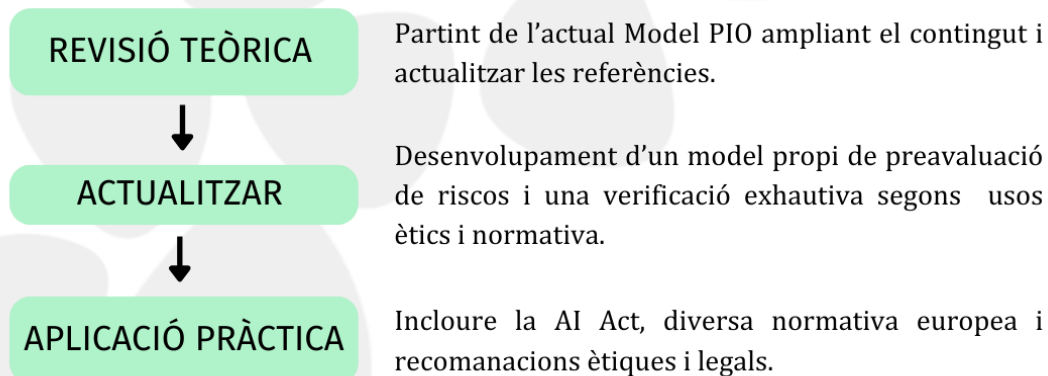
Per aquest motiu, també es vol subratllar que el nou **Model PIO** no només es tracta d'un interessant exercici d'autoavaluació organitzativa, sinó que pot utilitzar-se com una expressió

pràctica de la normativa europea sobre IA i drets humans vigents. Com veureu, es tracta d'una actualització molt considerable ja que inclou nous apartats com la preavaluació i avaluació extensa (amb referències i exemples), catàlegs extensos sobre textos legislatius a tenir en compte i múltiples exemples i recomanacions de clàusules de compra, entre altres. Entenem que tots aquests recursos contribueixen a millorar la comprensió i l'aplicació de principis ètics així com del compliment de la normativa, de manera que segueixen sent rellevants per a tots els sectors i estableixen un procés de millora contínua basat en el coneixement i en l'experiència pràctica.

Com l'anterior **Model PIO**, aquesta nova versió va dirigida a totes les organitzacions públiques i privades que tenen interès en el disseny, desenvolupament o implementació de tecnologies d'IA, així com a totes les persones que utilitzin, comprin o siguin destinatàries d'aquestes tecnologies. En aquest sentit, és fonamental reconèixer que el **Model PIO** és dinàmic: més enllà de proporcionar informació i orientació sobre les àrees que requereixen més atenció, cal integrar nous coneixements i compartir aprenentatges a partir de les experiències pràctiques de diverses organitzacions.

2. ORIGEN

Per tal de reflectir l'origen de les preguntes, s'ha redactat un breu paràgraf que cita les fonts emprades en l'elaboració de cada qüestió. Si bé aquesta informació bibliogràfica ja existeix de manera detallada a [l'informe de presentació del Model PIO publicat per aquest Observatori](#), en aquesta darrera iteració es traslladen les referències a la pàgina web, i s'enllaça de la manera més concreta possible la secció, capítol o pàgina on es troba la informació que va inspirar la pregunta. Així, la part que versa sobre l'origen de les preguntes facilita l'accés a documents molt diversos elaborats per organitzacions amb una palmària solvència tècnica, com ara l'UNESCO i les seves recomanacions ètiques sobre la IA², la llista d'avaluació ALTAI per a una IA confiable desenvolupada per l'AI HLEG³, el *framework* interdisciplinari per racionalitzar l'ètica en la IA d'AIEIG⁴, i la Declaració de Barcelona de 2017⁵, així com a articles acadèmics d'experts en ètica i IA⁶.



Il·lustració 1 Procès de desenvolupament del Model PIO.

² UNESCO (2021) Esborrany del text de la recomanació sobre l'ètic de la Intel·ligència Artificial. SHS/IGM-AIETHICS/2021/JUN/3Rev.2. Disponible a: <https://shorturl.at/kjblU> (consultada el 7 de març de 2023).

³ High-Level Expert Group on Artificial Intelligence (2020) Llista d'avaluació per a una Intel·ligència Artificial de confiança. Disponible a: <https://shorturl.at/mC754> (consultada el 7 de març de 2023).

⁴ AI Ethics Impact Group (2020) D'els principis a la pràctica: Un marc interdisciplinari per operacionalitzar l'ètica de la IA. Disponible a: <https://shorturl.at/Va2wc> (consultada el 7 de març de 2023).

⁵ Barcelona Declaration (2017) Declaració de Barcelona per al Desenvolupament i ús adequat de la Intel·ligència Artificial a Europa, IIIA CSIC. Disponible a: <https://www.iiia.csic.es/barcelonadeclaration/> (consultada el 7 de març de 2023).

⁶ Mörch, C. M. et al (2020) Protocol de Canadà: Una llista de comprovació ètica per a l'ús de la Intel·ligència Artificial en la prevenció del suïcidi i la salut mental. Intel·ligència Artificial en la Medicina 108.(2020)1019342. Disponible a: <https://doi.org/10.1016/j.artmed.2020.101934> (consultada el 16 d'octubre de 2023).; Attard-Frost, B., De los Ríos, A. & Walters, D.R. (2022). The ethics of AI business practices: a review of 47 AI ethics guidelines. Disponible a: <https://doi.org/10.1007/s43681-022-00156-6> (consultada el 7 de març de 2023).

3. DESTINACIÓ: OBLIGACIONS I DRETS

3.1. Un model d'obligacions

Respecte a la destinació de les preguntes, això és, l'expressió normativa i jurídica dels principis continguts al qüestionari, el principal instrument relacionat a la pestanya d'*obligacions i drets* és el Reglament 2024/1689 del Parlament i del Consell conegut com a **AI Act**⁷. Aquesta nova legislació europea és el primer gran instrument normatiu supranacional que cerca regular els sistemes d'intel·ligència artificial, i proporcionarà un marc general en el qual es concretin regles per a l'ús ètic dels sistemes d'IA⁸. D'aquesta manera, la **AI Act** crea un conjunt de normes harmonitzades que guiaran a les organitzacions en el desenvolupament i ús de sistemes d'IA confiables, d'acord amb les seves implicacions ètiques, legals i socials⁹.

La **AI Act** classifica diferents aplicacions i sistemes d'IA en quatre categories de risc diferenciades: a) Aquells que comporten un risc inacceptable, i conseqüentment queden prohibits (ex. sistemes de puntuació social) ; b) Els considerats d'alt risc pel seu potencial impacte sobre els drets fonamentals, la seguretat, la salut, la democràcia i l'estat de dret (ex. sistemes que determinen el dret d'una persona a accedir a serveis de salut), els quals són objecte de la majoria d'obligacions imposades per la **AI Act**, incloent-hi la superació d'una avaluació de conformitat per part de tercers abans de la seva comercialització posada en servei; c) Els sistemes de risc limitat, on s'inclouen les IA generatives (ex. *Chat GPT*), els sistemes de reconeixement d'emocions i identificació biomètrica, els models de propòsit general i qualsevol altre sistema que interactuï directament amb persones físiques, els quals únicament es veuran afectats per determinats requisits de transparència; i d) els sistemes considerats de risc mínim, una categoria residual on s'inclouen tots aquells sistemes que no es cataloguen en cap de les anterior, i la regulació dels quals és pràcticament inexistent.

Al llarg del procés legislatiu que ha donat lloc a la **AI Act**, les institucions que han participat en desenvolupament de la norma, concretament, la Comissió, el Parlament i el Consell, han publicat diversos textos amb esmenes a la proposta general. El **Model PIO**, s'ha modificat, ampliat i millorat per adaptar-se a cadascun d'aquest documents, de cara a la versió final de la normativa.

⁷ Reglament 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024. Disponible a: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (consultada el 4 de març de 2023).

⁸ Minkinen, M., Laine, J. & Mäntymäki, M. (2022) Auditoria continua de la Intel·ligència Artificial: conceptualització i avaluació d'eines i marcs. *DISO 1, 21* (2022). Disponible a: <https://doi.org/10.1007/s44206-022-00022-2> (consultada el 2 d'agost de 2023).

⁹ Floridi, L., Holweg, M., Taddeo, M., Amaya Silva, J., Mökander, J., i Wen, Y. (2022) Cap a la IA – Procediment per evaluar la conformitat dels sistemes d'IA segons la AI Act. Disponible a: <https://oecd.ai/en/catalogue/tools/capai-a-procedure-for-conducting-conformity-assessment-of-ai-systems-in-line-with-the-eu-artificial-intelligence-act> (consultada el 13 d'agost de 2023).

Per aquest motiu, aquesta versió del **Model PIO** ha recollit totes les fases per les que ha anat passant la proposta legislativa: la Proposta de Reglament del Parlament Europeu i del Consell pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial (**AI Act**) i es modifiquen determinats actes legislatius de la Unió, publicada per la Comissió el 21 d'abril de 2021¹⁰; les esmenes adoptades pel Parlament Europeu el 14 de juny de 2023¹¹; el 9 de desembre de 2023 s'adopta l'acord entre el Parlament Europeu i el Consell en relació amb gran part del contingut de la normativa, de cara aprovar el text definitiu¹²; el text definitiu aprovat pel Parlament el 13 de març de 2024¹³, i pel Consell el 21 de maig d'aquest mateix any¹⁴; i, finalment, el Reglament 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades sobre intel·ligència artificial i es modifiquen determinats actes legislatius (**AI Act**), que va ser publicat al Diari Oficial de la Unió Europea el 12 de juliol de 2024.

Una de les qüestions cabdals de la **AI Act** i, en conseqüència, una de les àrees més conflictives, són els criteris de classificació de les IA d'alt risc, i finalment, els canvis en relació amb la categorització dels sistemes d'IA per tal d'adaptar-nos a la versió definitiva de la **AI Act**.

En les primeres versions de la proposta, tots els sistemes d'IA inclosos en una llista preestablerta d'àrees concretes contemplada a l'annex III de la regulació eren considerats d'alt risc, juntament amb els sistemes afectats per les normatives contemplades a l'annex I del Reglament. Al llarg del procés legislatiu aquesta llista va ser alterada, de manera que es van modificar alguns casos i se'n van afegir d'altres.

¹⁰ Comissió Europea (2021) Proposta de Reglament del Parlament Europeu i del Consell, Normes harmonitzadores en matèria d'Intel·ligència Artificial (Artificial Intelligence Act) i modifica determinat actes legislatius de la UE. Disponible a: <https://shorturl.at/oYnOQ> (consultada el 4 de març de 2023).

¹¹Parlament Europeu (2023) Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 0206 – C9-0146/2021 – 2021/0106(COD) (1). Disponible a: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html (consultada el 16 de juny de 2023).

¹²Parlament Europeu (2023) Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI. Disponible a: <https://www.europarl.europa.eu/news/-/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai> (consultada el 9 de desembre de 2023).

¹³Parlament Europeu (2024) Resolució legislativa del Parlament Europeu de 13 de març de 2024 sobre la proposta de Reglament del Parlament Europeu i del Consell pel qual s'estableixen normes harmonitzades sobre intel·ligència artificial (Llei d'Intel·ligència Artificial) i es modifiquen determinats actes legislatius de la Unió (COM(2021) 0206 – C9-0146/2021 – 2021/0106(COD)). Disponible a: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html (consultada el 14 de març de 2024).

¹⁴Consell de la Unió Europea (2024) Artificial intelligence (AI) Act: Council gives final green light to the first worldwide rules on AI. Disponible a: <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/> (consultada el 21 de maig de 2024).

Així mateix, després de processos de discussió sobre la possibilitat d'incloure una sèrie d'excepcions¹⁵, s'han acabat integrant i permetent, als sistemes inclosos en aquestes matèries, evitar les obligacions imposades als sistemes d'alt risc quan es donen les següents condicions:

- 1) Que el sistema d'IA es destini a portar a terme una tasca de procediment limitat (ex. Classificar documents per categories).
- 2) Que el sistema d'IA es destini a revisar o millorar alguna cosa resultant d'una activitat humana prèvia (ex. [Scribens](#), un sistema que corregeix i millora textos, entraria dins d'aquesta excepció).
- 3) Que el sistema d'IA es destini exclusivament a identificar patrons de presa de decisions o desviacions dels mateixos per tal d'assenyalar anomalies (ex. Que el sistema s'utilitzi per identificar despeses inusuals en el patró de despeses d'una empresa).
- 4) Que el sistema d'IA es destini a preparar una avaluació d'usos d'alt risc del sistema (ex. Un software de gestió d'arxiu que permeti ordenar i classificar les dades abans de ser analitzades).

De la mateixa manera, l'article 7 de la AI Act adoptada atorga a la Comissió la potestat per modificar l'annex III afegint o modificant els usos considerats d'alt risc quan suposin un risc per als drets fonamentals, la seguretat o la salut, i per eliminar aquells que hi consten si aquest risc desapareix.

Aquest plantejament va ser criticat per l'opinió experta del servei legal del Parlament Europeu, segons el qual el mètode plantejat donava massa espai a la interpretació subjectiva, contribuït a la inseguretat jurídica¹⁶.

Respecte a la seva relació amb el formulari del **Model PIO**, els principals punts de connexió els trobem als capítols 2 i 3 del Títol III, que regulen els requisits exigibles als sistemes d'IA d'alt risc i les obligacions de les persones proveïdores i usuàries dels sistemes d'IA d'alt risc, respectivament. Si bé els considerants de la proposta legislativa comprenen de manera molt àmplia tots els aspectes continguts a la literatura especialitzada i al nostre propi informe, cal accentuar que la part normativa i exigible a les entitats i organitzacions que empren sistemes d'IA comença a partir del capítol 2.

Així doncs, el capítol esmentat regula la implementació d'un sistema de gestió de riscos i el testatge dels sistemes d'IA (article 9), exigeix el compliment de determinats estàndards en la recollida, processament i governança de dades (article 10), estableix l'obligatorietat de crear sistemes per registrar automàticament diverses operacions i esdeveniments (*logs*) del sistema d'IA (article 12), assegura que els sistemes d'IA d'alt risc es dissenyin i desenvolupin amb la

¹⁵ Bertuzzi, Luca. (2023) AI Act: Leading MEPs revise high-risk classification, ignoring negative legal opinion. Disponible a: <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-leading-meps-revise-high-risk-classification-ignoring-negative-legal-opinion/> (consultada el 26 de setembre de 2023).

¹⁶ Bertuzzi, Luca. (2023) Els responsables polític de la UE han estat debatent algunes condicions de filtre que permetien el desenvolupament de la IA amb un règim menys estricte. Però aquest compromís polític topa amb problemes legals. Disponible a: [AI Act: EU Parliament's legal office gives damning opinion on high-risk classification 'filters' – EURACTIV.com](#) (consultada el 26 de setembre de 2023).

deguda transparència (article 13), regula la vigilància humana dels sistemes d'IA (article 14) o estableix l'obligatorietat de garantir l'exactitud, robustesa i seguretat dels sistemes d'IA, incloent-hi la reducció dels biaixos (article 15).

D'altra banda, el capítol 3 regula les obligacions de les persones proveïdores dels sistemes d'IA d'alt risc (article 16), i estableix que han de desenvolupar un extens sistema de gestió de qualitat que inclogui una estratègia per al *compliance* que inclogui l'avaluació de conformitat del sistema, el testatge previ i *ex post* dels sistemes d'IA, un sistema de monitoratge, sistemes per a la gestió de dades, etc. (article 17), així com el requeriment de sotmetre el sistema a una avaluació d'impacte sobre els drets fonamentals (article 27).

De la mateixa manera, el **Model PIO** guarda relació amb les obligacions de transparència imposades als sistemes d'IA generativa (art. 50) així com els requisits exigits als models de propòsit general, que són aquells que han estat entrenats amb un gran nombre de dades i que es poden adaptar a una gran diversitat de tasques (articles 51 i següents).

Finalment, l'actualització del **Model PIO** també fa referència a l'article 95 relatiu a la promoció de codis de conducta d'aplicació voluntària que, si bé no estableixen obligacions jurídiques concretes, tracten matèries tan crucials com l'accessibilitat de persones amb discapacitat, la participació multisectorial en el disseny i desenvolupament dels sistemes, la diversitat dels equips de desenvolupament o la sostenibilitat ambiental. Així mateix, en aquesta iteració incloem referències a altres normatives, com la AI Liability Directive¹⁷, una proposta de normativa europea sobre responsabilitat per danys de la intel·ligència artificial, el Reglament General de Protecció de Dades (RGPD)¹⁸ i diversos textos en matèria de drets humans i drets fonamentals.

Ara bé, amb aquesta nova versió del model no només es formalitzen els principis ètics com a criteris legals en base a normativa, sinó que s'inclou literatura acadèmica, recomanacions i *toolkits* de diversos organismes i entitats especialitzades, condensats en el **Model PIO**, que reclamen per a l'ús responsable i segur de la intel·ligència artificial.

Partint d'aquesta base, i amb la intenció que el **Model PIO** pugui ser utilitzat com una autèntica eina de verificació normativa, en aquest informe no només s'actualitzen i incloent les referències legals a les preguntes ja existents, sinó que també se n'inclouen de noves que donen resposta a les novetats introduïdes per la **AI Act**, no contemplades fins ara a l'informe. És per aquest motiu que, en el qüestionari contingut en aquest informe, trobareu les qüestions incloses a l'antiga versió del **Model PIO**, juntament amb una extensa bateria de qüestions noves, juntament amb la seva referència al text normatiu i l'enllaç directe per a consultar l'article exacte que inspira la qüestió.

¹⁷ Comissió Europea (2022) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). Disponible a: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf (consultada el 20 de març de 2023).

¹⁸ Parlament Europeu i Consell de la UE. Regulation (Eu) 2016/679 Of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (consultada el 20 de març de 2023).

3.2. Un model basat en drets

La constant integració de sistemes d'IA a la nostra vida quotidiana augmenta el possible impacte d'aquesta tecnologia en els drets de les persones. Per aquest motiu, més enllà de l'adopció de principis ètics i la regulació del mercat, és necessari incorporar una perspectiva basada en els drets.

Importants organismes de promoció i protecció dels DDHH, com les Nacions Unides i el Consell d'Europa, ja han alertat sobre els perills que la IA pot suposar pels drets més essencials, i quines precaucions s'haurien d'adoptar per tal de garantir que aquesta tecnologia es converteix en una eina en favor de la humanitat, i no en contra d'ella¹⁹.

En el discurs pronunciat per Volker Türk a la Cimera sobre Intel·ligència Artificial Generativa i Drets Humans del passat 30 de novembre de 2023, l'Alt Comissari de les Nacions Unides per als Drets Humans recordava que la urgència d'assolir una governança de la IA basada en els DDHH. Governança que, segons precisava l'Alt Comissari, *“ha de ser capaç de promoure una conducta empresarial responsable i la rendició de comptes pels danys als quals contribueixen les empreses”*²⁰. Al seu torn, les institucions europees, alhora que desenvolupen la **AI Act**, exigeixen el respecte dels drets fonamentals recollits a la Carta de drets fonamentals de la UE²¹.

Paral·lelament, aquestes entitats han manifestat la urgència d'adoptar el que l'ACNUDH ha anomenat *“aproximació de dades basada en els drets humans”* (HRBAD, per les seves sigles en anglès)²². La qüestió de les dades està íntimament lligada a la IA, ja que són necessàries per a l'entrenament i funcionament dels sistemes. Per aquesta raó, és imprescindible prendre en consideració les reclamacions de les organitzacions expertes en DDHH sobre la matèria quan s'avalua un sistema d'IA.

Un marc de drets humans dissenyat i aplicable a la IA permetria proporcionar una base per a desenvolupar legislació en la matèria, inspirar noves definicions de drets relacionats amb l'ús d'aquesta tecnologia, i facilitar la mobilització dels moviments socials implicats en la qüestió²³.

El gener de 2023, el Comitè sobre Intel·ligència Artificial del Consell d'Europa (CoE) va començar a treballar en un conveni sobre drets humans i IA, fent públic el projecte de conveni marc el 18 de desembre de 2023.

¹⁹ Comissari per als Drets Humans del Consell d'Europa (2023) Artificial intelligence and human rights. Disponible a: <https://www.coe.int/en/web/commissioner/thematic-work/artificial-intelligence> (consultada el 7 de desembre de 2023).

²⁰ ONU (2023) La inteligencia artificial requiere una gobernanza basada en los derechos humanos. Disponible a: <https://news.un.org/es/story/2023/11/1526062> (consultada el 7 de desembre de 2023).

²¹ Parlament Europeu, Consell de la UE i Comissió. Carta de drets fonamentals de la UE, de 7 de desembre del 2000 (2000/C 364/01). Disponible a: https://www.europarl.europa.eu/charter/pdf/text_es.pdf (consultada el 20 de setembre de 2023).

²² ACNUDH (2018) A human rights-based approach to data: leaving no one behind in the 2030 Agenda for Sustainable Development. Disponible a: <https://shorturl.at/drR0o> (consultada el 20 de novembre de 2023).

²³ Bakiner, O. (2023) The promises and challenges of addressing artificial intelligence with human rights. Disponible a: <https://journals.sagepub.com/doi/full/10.1177/20539517231205476> (consultada el 15 de novembre de 2023).

Finalment, el 17 de maig de 2024 es va adoptar la versió definitiva del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret²⁴, convertint-se en el primer tractat internacional a establir normes vinculants en matèria d'IA. Aquest text és una important fita, ja que marca l'inici del desenvolupament d'un corpus jurídic específic en matèria de DDHH i IA, i permetrà completar el règim legal de la **AI Act**²⁵.

El Consell d'Europa és la principal organització internacional que vetlla per la promoció i protecció dels drets humans a Europa. Tot i la similitud entre el seu nom i el d'algunes institucions de la Unió Europea es tracta d'una organització independent amb un funcionament diferent. Ara bé, tots els membres de la UE ho són també del Consell d'Europa i ambdues organitzacions col·laboren estretament en les matèries comunes.

A més dels 27 Estats de la UE, el CoE compta amb 19 membres més. Si bé és cert que les convencions desenvolupades pel Consell d'Europa no són d'obligat compliment per tots els estats membres, sinó que és necessari que cadascun ratifiqui la convenció perquè cobri caràcter vinculant al seu territori, el Conveni marc ofereix un major abast d'aplicació territorial.

En qualsevol cas, a partir de les facultats que li han estat conferides per negociar i adoptar convenis en nom dels seus membres, la UE ha participat de manera activa en el desenvolupament del Conveni marc²⁶. En conseqüència, el seu contingut esdevindria obligatori en tot el territori comunitari. A més, l'article 31 del Conveni permet que el Comitè de Ministres del Consell d'Europa convidi a un estat no membre a signar-ho. D'aquesta manera, s'obre la porta a que el contingut del Conveni sigui d'aplicació més enllà del continent europeu.

D'altra banda, els articles del Conveni marc són el resultat de l'opinió experta del Comitè en intel·ligència artificial. Per tant, ofereix una important guia per establir paràmetres de drets humans aplicables a la IA que permetran una interpretació garant dels preceptes contemplats a la **AI Act** i a qualsevol altre norma aplicable als sistemes d'IA i el seu ús.

Els principis ètics en el que es vertebrava el **Model PIO**, estan estretament lligats amb els criteris aplicables a la IA i la governança de dades en matèria de drets. En aquest informe, hem volgut reflectir aquesta realitat de la següent manera: en primer lloc, hem inclòs dins de l'apartat de justificació que acompanya cada pregunta del qüestionari referències directes a algunes de les normes internacionals i comunitàries més rellevants en matèria de DDHH i DDDFF en les que es fonamenten les preguntes del model. En segon lloc, hem volgut explicar com cadascun dels principis que vertebrava el **Model PIO** es relacionen amb els textos jurídics que citem.

²⁴ Comitè sobre Intel·ligència Artificial del Consell d'Europa (2024) Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. Disponible a: <https://rm.coe.int/1680afae3c> (consultada el 20 de maig de 2024).

²⁵ Roekens, N. (2014) The Convention on AI and Human Rights that no one talks about. Disponible a: <https://www.linkedin.com/pulse/convention-ai-human-rights-one-talks-nele-roekens-6zzjf> (consultada el 16 de gener de 2024).

²⁶ Servei d'Acció Exterior de la UE (2023) Important advancements from Strasbourg and Brussels on first binding rules for Artificial Intelligence. Disponible a: https://www.eeas.europa.eu/delegations/council-europe/important-advancements-strasbourg-and-brussels-first-binding-rules-artificial-intelligence_en?s=51 (consultada el 19 de desembre de 2023).

A part del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, ens hem remès a la Declaració universal dels drets humans²⁷; el Pacte internacional de drets civils i polítics²⁸; el Pacte internacional de drets econòmics, socials i culturals²⁹; el Conveni europeu de drets humans³⁰; la Carta de drets fonamentals de la Unió Europea; i la Carta social europea³¹.

Aquesta selecció representa alguns dels textos més rellevants dins dels sistemes universal i europeu de drets humans, i estableixen els paràmetres de respecte a la dignitat humana que posteriorment han servit per al desenvolupament de normes més específiques. La Convenció sobre l'eliminació de totes les formes de discriminació contra les dones, per exemple, explica en el seu preàmbul que el tractat va ser adoptat amb la finalitat de promoure el dret a la no discriminació proclamat a Declaració universal dels drets humans i a l'obligació de garantir la igualtat entre dones i homes contemplada als pactes internacionals de drets humans³². De fet, a excepció de la Carta de drets fonamentals de la UE, el Conveni marc cita totes les normes que hem esmentat *supera* en el seu preàmbul.

Nogensmenys, els sistemes d'IA han de contemplar tots els drets reconeguts a les persones que poden patir l'impacte del seu ús, incloent-hi tota la normativa internacional, europea i domèstica, i no limitar-se al contingut dels drets continguts a les normes que citem, ja que aquestes només suposen els estàndards mínims de respecte a la dignitat humana.

Per aquest motiu, a part d'aquesta legislació bàsica hem contemplat alguns textos jurídics que reconeixen drets específics en matèria de governança de dades, tals com el Conveni 108 del Consell d'Europa per a la protecció de les persones respecte al tractament automatitzat de dades de caràcter personal³³ o el RGPD.

També ens hem referit a la Resolució 48/13, de 8 d'octubre de 2021 del Consell de Drets Humans de les Nacions Unides³⁴, mitjançant la qual Consell de Drets Humans va reconèixer per primer

²⁷ Assemblée General de les Nacions Unides (1948) Declaració Universal dels Drets Humans. Disponible a: <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (consultada el 12 de novembre de 2023).

²⁸ Assemblée General de les Nacions Unides (1966) Pacte Internacional de Drets Civils i Polítics. Disponible a: https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf (consultada el 8 de novembre de 2023).

²⁹ Assemblée General de les Nacions Unides (1966) Pacte internacional de drets econòmics, socials i culturals. Disponible a: <https://www.ohchr.org/sites/default/files/cescr.pdf> (consultada el 8 de novembre de 2023).

³⁰ Consell d'Europa (1950) Conveni europeu de drets humans, modificat per les disposicions del Protocol n° 15 (STCE n° 213) a partir de la seva entrada en vigor l'1 d'agost del 2021 i del Protocol n° 14 (STCE n° 194) a partir de la seva entrada en vigor l'1 de Juny de 2010. Disponible a: https://www.echr.coe.int/documents/d/echr-convention_ENG (consultada el 20 de setembre).

³¹ Consell d'Europa. Carta social europea (revisada) el 3 de maig 1996. Disponible a: <https://rm.coe.int/168047e013> (consultada el 20 de setembre).

³² Assemblée General de les Nacions Unides (1979) Convenció sobre l'eliminació de totes les formes de discriminació contra la dona. Disponible a: <https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/cedaw.pdf> (consultada el 14 de desembre de 2023).

³³ Consell d'Europa (1981) Conveni per a la Protecció de les Persones Respecte al Tractament Automatitzat de Dades de Caràcter Personal, fet a Estrasburg el 28 de gener de 1982. Disponible a: <https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447> (consultada el 15 de setembre de 2023).

³⁴ Consell de Drets Humans de les Nacions Unides (2021) Resolució A/HRC/48/L.23/Rev.1: El dret humà a un medi ambient sense riscos, net, saludable i sostenible. Disponible a:

cop a nivell internacional el medi ambient saludable com a dret humà. Aquest document no gaudeix de força jurídica, sinó política. No obstant, resulta una resolució important que cerca el compromís de tots els estats per treballar de manera conjunta i coordinada per a combatre la degradació mediambiental i el canvi climàtic, posant en el centre la protecció de la persona³⁵.

Malgrat que la IA sovint pot ser percebuda com quelcom intangible, la realitat és que aquesta depèn d'una sèrie de recursos (*AI compute*) que inclou estructura física, hardware, i software, els quals requereixen energia i altres recursos³⁶. La creixent demanda d'IA, especialment durant el 2023 i 2024, es tradueix en potencial creixement significatiu de la petjada energètica. De fet, s'estima que el 2027 els servidors d'IA podrien arribar a consumir entre 85,4 i 134,0 terabits d'energia per hora³⁷. Aquesta xifra s'aproxima a la despesa d'energia d'Argentina, Països Baixos o Suècia en un any, i representa el 0,5% de l'ús d'electricitat global³⁸.

Per tant, la valoració de qualsevol sistema d'IA des d'una perspectiva de drets, necessàriament ha d'incloure l'avaluació de l'impacte que l'ús i el desenvolupament aquest tipus de tecnologia pot suposar sobre el medi ambient.

Cal afegir que l'enfocament de drets, més enllà de preveure, mitigar i reparar els riscos i lesions produïts pels sistemes d'IA, permet posar la intel·ligència artificial al servei de les persones, reforçant els seus drets. En aquest sentit, s'ha explorat com la IA podria utilitzar-se per a combatre l'abús infantil en línia³⁹, o el tràfic d'éssers humans⁴⁰, per posar un parell d'exemples.

<https://digitallibrary.un.org/record/3983329?ln=fr&ln=%5B%22%5B%27en%27%5D%22%5D&v=pdf> (consultada el 7 de desembre de 2023).

³⁵ Castilla Juárez, K. (2022) El dret humà: tard o insuficient? Disponible a: <https://www.idhc.org/es/publicaciones/el-derecho-humano-al-medioambiente-tarde-e-insuficiente.php> (consultada el 22 de gener de 2023).

³⁶ OCDE (2022) Mesurant l'impacte ambiental de la computació i les aplicacions d'Intel·ligència Artificial. Disponible a: <https://www.oecd-ilibrary.org/docserver/7babf571-en.pdf?expires=1703161916&id=id&accname=quest&checksum=D9D870FC7CF0D306C078BEA8B4E1F1AC> (consultada el 13 de desembre de 2023).

³⁷ De Vries, A. (2023) La creixent empremta energètica de la Intel·ligència Artificial. Disponible a: [https://www.cell.com/joule/fulltext/S2542-4351\(23\)00365-3](https://www.cell.com/joule/fulltext/S2542-4351(23)00365-3) (consultada el 22 de desembre de 2023).

³⁸ Erdenesanaa, D. (2023) La Intel·ligència Artificial podria necessitar aviat tant electricitat com tot un país. Disponible a: <https://www.nytimes.com/2023/10/10/climate/ai-could-soon-need-as-much-electricity-as-an-entire-country.html> (consultada el 22 de desembre de 2023).

³⁹ Comissió Europea (2020) Exploració potencial de la IA en la lluita contra l'abús de menors en línia. Disponible a: <https://digital-strategy.ec.europa.eu/en/library/exploring-potential-ai-fight-against-child-online-abuse> (consultada el 23 de desembre de 2023).

⁴⁰ Calaway, A. (2021) Intel·ligència artificial i lluita contra la tracta d'éssers humans. Disponible a: <https://www.business-humanrights.org/es/blog/artificial-intelligence-and-the-fight-against-human-trafficking/> (consultada el 23 de desembre de 2023).

En tot cas, el que queda clar és que les empreses juguen un rol cabdal en l'adopció d'un enfocament de la IA basat en drets. En virtut del dret internacional, així com de les seves cartes magnes⁴¹, els estats tenen l'obligació de protegir a les persones de les vulneracions de drets que tenen lloc al seu territori, incloent-hi aquelles que comeses per empreses⁴².

Així mateix, l'ACNUDH ha declarat que la responsabilitat de respectar els drets humans és un estàndard global aplicable per a totes les empreses independent del compliment per part dels estats de les seves pròpies obligacions, i que existeix més enllà de l'ajustament a la normativa domèstica⁴³. Això és, les empreses també tenen el deure de garantir i respectar els drets humans, i el seu compliment no queda condicionat per les accions de l'estat on es troben ni l'existència de normativa interna, sinó que és una obligació pròpia i independent.

Aquesta obligació s'estén a tots els àmbits, inclosa la intel·ligència artificial. En conseqüència, les empreses que desenvolupen, comercialitzen o utilitzen un sistema d'IA, haurien de prendre mesures per promoure els drets de les persones afectades pel seu sistema, preveure els riscos que se'n deriven, i establir eines que permetin la reparació dels danys que puguin ser causats. A tal fi, és recomanable comptar amb una avaluació d'impacte sobre drets humans, com per exemple el model proposat per Alessandro Mantelero⁴⁴. Similarment, l'Organització per a la Cooperació i el Desenvolupament Econòmic (OCDE) ha establert recomanacions sobre com aplicar les seves directrius la *due diligence* en matèria de drets humans en l'àmbit de la IA⁴⁵.

En aquest sentit, el **Model PIO** resulta un instrument de gran utilitat que les empreses, o altres entitats, poden emprar per a valorar el grau d'adequació del seu sistema d'IA als drets que inspiren els nostres **7 principis**:

- | | |
|---|--------------------|
| (1) Transparència i explicabilitat | (5) Privacitat |
| (2) Justícia i equitat | (6) Autonomia |
| (3) Seguretat i no maleficència | (7) Sostenibilitat |
| (4) Responsabilitat i retiment de comptes | |

⁴¹ [L'article 10 de la Constitució espanyola](#) proclama la dignitat humana i els drets que li són inherents com a fonament de l'ordre polític i de la pau social, al mateix que proclama que els drets i llibertats fonamentals reconeguts a la Constitució hauran de ser interpretats de conformitat amb la Declaració Universal dels Drets Humans.

⁴² ACNUDH (2023) OHCHR i les empreses i els drets humans. Disponible a: <https://www.ohchr.org/en/business-and-human-rights> (consultada el 23 de desembre de 2023).

⁴³ ACNUDH (2011) Principis rectors sobre les empreses i els drets humans. Disponible a: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (consultada el 23 de desembre de 2023).

⁴⁴ Mantelero, A. (2022) Avaluació de l'impacte dels Drets Humans i la IA. Disponible a: https://link.springer.com/chapter/10.1007/978-94-6265-531-7_2 (consultada el 20 de novembre de 2023).

⁴⁵ OCDE (2021) OECD Perspectives empresarials i financeres 2021: IA en els negocis i finances. Disponible a: <https://www.oecd-ilibrary.org/sites/31e7edcc-en/index.html?itemId=/content/component/31e7edcc-en> (consultada el 23 de desembre de 2023).

4. JUSTIFICACIÓ

La IA té un impacte social d'unes magnituds tals que requereix regulació específica. Aquest és el repte en el qual les institucions europees i els estats membres de la Unió Europea fa anys que hi treballen, i es tradueix en la **AI Act** i les reformes que l'acompanyen, així com la normativa complementària i desenvolupadora de la matèria.

Aquesta voluntat reguladora respon a la necessitat de dotar de seguretat jurídica situacions noves que no encaixen amb la normativa existent fins ara. Altres matèries que van tenir un impacte social elevat també van comptar amb normativa per a poder adequar-la a la societat i garantir el respecte dels drets reconeguts i la correcta articulació de tots els agents implicats.

Un exemple és la descoberta de matèries transgèniques als aliments, que va donar lloc a que l'any 2001 es publicués la Directiva 2001/18/CE del Parlament Europeu i del Consell sobre l'alliberament intencional en el medi ambient d'organismes modificats genèticament, la qual va ser modificada el 2008 i al 2015. Posteriorment, aquesta matèria va continuar desenvolupant-se amb diversos reglaments del 2003: sobre els pinsos i aliments modificats genèticament⁴⁶; sobre el moviment transfronterer d'aquests organismes⁴⁷; sobre la traçabilitat en l'etiquetatge d'aliments modificats⁴⁸; i al 2004 per a desenvolupar les anteriors qüestions sobre autoritzacions dels nous aliments i pinsos modificats⁴⁹

Aquesta regulació va continuar desenvolupant-se amb la Directiva del 2009 sobre la utilització confinada de microorganismes modificats genèticament⁵⁰; el Reglament de 2011 elaborat per la Comissió per a establir i harmonitzar els mètodes de mostreig i anàlisi per al control oficial de

⁴⁶ Parlament Europeu i Consell de la UE (2003) Reglament (CE) 1829/2003 del Parlament Europeu i del Consell, de 22 de setembre de 2003, sobre aliments i pinsos modificats genèticament. Disponible a: <https://eur-lex.europa.eu/eli/reg/2003/1829/oj> (consultada el 20 de maig de 2024).

⁴⁷Parlament Europeu i Consell de la UE (2003) Reglament (CE) 1946/2003 del Parlament Europeu i del Consell, de 15 de juliol de 2003, sobre els moviments transfronterers d'organismes modificats genèticament. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32003R1946> (consultada el 20 de maig de 2024).

⁴⁸Parlament Europeu i Consell de la UE (2003) Reglament (CE) 1830/2003 del Parlament Europeu i del Consell, de 22 de setembre de 2003, relatiu a la traçabilitat i l'etiquetatge dels organismes modificats genèticament i la traçabilitat dels aliments i pinsos produïts a partir d'organismes modificats genèticament i pel qual es modifica la Directiva 2001/18/CE. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003R1830> (consultada el 20 de maig de 2024).

⁴⁹ Parlament Europeu i Consell de la UE (2003) 641/2004 de la Comissió, de 6 d'abril de 2004, sobre les normes de desenvolupament del Reglament (CE) núm. 1829/2003 del Parlament Europeu i del Consell, pel que fa a la sol·licitud d'autorització de nous aliments i pinsos modificats genèticament, la notificació de productes existents i la presència accidental o tècnicament inevitable de material modificat genèticament l'avaluació de risc del qual hagi estat favorable. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003R1830> (consultada el 20 de maig de 2024).

⁵⁰ Parlament Europeu i Consell de la UE (2009) Directiva 2009/41 del Parlament Europeu i del Consell, de 6 de maig de 2009, sobre la utilització confinada de microorganismes modificats genèticament. Disponible a: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32009L0041> (consultada el 21 de maig de 2024).

pinso⁵¹; el Reglament de 2013 d'execució sobre la matèria del Reglament anterior⁵²; i finalment, també la normativa no vinculant elaborada en la matèria com són les diverses recomanacions així com protocols.

A més, la regulació en matèria europea implica el desplegament de normativa pròpia a cada estat, i per això, destaquem la Llei 9/2003, de 25 d'abril per la qual s'estableix el règim jurídic de la utilització confinada, alliberament voluntari i comercialització d'organismes modificats genèticament i ha estat desenvolupada en diferents Reials Decrets de l'any 2004, 2013, 2017 i 2019. Així com el Decret 62/2015, de 28 d'abril, pel qual s'estableixen mesures per a l'exercici de les competències de la Generalitat de Catalunya en matèria dels organismes modificats genèticament.

Una altra matèria que també va comptar amb una regulació extensa ha estat l'erradicació de l'amiant com a agent químic utilitzat àmpliament en la construcció i indústria fins a l'any 2002 que es va fer efectiva la prohibició del seu ús, producció i comercialització. El Parlament Europeu va elaborar una Resolució el 2013 sobre els riscos que causa a la salut en el lloc de treball i la perspectiva d'eliminació de tot l'amiant existent. Destaquem també el Dictamen del Comitè Econòmic i Social Europeu de l'any 2015 sobre l'erradicació en l'àmbit de la UE per assolir l'objectiu a finals del 2032. Amb aquest context, també ressaltem l'Acord de Govern de la Generalitat de Catalunya, el 21 de març pel qual s'aprova el Pla nacional per a l'erradicació de l'amiant a Catalunya 2023-2032.

Com ja vam establir a l'informe previ, el **Model PIO** no proporciona un instrument legal d'autoavaluació, sinó que les organitzacions gaudeixen de flexibilitat per triar com s'hi acosten. Nogensmenys, és important començar a reflexionar al voltant del *compliance* i estàndards concrets de millora que permetin implementar els principis ètics en les dades i sistemes d'IA. La IA és un ventall que aglutina moltes tecnologies relacionades, algunes de les quals estan tenint un progrés molt notable però accelerat. Des de la publicació del **Model PIO** de l'**OEIAC**, en pocs mesos, aquesta acceleració s'ha produït de manera extraordinària, per exemple, amb la irrupció del *ChatGPT* (ara ja basat en el GPT-4).

Els potencials impactes negatius d'aquestes tecnologies han de poder identificar-se, prevenir-se i solucionar-se amb l'ajut d'una regulació basada en principis ètics—normatius amb l'objectiu de descoratjar o eliminar la innovació, sinó de millorar-la a través de mitjans tècnics i socio-jurídics que garanteixin el compliment de certes obligacions⁵³.

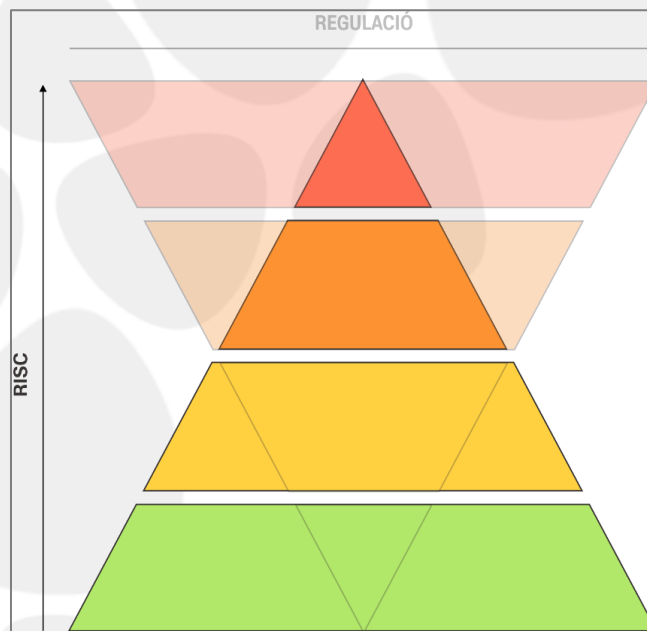
⁵¹Parlament Europeu i Consell de la UE (2011) Reglament 1169/2011 del Parlament Europeu i del Consell, del 25 d'octubre, elaborat per la Comissió per a establir i harmonitzar els mètodes de mostreig i anàlisi per al control oficial de pinso. Disponible a: <https://shorturl.at/Tx00a> (consultada el 21 de maig de 2024).

⁵²Parlament Europeu i Consell de la UE (2011) Reglament d'execució 1137/2013 de la Comissió, de 13 de desembre, s'estableixen disposicions d'aplicació del Reglament (UE) n° 1169/2011 del Parlament Europeu i del Consell relatiu a les indicacions del país d'origen o el lloc de procedència per a la carn fresca, refrigerada o congelada de porc, ovella, cabra i aus de corral. Disponible a: <https://shorturl.at/ZIGqM> (consultada el 21 de maig de 2024).

⁵³Theodorou, A. & Dignum, V. (2020) Cap a una governança ètica i sociojurídica de la IA. Disponible a: <https://www.nature.com/articles/s42256-019-0136-y> (consultada el 20 de novembre de 2023).

Així el *compliance* fa referència a un paradigma multitasca de diferents instruments que podem utilitzar per avaluar els sistemes d'IA d'una manera específica que connecti obligacions, drets i principis tant tècnics com jurídics.⁵⁴ D'aquesta manera, des de la informàtica podem avaluar els sistemes d'IA basant-nos en la correcció de les seves decisions, i des de la regulació jurídica podem introduir obligacions envers les persones desenvolupadores, comercialitzadores i usuàries d'aquests sistemes que garanteixin la transparència; la correcta gestió de dades; la no discriminació; la seguretat i el control de qualitat del sistema, entre d'altres.

En aquest sentit, l'actualització del **Model PIO** es basa en aquest paradigma de *compliance* multitasca, prenent com a referència la literatura especialitzada a nivell ètic i tècnic per tal d'aprofundir i aclarir els principis que orienten el qüestionari, i com a marc regulador i jurídic les propostes legislatives de la Comissió Europea, que justifiquen diversos dels esmentats principis sòcio-tècnics i ofereixen definicions comunes sobre els sistemes d'IA.



Il·lustració 2 Piràmide de risc i grau de regulació de la IA Act.

Nogensmenys, cal aclarir que la **AI Act** és una legislació limitada respecte a la regulació dels sistemes d'IA amb base als riscos.

Això vol dir que principalment l'objectiu és regular aquells sistemes d'IA que el propi instrument determina com d'alt risc, així els que no ho són considerats (i no són expressament prohibits, com per exemple els sistemes de puntuació social) són objecte d'una regulació molt més limitada; o bé, en el cas dels sistemes categoritzats de risc mínim que compten amb una regulació més laxa.

En aquest sentit, hem d'incidir en què el **Model PIO** no pot avaluar sistemes que es troben expressament prohibits per la legislació, no obstant si que es proposa com una eina d'avaluació

⁵⁴ Hacker, P., Naumann, F., Friedrich, T., Grundmann, S., Lehmann, A., & Zech, H. (2022) Compliment de la normativa sobre IA: el repte d'unir la ciència de les dades i el dret. Disponible a: <https://dl.acm.org/doi/10.1145/3531532> (consultada el 12 de setembre de 2023).

transversal que pot ser útil, fins i tot per verificar tot tipus de sistemes d'IA inclosos i també aquells que no siguin considerats d'alt risc a la legislació.

5. INSTRUCCIONS

Abans d'aprofundir en l'actualització del qüestionari, en aquest capítol s'exposaran les instruccions a seguir per tal de completar el qüestionari de manera òptima.

1	Prevaluació 1 Per saber si el sistema d'IA està considerat de risc inacceptable a partir de la normativa de la AI Act.
2	Prevaluació 2 Per classificar el sistema d'IA segons si el seu risc és alt, limitat o mínim d'acord amb la normativa de la AI Act.
3	Resultats de la prevaluació Permet posicionar als usuaris del Model PIO Obligacions i Drets sobre alguns dels principals requisits legals de la normativa de la AI Act.
4	Inici de l'avaluació A través d'una llista de verificació o "checklist" organitzat sobre la base de principis ètics, disposicions legals, recomanacions ètiques i exemples.
5	Recollida de dades Mitjançant la informació que proporcionen els usuaris del Model PIO a través de la llista de verificació o "checklist" sobre la base ètica i legal.
6	Obtenció de mètriques Adequació a les disposicions legals i recomanacions ètiques del Model PIO tenint en compte les categories de risc de la normativa de la AI Act.
7	Visualització de resultats A través d'una insígnia que reflecteix el grau d'assoliment dels principis ètics i disposicions legals contingudes en el Model PIO.

Il·lustració 3 Funcionament del Model PIO.

A continuació trobareu un circuit on es mostren els passos a seguir per tal de poder completar el qüestionari, seguidament es desplega una explicació de cadascun d'aquests, per tal que serveixin com a guia en el moment de completar l'avaluació.

0) Abans d'iniciar el procés d'avaluacions pròpiament, hi ha les 10 preguntes inicials o preguntes bàsiques que reflecteixen el contingut ètic essencial de les qüestions que conformen el **Model PIO**, i us permetran fer una primera aproximació, i així us situarà prenent consciència sobre els sistemes d'IA.

1) El procés s'inicia amb la fase de preavaluació on l'entitat efectua una primera distinció per saber si el seu sistema està categoritzat com a **risc inacceptable** d'acord amb la definició que en fa l'article 5 de la **AI Act** sobre aquells sistemes que són d'usos prohibits. Aquest us permetrà saber si el vostre sistema d'IA pot ser implementat legalment dins del territori de la UE. En cas que el vostre sistema coincideixi amb un dels usos prohibits no serà necessari que continuen amb la resta del formulari, ja que el **Model PIO** està destinat a aquells sistemes que poden ser efectivament comercialitzats i utilitzats d'acord amb la legalitat.

Pel contrari, si el vostre sistema no es troba entre els usos prohibits que se us han mostrat, continueu amb la segona part de la preavaluació, amb la qual coneixereu quin és el grau de risc d'entre tots els permesos que pertoca al vostre sistema d'IA d'acord amb la **AI Act**. En aquest cas se us presenta un breu llistat de preguntes dividides en dues taules.

2) La segona distinció que ha d'efectuar l'entitat és per a conèixer quina categoria de risc té associada el seu sistema d'acord amb la **AI Act**. Conèixer el grau de risc en el que es classifica el vostre sistema serà important en termes de compliment de la normativa, ja que depenent de llur classificació, la normativa preveu mesures més o menys restrictives.

Així doncs, la primera de les taules es basa en l'article 6 de la **AI Act**, relativa als sistemes **d'alt risc**. En cas que contesteu afirmativament a com a mínim una de les 7 preguntes aquesta serà la categoria de risc associada al vostre sistema.

La segona i tercera taules es basen en preguntes extretes dels articles 50 i següents de la **AI Act**. D'acord amb la classificació feta per la UE, les preguntes incloses en aquestes dues taules corresponen a sistemes de **risc limitat**. No obstant, dins d'aquesta categoria, trobem obligacions diferenciades en funció del tipus de sistema. Per aquest motiu, i amb la finalitat d'adaptar el qüestionari a la realitat específica de les persones que sostenen el seu sistema a la nostra avaluació, hem dividit aquesta categoria en sistemes de propòsit general (segona taula) i sistemes d'IA generativa (tercera taula).

En cas que no hagueu contestat afirmativament a cap de les preguntes contingudes a ambdues taules, el vostre sistema ha de ser catalogat de **risc mínim**. La **AI Act** no contempla cap articulat específic per als sistemes d'IA de risc mínim, tot i que podem extreure les referències de l'article 95 relatiu als codis de conducta per a l'aplicació voluntària de requisits específic previst per aquells sistemes diferents dels d'alt risc o naturalesa específica per poder així formular recomanacions.

3) D'aquesta segona distinció s'obté una **primera classificació** en una de les tres categories de risc segons la **AI Act** que permet a l'entitat obtenir un punt de partida per a conèixer millor el seu sistema.

4) Després de realitzar la preavaluació, s'iniciarà el formulari de **l'avaluació** que consisteix en un llistat de verificació o checklist organitzat seguint els set principis. Les preguntes que conformen el qüestionari són fruit de la suma de les obligacions extretes de la **AI Act** fonamentalment, i també d'altres textos normatius, així com de recomanacions ètiques i legals. A més, hi trobareu exemples a cada pregunta que us permetran concretar millor allò que s'està preguntant.

Cada pregunta s'ha de respondre en funció de si el vostre sistema compleix o no. Veureu que en algunes preguntes, també hi ha una tercera opció que és "no aplica" per aquells casos els quals en el vostre sistema d'IA no heu previst allò preguntant.

5) Totes les preguntes compten amb etiquetes en funció de la categoria de risc que té assignada aquella pregunta d'acord amb la justificació legal que es fonamenta.

Aquestes etiquetes són de tres tipus que correspon a les tres classificacions:

Alt ■ Limitat ■ Mínim ■

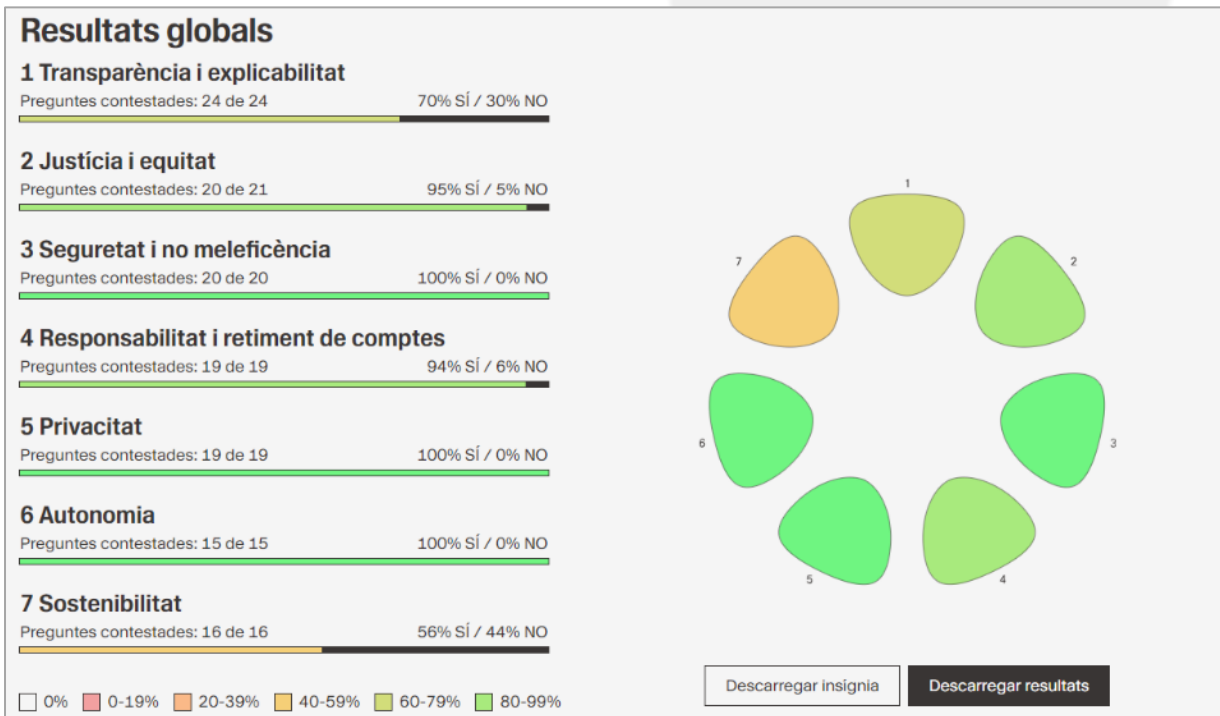
D'una banda, hem de destacar que algunes preguntes tenen assignada més d'una etiqueta, ja que és possible fonamentar-les en diversos textos legals i recomanacions ètiques i legals alhora.

D'altra banda, recordar que la categorització del risc limitat l'hem dividit d'acord amb la **AI Act** en sistemes d'IA generativa o de propòsit general o bé, sistemes de reconeixement d'emocions i identificació biomètrica, i per aquesta raó les preguntes que corresponen a aquesta categorització hi consta el símbol d'un asterisc (*).

6) La suma de respostes a totes les preguntes dona lloc a uns percentatges que atribueixen el grau d'adequació de cada principi i en general, l'avaluació dels sistemes i dades de la IA. Aquests percentatges es tradueixen en un conjunt de **mètriques** del sistema d'IA sotmès a l'avaluació pel **Model PIO Obligacions i Drets**.

Les mètriques obtingudes són el reflex de l'adequació o no del sistema d'IA que l'entitat ha sotmès a avaluació com que partim d'una confiança implícita en una declaració de responsabilitat sobre la informació donada.

7) En finalitzar l'avaluació s'atribueix una **insígnia** gràfica que és la suma de les mètriques obtingudes de les respostes donades la qual reflecteix l'adequació de manera percentual de l'entitat als requisits legals i estàndards ètics de cada principi del model. Aquests valors es recullen amb una escala de colors sent el color blanc representatiu del no aplica, el color verd l'assumpció total del principi, vermell la no assumpció i els tons verd clar, caqui, groc i taronja les opcions intermèdies.



Il·lustració 4. Resultats globals al finalitzar el **Model PIO** Obligacions i Drets.

A més de la insígnia, que es tracta de la resposta sintetitzada, es facilita la matriu de riscos que es tracta d'una eina per obtenir un resum visual del nivell de risc segons la severitat de la **AI Act** i la normativa amb relació a la probabilitat de portar a terme una acció al respecte. Aquesta probabilitat referent al temps poden ser cinc opcions: molt alta, ja que, l'efectueu aviat; alta perquè l'efectueu en un termini breu en temps sense ser immediat; ni alta ni baixa, ja que, compteu en realitzar-la en un mitjà termini; baixa perquè no forma part de les vostre prioritats, tot i que sou conscients que caldria efectuar-la; i molt baixa, ja que, no teníeu pensat dur-la a terme. Per tant, la taula recull les respostes negatives proporcionades segons la normativa i la probabilitat de dur a terme la qüestió sol·licitada a la pregunta que resumeix els punts de millora.

PROBABILITAT DE PORTAR A TERME UNA ACCIÓ	SEVERITAT SEGONS LA NORMATIVA O AI ACT		
	Mínima	Limitada	Alta
Molt alta	1	0	4
Alta	2	0	4
Ni alta ni baixa	1	0	0
Baixa	1	1	2
Molt baixa	0	0	0

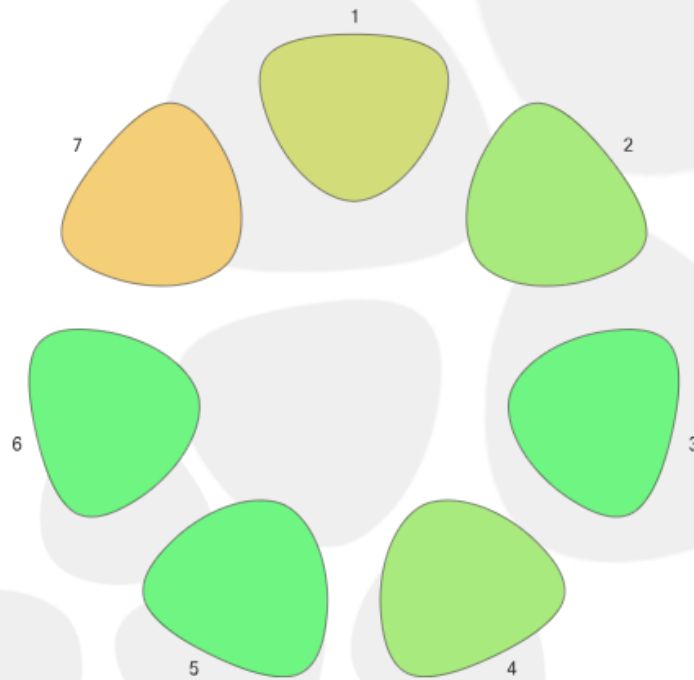
Il·lustració 5. Matriu de riscos del **Model PIO Obligacions i Drets**

Els punts de millora són totes les preguntes on heu contestat negativament i heu precisat el grau de severitat i probabilitat en la qual duríeu a terme aquella qüestió per tal, de contestar positivament. Novament, fem servir la mateixa gamma de colors abans explicada.

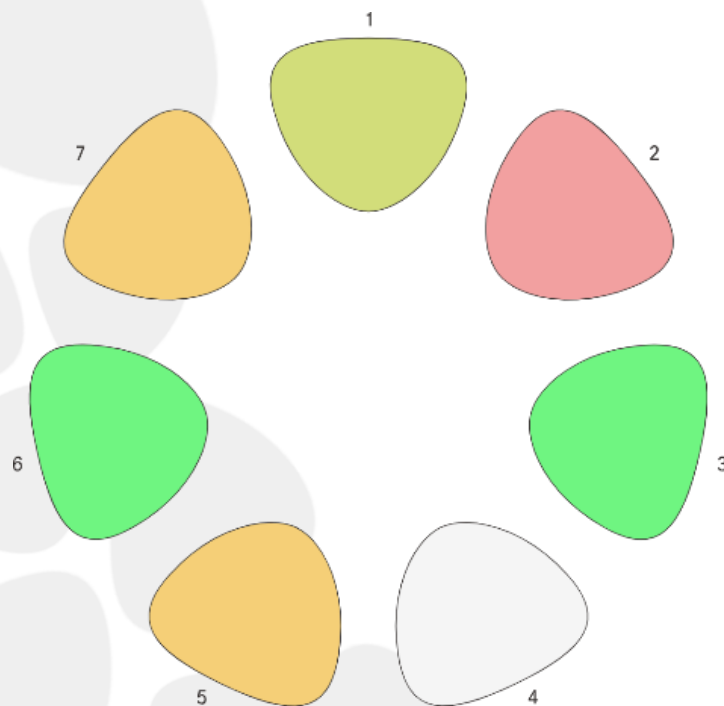
<p>2.1.1 Heu establert mesures d'inclusió i equitat com provar els resultats del vostre sistema d'IA per a diferents grups afectats?</p>	<p>Aquesta pregunta fa referència als articles 9, 10.3, 15.3, 27.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre <u>intelligència artificial (AI Act)</u>, relatiu a les mesures de gestió de riscos, la governança de dades, la resiliència i robustesa dels sistemes d'IA, l'avaluació d'impacte dels drets fonamentals per a sistemes d'IA d'alt risc i la promoció de codis de conducta d'aplicació voluntària per a persones o grups vulnerables.</p> <p>La pregunta també es relaciona amb els articles 10 i 16 del <u>Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret</u>, que versen sobre la Igualtat i no discriminació i el marc de gestió de riscos i impactes. Juntament amb el dret humà a no discriminació, consagrat a l'article 14 del <u>Conveni Europeu de Drets Humans</u>, l'article 21 de la Carta de Drets Fonamentals de la UE, l'article 26 del Pacte Internacional de Drets Civils i Polítics i l'article 7 de la Declaració Universal dels Drets Humans.</p> <p>A més, la pregunta també està relacionada a l'apartat <i>Specific safeguards to ensure non-discrimination when using de l'informe Getting The Future Right, Artificial Intelligence And Fundamental Rights</i> de la FRA.</p> <p>D'altra banda, la pregunta es fonamenta en l'apartat de <i>Fairness and non-discrimination</i> de les recomanacions sobre ètica en la <u>Intelligència Artificial d'UNESCO</u>, i està relacionada amb l'apartat <i>Fairness del AI Ethics Assessment</i> de GSMA.</p>
<p>2.1.2 Us heu assegurat que el vostre sistema d'IA no utilitza variables o "proxies" que poden ser injustament discriminatòries?</p>	<p>Aquesta pregunta fa referència als articles 9, 15.3, 27.1, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre <u>intelligència artificial (AI Act)</u>, relatiu a les mesures de gestió de riscos, la resiliència i robustesa dels sistemes d'IA, l'avaluació d'impacte dels drets fonamentals per a sistemes d'IA d'alt risc, les obligacions des proveïdors de sistemes de propòsit general de risc sistemàtic i la promoció de codis de conducta d'aplicació voluntària per a persones o grups vulnerables, i la promoció de codis de conducta d'aplicació voluntària per a persones o grups vulnerables.</p> <p>A més, la pregunta es fonamenta en l'article 10 del <u>Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret</u>, que versa sobre la Igualtat i no discriminació, així com el dret humà a la no discriminació, consagrat a l'article 14 del <u>Conveni Europeu de Drets Humans</u>, l'article 21 de la Carta de Drets Fonamentals de la UE, l'article 26 del Pacte Internacional de Drets Civils i Polítics i l'article 7 de la Declaració Universal dels Drets Humans.</p> <p>En aquest sentit, la pregunta també està relacionada amb l'apartat <i>Specific safeguards to ensure non-discrimination when using de l'informe Getting The Future Right, Artificial Intelligence And Fundamental Rights</i> de la FRA.</p> <p>Finalment, destaquem l'apartat de <i>Fairness and non-discrimination</i> de les recomanacions sobre ètica en la <u>Intelligència Artificial d'UNESCO</u> i l'apartat <i>Fairness del AI Ethics Assessment</i> de GSMA.</p>
<p>2.1.3 Heu avaluat si el vostre sistema d'IA s'adapta a un ampli espectre de preferències i habilitats individuals, incloent-hi usuaris que requereixen tecnologies d'assistència?</p>	<p>Aquesta pregunta fa referència a l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre <u>intelligència artificial (AI Act)</u>, relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria d'accessibilitat.</p> <p>A més, la pregunta es fonamenta en l'article 10 del <u>Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret</u>, que versa sobre la Igualtat i no discriminació, així com el dret humà a la no discriminació, consagrat a l'article 14 del <u>Conveni Europeu de Drets Humans</u>, l'article 21 de la Carta de Drets Fonamentals de la UE, i l'article 26 del Pacte Internacional de Drets Civils i Polítics.</p> <p>Destaquem també les recomanacions contingudes a l'apartat de <i>Diversity, Non-discrimination and Fairness: Accessibility and Universal Design</i> d'ALTAI, i està relacionada amb l'apartat <i>Fairness del AI Ethics Assessment</i> de GSMA.</p>

Il·lustració 6. Punts de millora del **Model PIO Obligacions i Drets**.

Finalment, tota aquesta informació detallada per a cadascun dels principis i el percentatge assolit d'aquest el rebreu a l'adreça de correu de registre mitjançant un informe i la insígnia descarregable.



*Il·lustració 7. Exemple 1 d'insígnia obtinguda al finalitzar el **Model PIO** Obligacions i Drets.*



*Il·lustració 8. Exemple 2 d'insígnia obtinguda al finalitzar el **Model PIO** Obligacions i Drets.*

6. LES 10 PREGUNTES INICIALS O BÀSIQUES

A la següent taula trobareu un llistat de qüestions que hem anomenat “10 preguntes inicials o bàsiques”. Les 10 preguntes reflecteixen el contingut ètic essencial de les qüestions que conformen el **Model PIO**, i us permetran fer una primera aproximació abans d’iniciar-lo.

10 preguntes inicials
Sabeu quin és el problema que esteu intentant resoldre amb l’ús d’un sistema d’IA?
Us heu plantejat si és necessari utilitzar un sistema d’IA per resoldre aquest problema?
Heu considerat els beneficis que aportarà l’ús d’un sistema d’IA i si aquests superen els riscos que planteja?
Sabeu explicar de quina manera el sistema d’IA resoldrà el problema o objectiu concret d’una manera comprensible?
Heu establert mecanismes per evitar que el sistema d’IA no s’exploti de manera maliciosa?
Sou conscients del vostre grau de responsabilitat respecte els possibles perjudicis d’utilitzar un sistema d’IA?
Utilitzeu dades d’una forma que es garanteixen drets fonamentals com el dret a la privadesa i els drets d’autoria?
Sabeu que un sistema d’IA ha d’augmentar capacitats però, en cap cas, limitar l’autonomia de les persones i la seva presa de decisions?
Teniu en compte que la sobreestimació de les capacitats d’un sistema d’IA contribueix a la desinformació tècnica i comercial?
Coneixeu l’impacte ambiental com la petjada de carboni associada a l’ús del sistema d’IA?

7. ACTUALITZACIÓ DEL QÜESTIONARI

A continuació detallem les actualitzacions de cada pregunta, classificades per principi, afegint la font exacta en la qual es basa i una referència específica dins de la legislació, així com les noves preguntes dissenyades en base al contingut de la nova normativa.

1. TRANSPARÈNCIA I EXPLICABILITAT																							
Anàlisi preliminar de l'ús del sistema (6)						Explicabilitat (9)									Traçabilitat i representativitat (5)					Protocols de comunicació (4)			
1.1.	1.2.	1.3.	1.4.	1.5.	1.6.	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.	3.1.	3.2.	3.3.	3.4.	3.5.	4.1.	4.2.	4.3.	4.4.
■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
2. JUSTICIA I EQUITAT																							
Inclusió i diversitat (10)										Identificar i mitigar biaixos (11)													
1.1.	1.2.	1.3.	1.4.	1.5.	1.6.	1.7.	1.8.	1.9.	1.10.	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.	2.10.	2.11.			
■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		
3. SEGURETAT I NO MALEFICIÈNCIA																							
Funcionament del sistema (5)					Traçabilitat per a la gestió del risc (9)									Mecanismes de seguretat (4)				Protecció enfront d'atacs (2)					
1.1.	1.2.	1.3.	1.4.	1.5.	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.	3.1.	3.2.	3.3.	3.4.	4.1.	4.2.				
■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■				
4. RESPONSABILITAT I RETIMENT DE COMPTE																							
Control (6)						Retiment de comptes (4)				Figures de protecció (3)			Capacitats de la IA (2)		Promoció d'IA responsable (4)								
1.1.	1.2.	1.3.	1.4.	1.5.	1.6.	2.1.	2.2.	2.3.	2.4.	3.1.	3.2.	3.3.	4.1.	4.2.	5.1.	5.2.	5.3.	5.4.					
■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■					
5. PRIVACITAT																							
Protecció de la privacitat (11)											Governança de dades (8)												
1.1.	1.2.	1.3.	1.4.	1.5.	1.6.	1.7.	1.8.	1.9.	1.10.	1.11.	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.					
■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■					
6. AUTONOMIA																							
Impacte en la capacitat dels usuaris (7)								Percepció del sistema (8)															
1.1.	1.2.	1.3.	1.4.	1.5.	1.6.	1.7.	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.									
■	■	■	■	■	■	■	■	■	■	■	■	■	■	■									
7. SOSTENIBILITAT																							
Desenvolupament sostenible (7)										Impacte ambiental (9)													
1.1.	1.2.	1.3.	1.4.	1.5.	1.6.	1.7.	2.1.	2.2.	2.3.	2.4.	2.5.	2.6.	2.7.	2.8.	2.9.								
■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■								

Taula 1 Categories de risc relacionades per cadascuna de les preguntes del Model PIO

7.1. Preavaluació

Com s'ha explicat, la **AI Act** ha optat per una aproximació del risc, en base a la qual es determinen diferents obligacions pels sistemes que corresponen a una categoria o l'altra. Com a conseqüència, no totes les preguntes del qüestionari reflecteixen requisits d'obligatori compliment per tots els sistemes d'IA, sinó que serà la naturalesa del vostre sistema la que determinarà quines resulten rellevants en el vostre cas. Per aquesta raó, amb l'actualització del qüestionari s'ha inclòs una preavaluació que us permetrà saber, en primer lloc, si el vostre sistema pot ser desenvolupat, comercialitzat i utilitzat d'acord amb la legalitat; i, en cas que així sigui, quin és el nivell de risc que se li associa d'acord amb la **AI Act**.

Nogensmenys, les obligacions de respecte i garantia de drets humans i fonamentals que venen imposades pel compliment de la normativa internacional i comunitària són aplicables a tots els sistemes, independentment de quin nivell de risc se'ls reconegui.

7.1.1 Risc inacceptable:

La **AI Act** contempla en el seu article 5 un conjunt de pràctiques considerades de risc inacceptable perquè incideixen en els drets fonamentals i la seguretat humana de manera tan greu que el seu ús no pot ser permès. Per aquest motiu, qualsevol sistema d'IA que coincideixi amb alguna d'aquestes pràctiques no podrà ser comercialitzada, desenvolupada ni utilitzada dins del territori de la UE.

A continuació trobareu un llistat dels usos inacceptables. Si algun d'ells s'aplica al vostre sistema, no és necessari que completeu les preguntes del model, ja que aquest ha estat pensat per avaluar sistemes que podran ser efectivament utilitzats d'acord amb la legislació.

Aquesta taula conté les pràctiques considerades d'usos prohibits per l'article 5 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act). Si el vostre sistema d'IA s'identifica amb qualsevol de les següents, li correspon la categoria d'USOS PROHIBITS.

- | | |
|---|---|
| 1 | <p>Sistemes que despleguen tècniques subliminars, enganyoses o manipuladores que alterin el comportament d'una persona o grup de persones perquè prenguin una decisió que causi perjudicis significatius a ella mateixa o altres persones.</p> <p>Aquesta pregunta es basa en article 5 apartat 1.a).</p> |
| 2 | <p>Sistemes d'IA que exploten les vulnerabilitats d'una persona o grup de persones (per exemple l'edat, la situació social o econòmica o la capacitat mental) alterant el seu comportament de manera que causi perjudicis significatius a ella mateixa o altres persones.</p> <p>Excepció: Quan el sistema està destinat a fins terapèutics autoritzats sempre que es compti amb el consentiment informat de la persona afectada.</p> <p>Aquesta pregunta es basa en article 5 apartat 1.b).</p> |

3	<p>Sistemes d'IA que avaluen o classifiquen persones físiques o grups de persones durant un període de temps determinat en funció del seu comportament social o les seves característiques personals o altres conegudes, deduïdes o previstes amb els següents efectes:</p> <ol style="list-style-type: none"> 1. contextos socials que no guarden relació amb la raó que van donar lloc a la recopilació originària o generació de les dades. 2. tracte no justificat o desproporcionat respecte al comportament social o llur gravetat. <p>Aquesta pregunta es basa en article 5 apartat 1.c).</p>
4	<p>Sistemes d'IA que duen a terme avaluació de riscos de persones físiques amb el fi d'avaluar o predir el risc que una persona cometi un delictes basat únicament en l'elaboració de perfils, avaluació dels seus trets i característiques de personalitat.</p> <p>Excepció: Sistemes d'IA utilitzats per a recolzar l'avaluació humana de l'impacte d'una persona en una activitat delictiva basada en fets objectius i verificables directament de tal activitat.</p> <p>Aquesta pregunta es basa en article 5 apartat 1.d).</p>
5	<p>Sistemes d'IA que creen o amplien les bases de dades de reconeixement facial mitjançant l'abocament no selectiu d'imatges facials d'internet o gravacions de càmeres de videovigilància.</p> <p>Aquesta pregunta es basa en article 5 apartat 1.e).</p>
6	<p>Sistemes d'IA que infereixen en les emocions d'una persona física en els àmbits del lloc de feina i les institucions educatives.</p> <p>Excepció: Sistema està destinat al mercat o activat per raons mèdiques o de seguretat.</p> <p>Aquesta pregunta es basa en article 5 apartat 1.f).</p>
7	<p>Sistemes de categorització biomètrica que categoritzen individualment a persones físiques a partir de llurs dades biomètriques per a deduir o inferir la seva raça, opinions polítiques, afiliació sindical, creences religioses o filosòfiques, vida sexual o orientació sexual.</p> <p>Excepció: Etiquetatge o filtrat de conjunts de dades biomètriques adquirides legalment en l'àmbit d'aplicació de la llei.</p> <p>Aquesta pregunta es basa en article 5 apartat 1.g).</p>
8	<p>Sistemes d'identificació biomètrica remota en temps real en espais d'accés públic amb fins policials.</p> <p>Excepció: Aquest ús és permès si es compta amb autorització judicial per a una de les següents finalitats:</p> <ol style="list-style-type: none"> 1. identificació de víctimes de segrest, tràfic d'éssers humans o explotació sexual i persones desaparegudes. 2. prevenir una amenaça substancial, específica i imminent per a la vida o seguretat; o una amenaça real i actual o real i previsible d'atemptat terrorista.

3. localització o identificació d'una persona sospitosa d'haver comès una infracció penal que comporti una investigació, enjudiciament o execució de sanció dels especialment greus enumerat a l'Annex II d'aquesta llei.

I valorant els següents elements:

1. La gravetat, probabilitat i magnitud del perjudici causat per no utilitzar-se el sistema.
2. La conseqüència per als drets i llibertats de totes les persones afectades, en particular la gravetat, probabilitat i magnitud.

I respectat el seu ús les tuteles i exercici de condicions necessàries i proporcionades per la llei, així com supeditat a l'autorització prèvia concedida per l'autoritat judicial o l'administrativa independent. Excepcionalment en situacions d'urgència degudament justificada, es pot iniciar la utilització del sistema sense autorització sempre que se sol·liciti en un termini de 24 hores.

Aquesta pregunta es basa en [article 5 apartat 1.h\)](#) i [apartat 2.](#)

7.1.2. Qüestionari de classificació dels sistemes en funció dels riscos:

En aquest apartat trobareu les qüestions que us permetran saber el nivell de risc associats al vostre sistema.

Per a completar la preavaluació si us plau seguiu el següent circuit:

Aquesta taula conté les practiques considerades d'alt risc per l'article 6 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act). Si el vostre sistema d'IA s'identifica amb qualsevol de les següents, li correspon la categoria d'ALT RISC.

1 El vostre sistema d'IA és un producte, o es tracta d'un component de seguretat d'un producte, subjecte a la normativa europea continguda a l'Annex I de la AI Act?

Aquesta pregunta es basa en [l'article 6.1.a\)](#).

2 El vostre sistema d'IA és un producte, o es tracta d'un component de seguretat d'un producte, que ha de ser sotmès a una avaluació de conformitat per tercers abans de poder ser comercialitzada o posada en servei d'acord amb la normativa europea continguda a l'Annex I de la IA Act?

Aquesta pregunta es basa en [l'article 6.1.b\)](#).

3 El vostre sistema s'utilitza per a la identificació biomètrica i categorització de persones físiques en base a dades sensibles o reconeixement d'emocions (sense incloure sistemes que únicament confirmen la identitat de la persona física) ?

Aquesta pregunta es basa en [l'article 6.2.](#)

4 El vostre sistema s'utilitza com a component de seguretat en la gestió i funcionament d'infraestructures digitals crítiques, trànsit en temps real o subministrament de gas, aigua, calefacció o electricitat?

	Aquesta pregunta es basa en l'article 6.2.
5	El vostre sistema s'utilitza a l'àmbit educatiu o de formació professional per a determinar l'admissió o l'accés d'alumats; per avaluar resultats, o el nivell d'educació adequat; o per a monitorar i detectar comportaments prohibits? Aquesta pregunta es basa en l'article 6.2.
6	El vostre sistema s'utilitza per controlar l'accés als llocs de feina i el departament de Recursos Humans, en general? Aquesta pregunta es basa en l'article 6.2.
7	El vostre sistema és utilitzat per entitats, públiques o privades, les quals presten serveis essencial (per exemple un sistema que determini quines persones podran beneficiar-se d'ajudes econòmiques públiques o bé, de la seva admissió a programes socials d'entitats privades) ? Aquesta pregunta es basa en l'article 6.2.
8	El vostre sistema és utilitzat en l'àmbit jurídic per part de les autoritats policials, agències, administracions o institucions per tal d'avaluar els riscos que té una persona de ser víctima d'infraccions penals; en l'ús de polígrafs o eines semblants; avaluar les proves usades durant les investigacions; o avaluar les probabilitats de delinquir o reincidir, més enllà de l'elaboració de perfils? Aquesta pregunta es basa en l'article 6.2.
9	El vostre sistema es utilitza en matèria de migració, asil i control de fronteres per les autoritats públiques mitjançant eines com el polígraf o similars per avaluar riscos (en la seguretat, sanitat i migració irregular), sol·licituds (d'asil, visat, permís de residència i reclamacions) o detectar, reconèixer o identificar persones (excepte, la verificació de documents de viatge) ? Aquesta pregunta es basa en l'article 6.2.
10	El vostre sistema té com a finalitat ser utilitzat en l'administració de justícia (durant la investigació, interpretació de fets i de la llei o aplicació) i en processos democràtics (per exemple, per facilitar el recompte de vots i sense incloure sistemes pensats per organitzar campanyes polítiques en una vessant administrativa i logística) ? Aquesta pregunta es basa en l'article 6.2.

ATENCIÓ! Tot i contestar afirmativament a les preguntes anteriors, el vostre sistema no serà considerat d'alt risc si el seu ús es destina a una de les tasques contemplades a **l'article 6.3 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act)**

- a) el sistema d'IA està pensat per dur a terme una tasca de procediment limitada;
- b) el sistema d'IA està pensat per millorar el resultat d'una activitat feta per una persona prèviament;
- c) el sistema d'IA està pensat per detectar patrons de presa de decisions o desviacions de patrons previs a la presa de decisions i no pretén substituir o influir en l'avaluació humana prèviament completada, sense que es dugui a terme una revisió; o
- d) el sistema d'IA està destinat a realitzar una tasca preparatòria d'una avaluació rellevant als efectes dels casos d'ús enumerats a l'annex III.

Aquesta taula conté les practiques relatives als sistemes d'IA generativa i els sistemes de reconeixement d'emocions i identificació biomètrica que no poden ser categoritzats com a sistemes prohibits o d'alt risc, contemplats a **l'article 50 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act).**

1	<p>El vostre sistema es utilitzat per a crear contingut de text, so, imatge o vídeo?</p> <p>Aquesta pregunta es basa en l'article 50.2 i 4.</p>
2	<p>El vostre sistema és tracta d'una eina de reconeixement d'emocions o categorització biomètrica?</p> <p>Aquesta pregunta es basa en l'article 50.3.</p>
3	<p>El vostre sistema d'IA està pensat per interactuar amb persones físiques?</p> <p>Aquesta pregunta es basa en l'article 50.1.</p>
4	<p>El vostre sistema és tracta d'un model de propòsit general?</p> <p>Aquesta pregunta es basa en l'article 52 i següents.</p>

Aquesta taula conté les practiques relatives als sistemes de propòsit general regulats **als articles 51 i següents del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act).**

El vostre sistema té la capacitat de servir per a una varietat de propòsits, tant per a l'ús directe com per a la integració en altres sistemes d'IA?

Aquesta pregunta es basa en [l'article 3 i 51 de la AI Act.](#)

En cas que el vostre sistema no recaigui en cap de les categories anteriors ha de ser classificat de RISC MÍNIM ■

Un cop sabeu la categoria de risc associada amb el vostre sistema d'IA, podeu iniciar el qüestionari seguint les directrius que us expliquem al següent apartat.

7.2. Qüestionari:

En aquest apartat trobareu les preguntes que us permetran saber fins a quin grau el vostre sistema d'IA respon als nostres principis ètics i legals. Les preguntes estan agrupades d'acord amb els **7 principis** que vertebreren el **Model PIO**.

Així mateix, cada principi es divideix en taules segons la temàtica que aborden (1), de manera que cada pregunta es troba inclosa en una casella (2). El requadre de la qüestió a respondre ve acompanyat de dues altres caselles. La primera conté les referències legals, acadèmiques i documents d'institucions rellevants en la matèria en els quals es basa la pregunta (3), mentre que la segona exposa un exemple amb finalitats il·lustratives, així com la bibliografia de la qual s'ha extret el mateix (4). Finalment, el sistema d'etiquetes indica a quina o quines classificacions de risc correspon allò que es demana amb la pregunta (5).

(1) 1.1. Anàlisi preliminar de l'ús del sistema

Nº	Pregunta
----	----------

(5) 1.1.1*	El procés de generació de resultats del vostre sistema d'IA està ben documentat i és reproducible per si cal descobrir problemes en el futur?	(2)
------------	---	-----



Aquesta pregunta està relacionada amb [els articles 11, 12, 53.1 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la documentació tècnica, els registres i les obligacions de les persones proveïdores dels models de propòsit general.

També fa referència a [l'apartat de fairness del toolkit d'ICO](#) i a l'apartat de [Reliability, Fall-back plans and Reproducibility](#) d'ALTAI.

Exemple: En cas que el vostre sistema estigui generant falsos positius podeu comprovar quin ha estat el procés que ha donat lloc als mateixos per identificar quin ha estat el problema i donar-li solució perquè no torni a passar.

Al 2008 [Google Flu Trends](#) va publicar un sistema de seguiment de la grip en base a dades de cerca però, l'algoritme no estava documentat de manera adequada i va comportar prediccions inexactes en brots de grip.

Aquest exemple està documentat a [What we can learn from the epic failure of Google Flu Trends](#) i [Google Flu Trends is no longer good at predicting flu, scientists find](#).

D'altra banda, el model actualitzat també compta amb un nou apartat que versa sobre la repartició d'obligacions relatives al desenvolupament, comercialització o ús d'un sistema d'IA en el marc d'una relació contractual. Així doncs, amb aquesta taula volem traslladar la consciència d'assumir la responsabilitat de cada subjecte relacionat amb els sistemes d'IA.

7.2.1. Principi 1: Transparència i explicabilitat

La transparència s'ha convertit en un dels principis més debatuts en el context dels usos ètics de la IA. Aquest principi és pot entendre de dues maneres. D'una banda, es refereix a la necessitat que la pròpia tecnologia de la IA sigui comprensible i que hi hagi una obertura respecte a la informació que s'utilitza. D'altra banda, inclou la transparència de les organitzacions que desenvolupen i/o utilitzen sistemes d'IA. Mentre que la primera forma de transparència es discuteix regularment, especialment en relació amb els processos necessaris per garantir explicabilitat, comprensió i comunicació, la segona ha quedat en segon pla i necessita ser reforçada per assegurar i protegir els drets humans i el benestar de les persones.

Generalment, aquest principi cerca garantir la transparència i la divulgació responsable perquè les persones puguin entendre quan la IA els afecta de manera significativa i esbrinar quan un sistema d'IA s'està relacionant amb ells⁵⁵. Les preguntes d'aquest apartat provenen majoritàriament de les seccions relatives a la transparència, *fairness*, i privacitat dels diferents instruments i recomanacions consultades, i troben la seva referència normativa als articles 11 a 16, 22, 50, 53 a 55 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (**AI Act**).

La transparència és un principi legal essencial per a garantir els drets de les persones, i no deixa de ser una basant del dret a la informació⁵⁶ reconegut en diversos instruments internacionals, com per exemple l'article 19 del Pacte internacional de drets civils i polítics; l'article 11 de la Carta de drets fonamentals de la UE; l'article 10 i 14 del Conveni europeu de drets humans i l'article 19 de la Declaració universal dels drets humans.

Per la seva banda, el principi de transparència i explicabilitat es veu reflectit l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, que versa sobre la transparència i la supervisió dels sistemes d'IA. Segons es recull a l'informe explicatiu del Conveni marc⁵⁷, la transparència compren la informació clara i accessible sobre el funcionament general del sistema, els processos de decisions i les decisions preses per la IA, i la governança de les activitats incloses en tot el cicle de vida del sistema. Aquesta informació inclouria, per exemple, una explicació dels algorismes utilitzats i el seu funcionament, les dades utilitzades, i la identificació del contingut generat amb intel·ligència artificial per a evitar enganys.

Respecte a la normativa elaborada per la Unió Europea destaquem el Reglament 2016/679, de 27 d'abril del 2016 relatiu a la protecció general de les dades; la Directiva 2016/2102, de 26 d'octubre del 2016 sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic; la Directiva 2019/882, de 17 d'abril del 2019 relativa als requisits d'accessibilitat dels productes i serveis; la Regulació 2022/868, de 30 de maig del 2022 relativa a la governança

⁵⁵ Mantelero, A. (2020) Regular la IA dins el marc dels Drets Humans: una metodologia per a la planificació. Disponible a: <https://iris.polito.it/handle/11583/2861372> (consultada el 18 de gener de 2024).

⁵⁶ ACNUDH (2018) Un enfocament basat en els drets humans per a les dades: no deixar ningú enrere en l'Agenda 2030 per al desenvolupament sostenible. Disponible a: <https://shorturl.at/nKpoo> (consultada el 20 de novembre de 2023).

⁵⁷ Consell d'Europa (2024) Informe explicatiu del Conveni Marc del Consell d'Europa sobre Intel·ligència Artificial i Drets Humans, Democràcia i Estat de Dret. Disponible a: <https://rm.coe.int/1680afae67> (consultada el 20 de juliol de 2024).

de dades; i finalment, la Proposta de Directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial (AI Liability Directive).

Dins d'aquest principi també s'inclouen qüestions relacionades amb la representativitat. Segons les recomanacions de l'ACNUDH en relació amb una aproximació a les dades basada en DDHH⁵⁸. Aquestes adverteixen que per a la recopilació de les dades d'un determinat grup, és important comptar amb la participació de les persones que hi formen part. Així mateix, s'ha de procurar que les dades són significants per a l'ús desitjat i els interessos de la població afectada.

En aquest sentit, l'article 19 del Conveni marc també contempla que les qüestions rellevants de caràcter social, econòmic, legal, ètic o ambiental relacionades amb un sistema d'IA, tant en el seu desenvolupament com en qualsevol moment posterior, puguin ser objecte de debat públic, i es consultin a les parts interessades.

1.1. Anàlisi preliminar de l'ús del sistema

Nº	Pregunta
----	----------

1.1.1*	El procés de generació de resultats del vostre sistema d'IA està ben documentat i és reproduïble per si cal descobrir problemes en el futur?
--------	---

Aquesta pregunta fa referència [als articles 11, 12, 53.1 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la documentació tècnica, els registres i les obligacions de les persones proveïdores dels models de propòsit general.

També fa referència a [l'apartat de fairness del toolkit d'ICO](#) i a l'apartat de [Reliability, Fall-back plans and Reproducibility d'ALTAI](#).

Exemple: En cas que el vostre sistema estigui generant falsos positius podeu comprovar quin ha estat el procés que ha donat lloc als mateixos per identificar quin ha estat el problema i donar-li solució perquè no torni a passar.

Al 2008 *Google Flu Trends* va publicar un sistema de seguiment de la grip en base a dades de cerca però, l'algoritme no estava documentat de manera adequada i va comportar prediccions inexactes en brots de grip.

Aquest exemple està documentat a [What we can learn from the epic failure of Google Flu Trends](#) i [Google Flu Trends is no longer good at predicting flu, scientists find](#).

1.1.2*	Coneixeu amb precisió per a què s'utilitza el vostre sistema d'IA?
--------	---

Aquesta pregunta fa referència [als articles 13.3, 14, i 53.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la transparència i comunicació d'informació a les persones usuàries, la vigilància humana i les obligacions de les persones proveïdores de models de propòsit general.

⁵⁸ ACNUDH (2018) Un enfocament basat en els drets humans per a les dades: no deixar ningú enrere en l'Agenda 2030 per al Desenvolupament Sostenible. Disponible a: <https://shorturl.at/rX107> (consultada el 20 de novembre de 2023).

També està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Així mateix, la pregunta es fonamenta en [els articles 8, 14 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA, els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA i el marc de gestió de riscos i impactes.

Finalment, també és relaciona amb [l'apartat de fairness del toolkit d'ICO](#).

Exemple: El 2015 l'ús de l'algoritme *RankBrain* per part de Google era un misteri i no es sabia a quantes consultes i de quina manera intervenia.

Aquesta situació està esmentada en aquest enllaç [FAQ: Everything you need to know about Google's RankBrain in 2021](#).

1.1.3

Sabeu si el vostre sistema d'IA utilitza el model més simple i intel·ligible en favor de la transparència?

Aquesta pregunta fa referència a [l'article 13.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la transparència i comunicació d'informació a les persones usuàries.

Així com [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Així mateix, la pregunta està relacionada amb [l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la transparència i supervisió dels sistemes d'IA. Juntament amb el dret a la informació consagrat a [l'article 19 del Pacte internacional de drets civils i polítics](#), [l'article 11 de la Carta de drets fonamentals de la UE](#), [l'article 10 del Conveni europeu de drets humans](#) i [l'article 19 de la Declaració universal dels drets humans](#).

Finalment, destaquem [l'apartat de Transparency de ALTAI](#) i a [l'apartat 2.2.1. Transparency d'AIEIG](#).

Exemple: El model utilitzat pel vostre sistema d'IA és suficientment senzill com perquè les persones que interactuen amb ell siguin capaces de comprendre el seu funcionament.

El sistema de justícia penal per a valorar la reincidència anomenat COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) utilitzat als Estats Units per alguns jutges per ajudar-se en la presa de decisions sobre la llibertat provisional, condicions sobre aquesta i qüestions relacionades ha comportat controvèrsia perquè usa algoritmes d'IA poc transparents.

Aquesta notícia la trobem al següent enllaç [A popular Algorithm is no better at predicting crimes than random people](#) i [When an algorithm helps send you to prison](#).

1.1.4

El vostre sistema d'IA realitza registres automàtics del seu funcionament de manera continua?

Aquesta pregunta es fonamenta a [l'article 12 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu als registres i la traçabilitat del sistema.

Així mateix, la pregunta es basa en [l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la transparència i supervisió dels sistemes d'IA.

Exemple: De manera periòdica i continua mentre esta en funcionament el vostre sistema registra informació sobre el seu funcionament i si és produeixi algun problema podeu comparar la informació enregistrada per detectar l'error que ha tingut lloc.

Assistents de veu com *l'Alexa d'Amazon* du a terme registres automàtics de la teva veu per tal de poder actualitzar i ampliar les seves dades i poder així regenerar-se. Aquest exemple està documentat a [Does Alexa listen to your conversations at home?](#).

1.1.5*



Heu facilitat o posat a disposició informació sobre la identitat i les dades de contacte de la persona proveïdora (o els seus representants) ?

Aquesta pregunta es fonamenta en [els articles 13.3, 22 i 54 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i sobre les obligacions dels representants autoritzats de les persones proveïdores de sistemes d'alt risc i els models de propòsit general.

Així mateix, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA. Juntament amb el dret a la informació reconegut a [l'article 19 del Pacte internacional de drets civils i polítics](#), [l'article 11 de la Carta de drets fonamentals de la UE](#), [l'article 10 del Conveni europeu de drets humans](#) i [l'article 19 de la Declaració universal dels drets humans](#).

Exemple: Apple no va facilitar el nom ni les dades de contacte de les persones proveïdores específics dels components ni la subcadena de muntatge necessaris per a fer alguns dels seus productes.

Aquest exemple està documentat a [Apple finds more serious supplier problems as its audits expand](#) i [Assessing the reforms portrayed by Apple's supplier responsibility report](#).

1.1.6*



Heu tingut en compte les capacitats, competències i l'alfabetització en matèria d'IA de totes les possibles persones usuàries, incloent-hi grups vulnerables, amb problemes d'accessibilitat i/o necessitats especials?

Aquesta pregunta fa referència [als articles 13.2, 16, 50.5 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i comunicació d'informació a les persones usuàries, les obligacions de les proveïdores dels sistemes d'alt risc, les obligacions de les proveïdores de sistemes d'IA generativa, de reconeixement d'emocions, de categorització biomètrica, de propòsit general i altres sistemes que interactuïn amb persones, i la promoció de codis de conducta d'aplicació voluntària.

En el mateix sentit, la pregunta està relacionada amb [l'article 4 de la Directiva 2019/882, de 17 d'abril del 2019 \[Directiva sobre els requisits d'accessibilitat dels](#)

[productes i serveis](#)] i l'article 4 de la Directiva 2016/2102, de 26 d'octubre de 2016 [Directiva sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic].

A més, la pregunta es fonamenta en [els articles 10 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació i els drets de les persones amb discapacitat i dels infants. Juntament amb el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de Drets Fonamentals de la Unió Europea](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#).

Finalment, destaquem [el capítol 2 de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#), relatiu a la governança ètica i la custòdia i guarda relació amb a les recomanacions contingudes a l'apartat de [Diversity, Non-discrimination and Fairness: Stakeholder Participation d'ALTAI](#). I també guarda relació amb l'apartat [Transparency and Explicability del AI Ethics Assessment de GSMA](#). Així com amb [les demandes de ECNL, Liberties i ECF](#), concretament l'apartat I, el punt 1.3 sobre els grups vulnerables.

Exemple: [Google Assistant](#), el sistema de reconeixement de veu i assistència virtual alimentat per IA i desenvolupat per Google, ofereix diverses opcions d'accessibilitat, com per exemple la compatibilitat amb lectors de pantalla. Per a més exemples sobre ítems garants de l'accessibilitat i/o necessitats especials podeu consultar els següents articles: [Una pàgina web accessible i amable és possible](#) i [10 consejos sobre cómo hacer tu página web accesible](#).

1.2. Explicabilitat

Nº	Pregunta
----	----------

1.2.1*



El procés de desenvolupament del vostre sistema i les persones que hi han estat implicades estan documentats i són públics?

Aquesta pregunta es fonamenta en [els articles 11, 13.3 i 53.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), sobre a documentació tècnica dels sistemes d'IA, la transparència i les obligacions de les persones proveïdores de models d'IA de propòsit general.

Així mateix, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA. Juntament el dret a la informació reconegut a [l'article 19 del Pacte internacional de drets civils i polítics](#), [l'article 11 de la Carta de drets fonamentals de la UE](#), [l'article 10 del Conveni europeu de drets humans](#) i [l'article 19 de la Declaració universal dels drets humans](#).

Exemple: Al vostre lloc web compteu amb una secció on expliqueu quin ha estat el procés per desenvolupar el vostre sistema i quines son les persones que han participat en el projecte com per exemple [la pàgina web AllenNLP](#).

1.2.2*

La informació tècnica necessària per a l'ús del vostre sistema (suport físic, versions de software, actualitzacions, etc) està documentada i és pública?

Aquesta pregunta es fonamenta a [l'article 11.1 i 53.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), sobre la documentació tècnica dels sistemes d'alt risc i les obligacions de les persones proveïdores de sistemes de propòsit general.

Així mateix, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA. Juntament amb el dret a la informació reconegut a [l'article 19 del Pacte internacional de drets civils i polítics, l'article 11 de la Carta de drets fonamentals de la UE, l'article 10 del Conveni europeu de drets humans i l'article 19 de la Declaració universal dels drets humans](#).

Exemple: La pàgina web d'[IBM Watson](#), una plataforma d'eines per a l'anàlisi de dades propulsada per intel·ligència artificial, s'ha posat a disposició de les persones interessades documentació relativa a la informació tècnica necessària per utilitzar els seus serveis.

1.2.3*

Proporcioneu informació i instruccions concises, clares i accessibles, sobre el funcionament i manteniment del vostre sistema?

Aquesta pregunta és fonamenta en [els articles 13.2 i 3 i 53 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), en relació a la transparència i comunicació de la informació i les obligacions de les persones proveïdores de sistemes de propòsit general.

Així mateix, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA. Juntament amb el dret a la informació reconegut a [l'article 19 del Pacte internacional de drets civils i polítics, l'article 11 de la Carta de drets fonamentals de la UE, l'article 10 del Conveni europeu de drets humans i l'article 19 de la Declaració universal dels drets humans](#).

Exemple: El sistema *Autopilot* dels cotxes Tesla (juny 2023) estan infrainformats perquè no inclouen instruccions clares, concises i accessibles sobre el funcionament i manteniment del sistema automàtic de conducció i les conseqüències han estat accidents i víctimes mortals als Estats Units.

Aquest exemple està documentat a [Fed's deadline comes and goes without Tesla's reply to Autopilot questions, Tesla under investigation in California over Autopilot safety issues and false advertising i 17 fatalities, 736 crashes: The shocking toll of Tesla's Autopilot](#).

1.2.4*

Es possible identificar si el contingut que genera el vostre sistema ha estat creat per una IA (per exemple amb una etiqueta o segell) ?

Aquesta pregunta es fonamenta a [l'article 50.2 i 4 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre les obligacions de les persones proveïdores d'IA generativa.

Així mateix, la pregunta es fonamenta en [els articles 8, 14 i 15.2 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA, els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA i el requisit de notificar a les persones quan estan interactuant amb un sistema d'IA. Juntament amb el dret a la informació reconegut a [l'article 19 del Pacte Internacional de Drets Civils i Polítics](#), [l'article 11 de la Carta de drets fonamentals de la UE](#), [l'article 10 del Conveni europeu de drets humans](#) i [l'article 19 de la Declaració universal dels drets humans](#).

També l'article de l'agència espanyola en relació a [Intel·ligència artificial: Transparència](#).

Exemple: En el cas del *Chat-GPT* la persona usuària no pot identificar quina part de la informació proporcionada ha estat creada pel sistema d'IA i per tant, no compta amb aquesta etiqueta o segell. Es a dir, no es pot identificar que la informació que proporciona *Chat-GPT* ha estat creat per una IA.

Aquest exemple està documentat a [ChatGPT Makes Spotting Fake News Impossible for Most People](#), [ChatGPT maker OpenAI releases 'not fully reliable' tool to detect AI generated content](#) i [Reliably detecting AI-generated text is mathematically impossible](#).

1.2.5*



Sou capaces d'entendre i explicar com el vostre sistema d'IA arriba a un resultat determinat ?

Aquesta pregunta fa referència [als articles 13 i 53 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la transparència i comunicació d'informació a les persones usuàries i la vigilància humana, així com, les obligacions de les persones proveïdores dels sistemes de propòsit general.

Així com, [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Així mateix, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA.

Destaquem també [l'apartat de Transparency de ALTAI](#) i la relació amb l'apartat [Transparency and Explicability del AI Ethics Assessment de GSMA](#).

Exemple: El sistema *iTutorGroup's* va de descartar a tots els candidats de més de seixanta anys per als llocs de feina que oferia sense poder donar cap explicació a la raó per la qual el sistema ho havia fet.

Aquest exemple està documentat a [iTutorGroup's recruiting AI rejects applicants due to age](#).

1.2.6*



Sou coneixedors de les possibles limitacions del vostre sistema d'IA i les heu comunicat a tots els actors implicats, incloent-hi les persones usuàries?

Aquesta pregunta fa referència [als articles 13.3, 14.4 i 53 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la transparència i comunicació d'informació a les persones usuàries i les obligacions de les persones proveïdores de sistemes de propòsit general.

Així com [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Així mateix, la pregunta es fonamenta en [els articles 8, 14 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA, els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA i el marc de gestió de riscos i impactes. Juntament amb el dret a la informació reconegut a [l'article 19 del Pacte internacional de drets civils i polítics](#), [l'article 11 de la Carta de drets fonamentals de la UE](#), [l'article 10 del Conveni europeu de drets humans](#) i [l'article 19 de la Declaració universal dels drets humans](#).

Destaquem també [l'apartat de Transparency de ALTAI](#) i la relació amb l'apartat [Transparency and Explicability del AI Ethics Assessment de GSMA](#).

Exemple: *Siri*, així com altres sistemes d'IA de processament de llenguatge natural (NLP), no detecta bé els diferents accents i/o variants lingüístiques d'una llengua, la qual cosa implica un perjudici per a garantir la diversitat i riquesa de les variants dialectals. A més, aquesta circumstància no s'ha comunicat a les persones usuàries quan en fan ús.

Aquest exemple està documentat a [How Siri Works, Apple's Challenge in AI: Examining Siri's Limitations and Rival Advancements](#) i [The Advantages and Disadvantages of Siri](#).

1.2.7

Heu donat informació a les persones que utilitzen el vostre sistema d'IA sobre l'intercanvi de dades, els resultats previstos i com exercir els seus drets?

Aquesta pregunta fa referència a [l'article 10.5 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la governança de dades.

Des de la perspectiva jurídica la pregunta es fonamenta en [l'article 13 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre la informació que ha de facilitar-se a la persona que cedeix les seves dades.

En relació a la governança de dades, la pregunta es basa en [l'article 21 de la Regulació 2022/868, de 30 de Maig del 2022 \[Llei Europea sobre la Governança de dades\]](#), sobre els requisits específics per a protegir els drets i els interessos de les persones interessades i titulars de dades perquè respecta a les seves dades.

D'altra banda, la pregunta està relacionada amb els [articles 8, 11 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA, la privacitat i protecció de dades personals, i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA. Juntament amb el dret a la informació reconegut a [l'article 19 del Pacte internacional de drets civils i polítics](#), [l'article 11 de la Carta de](#)

[drets fonamentals de la UE](#), [l'article 10 del Conveni europeu de drets humans](#) i [l'article 19 de la Declaració universal dels drets humans](#).

Finalment destaquem [l'apartat de transparència del toolkit d'ICO](#).

Un exemple d'aquest tema el podem trobar a la següent informe publicat per a l'ICO: [Intel·ligència artificial: transparència](#).

Exemple: Meta amb la xarxa social *Facebook* o *Instagram* és poc clara amb quin ús fa de les dades de les persones usuàries i tampoc ho comunica a aquestes. Aquest exemple està documentat a [Instagram comparte con terceros el 79% de los datos de sus usuarios](#) i [Meta comparte los datos de sus usuarios](#).

1.2.8

Considerem que heu establert un nivell de transparència i explicabilitat que no posa en risc la privacitat de les persones?

Aquesta pregunta fa referència [als articles 10 i l'article 13 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la governança de dades i la transparència i comunicació d'informació a les persones usuàries.

Així com, [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

La pregunta també està relacionada amb [l'article 5 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre els principis del tractament de dades.

Per l'altra banda, la pregunta es fonamenta en els [articles 8 i 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i la privacitat i protecció de dades personals.

Finalment destaquem l'apartat de [Right to Privacy, and Data Protection de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#).

Exemple: Heu pres mesures a favor de la transparència de les dades d'entrament utilitzades i les heu anonimitzat per tal de protegir la privacitat de les persones de les quals les heu obtingudes.

1.2.9

Considerem que heu establert un nivell de transparència i explicabilitat que no posa en risc la seguretat del vostre sistema d'IA?

Aquesta pregunta fa referència [als articles 10 i 15 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la governança de dades i precisió, solidesa i ciberseguretat dels sistemes d'IA.

Per l'altra banda, la pregunta es fonamenta en [l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la transparència i supervisió dels sistemes d'IA.

Destaquem l'apartat de [Right to Privacy, and Data Protection de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#).

Exemple: Heu facilitat una explicació del funcionament del vostre sistema però no heu inclòs informació que permeti a tercers no autoritzats alterar el seu funcionament.

1.3. Traçabilitat i representativitat

Nº	Pregunta
----	----------

1.3.1*	Heu assegurat que les dades utilitzades pel vostre sistema d'IA son suficientment representatives i adequades?
--------	---

Aquesta pregunta es basa en [els articles 10.3 i 53 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), sobre la representativitat de les dades utilitzades per sistemes d'IA i les obligacions de les persones proveïdores de models de propòsit general.

Així mateix, està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Per l'altra banda, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA.

La pregunta també està relacionada amb el principi [Participation del document A Human Rights-Based Approach To Data](#) de l'ACNUDH.

Exemple: El *sepsis model* creat per l'empresa EPIC Systems es tractà d'un sistema d'IA dissenyat per a detectar malalties en tot tipus de pacients i utilitzats en els hospitals. Però, no el van documentar amb dades suficientment representatives de tota la població i en la seva actualització va donar un elevat nombre de falses alarmes. Aquest exemple està documentat a [Epic's widely used sepsis prediction model falls short among Michigan Medicine patients](#) i ["Flying in the Dark": Hospital AI Tools Aren't Well Documented](#).

1.3.2*	Heu documentat els tipus de dades, la seva procedència i els canvis efectuats en cada fase del cicle de vida del vostre sistema d'IA?
--------	--

Aquesta pregunta fa referència [als articles 10, 13.3, 53.1 i 61 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la governança de dades, la transparència i comunicació d'informació als usuaris, les obligacions de les persones proveïdores de models de propòsit general i el seguiment postmercat dels sistemes d'alt risc.

Per l'altra banda, la pregunta es fonamenta en [els articles 8, 12 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes, la fiabilitat dels sistemes d'IA, i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA.

La pregunta també està relacionada amb el principi [Transparency del document A Human Rights-Based Approach To Data](#) de l'ACNUDH i a les recomanacions contingudes als apartats de [Reliability, Fall-back plans and Reproducibility](#) i [Privacy and Data Governance](#) d'ALTAI.

Exemple: El 2022 [The Guardian](#) va informar sobre la falta de transparència en relació amb les dades utilitzades pels algoritmes d'IA que el Departament de Treball i Pensions de Regne Unit fa servir per identificar fraus i errors en reclamacions d'ajudes de crèdit universal, així com la negativa del Departament davant les sol·licituds d'informació. L'11 de juliol [una altra publicació del mateix mitjà](#) denunciava que el Departament ha ampliat el desplegament d'aquesta tecnologia opaca a altres tipus d'ajudes públiques malgrat l'advertència de possibles biaixos.

1.3.3



Per tal de protegir les dades de persones menors d'edat, heu tingut en compte salvaguardes com la traçabilitat de les dades per verificar l'edat de les persones?

Aquesta pregunta fa referència [als articles 10 i 17 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la governança de dades i el sistema de gestió de qualitat.

La pregunta també està relacionada amb [l'article 8 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre el consentiment de les persones menors d'edat.

Per l'altra banda, la pregunta es fonamenta en [els articles 11 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la privacitat i protecció de dades personals i sobre els drets de les persones amb discapacitat i dels infants.

Destaquem també les possibles afectacions de drets fonamentals assenyalades per [Assessment List for Trustworthy \(ALTAI\)](#) i [l'apartat de Transparency](#).

Exemple: Abans de recollir les dades utilitzades, cal que es verifiqui i es faci constar l'edat de la persona de les quals s'extreuen.

1.3.4*



En el cas d'utilitzar dades demogràfiques, heu validat la seva representativitat tenint en compte el context més proper a través de la informació mostral o poblacional d'una organització d'estadística?

Aquesta pregunta fa referència [als articles 10.4 i 53 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la governança de dades i les obligacions de les persones proveïdores de sistemes de propòsit general.

La pregunta també està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil](#)

[extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Així mateix, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA.

D'altra banda, la pregunta guarda relació amb l'apartat de [Deployment and monitoring del toolkit d'ICO](#), i està relacionada amb l'apartat [Fairness del AI Ethics Assessment de GSMA](#). La pregunta també està relacionada amb el principi [Participation del document A Human Rights-Based Approach To Data de l'ACNUDH](#).

Es pot trobar més informació al respecte a la següent publicació d'ICO: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/what-do-we-need-to-do-to-ensure-lawfulness-fairness-and-transparency-in-ai-systems/#whatdoweneed>

Exemple: En cas d'idear un sistema d'IA relatiu a dades demogràfiques per a ser aplicat a la ciutat de Barcelona podeu validar la representativitat de les vostres dades a través de l'Oficina Municipal de Dades de la ciutat.

1.3.5

Conserveu els registres dels arxius que genera el vostre sistema IA com a mínim sis mesos?

Aquesta pregunta fa referència [als articles 12 i 26 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre el manteniment de registres i les obligacions dels desplejadors dels sistemes d'IA d'alt risc.

Per l'altra banda, la pregunta es fonamenta en [l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la transparència i supervisió dels sistemes d'IA.

1.4. Protocols de comunicació

Nº	Pregunta
----	----------

1.4.1	Heu establert eines de comunicació que permetin a les persones usuàries del vostre sistema d'IA realitzar comentaris sobre el seu funcionament?
-------	--

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de participació de les parts interessades.

Així mateix, la pregunta es fonamenta [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes.

Per l'altra banda, està relacionada amb les recomanacions contingudes a l'apartat de [Diversity, Non-discrimination and Fairness: Stakeholder Participation d'ALTAI](#),

[l'apartat 2.2.2. Accountability d'AIEIG](#), l'apartat de [Comunicació i Informació de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#) i [l'apartat d'accountability del toolkit d'ICO](#).

Exemple: Crear una bústia digital on les persones usuàries del vostre sistema d'IA enviïn els comentaris relatius sobre el seu funcionament.

1.4.2

Heu consultat a altres organitzacions que hagin dissenyat i/o implementat un sistema d'IA similar per a conèixer antecedents i experiències?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de participació de les parts interessades.

Així mateix, la pregunta es fonamenta [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes.

L'altra banda, està relacionada amb les recomanacions contingudes a l'apartat de [Diversity, Non-discrimination and Fairness: Stakeholder Participation d'ALTAI](#).

1.4.3

Heu establert una política de participació de diferents grups d'interès (stakeholders), incloent-hi usuàries finals i/o receptors del vostre sistema d'IA?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de participació de les parts interessades.

Així mateix, la pregunta es fonamenta [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes.

També està relacionada amb les recomanacions contingudes a l'apartat de [Diversity, Non-discrimination and Fairness: Stakeholder Participation d'ALTAI](#) i a l'apartat [Injustice in Algorithmic Systems del Algorithmic Equity Toolkit d'ACLU](#).

Finalment, destaquem el principi [Participation del document A Human Rights-Based Approach To Data de l'ACNUDH](#).

Exemple: Establir un comitè d'ètica per tal de revisar decisions crítiques de la IA i el seu impacte conformat per subjectes que formin part de diferents grups d'interès i receptors del vostre sistema.

1.4.4

En cas d'incident greu o error en el funcionament del vostre sistema d'IA heu previst un sistema de notificació?

Aquesta pregunta fa referència a [l'article 9 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la gestió de riscos.

D'altra banda, la pregunta es fonamenta en [els articles 8, 14 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió, els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: Si es detecta un incident greu es notifica immediatament a un equip de resposta interna. Aquest equip avalua la naturalesa i l'impacte de l'incident i la notifica a les parts interessades rellevants.

7.2.2. Principi 2: Justícia i equitat

Quan fem referència a que un sistema d'IA és just i equitatiu, volem dir que no perjudica les persones i promou la igualtat en relació amb els drets, la dignitat i la llibertat de cada persona per prosperar. Per assolir aquest objectiu, és fonamental garantir una major diversitat entre les persones que treballen en el disseny i la implementació dels sistemes d'IA. Les organitzacions, per tant, no només han de requerir-lo a través de la inclusió sinó també fomentar l'activació constant de la inclusió de persones minoritzades i vulnerables. A més, tot i que és comprensible que les persones que dissenyen els sistemes d'IA tenen els seus propis valors, calen mecanismes de control per evitar que desenvolupin algorismes d'IA que reproduïen prejudicis injustos a través de biaixos cognitius i estadístics.

Així doncs, podem dir que aquest principi indica que els sistemes d'IA han de ser inclusius i accessibles, i per tant no haurien d'implicar ni provocar una discriminació injusta contra persones, comunitats o grups. Les preguntes d'aquest apartat provenen majoritàriament de les seccions relatives a la diversitat, no-discriminació i justícia dels diferents instruments i recomanacions consultades. Trobem la seva referència normativa a l'article 95 de la **AI Act**, relatiu a la promoció de codis de conducta d'aplicació voluntària, i també als articles 9 i 15 de la mateixa norma, relatius a les mesures de gestió de riscos i la resiliència i robustesa dels sistemes d'IA. Del mateix text normatiu també és aplicable per aquest principi els articles 10, 13, 14, 16, 27, 53, 55 i 72 com tot seguit es justificarà en les preguntes.

El principi de justícia i equitat està directament relacionat amb els dret a la igualtat i la prohibició de discriminació. Aquests han estat recollits en un gran nombre de normes internacional i comunitàries, entre les quals s'inclouen els articles 7, 8, 11, 21, 26 i 47 de la Carta de drets fonamentals de la Unió Europea; els articles 2, 17, 19 i 26 del Pacte internacional de drets civils i polítics; l'article 15 de la Carta social europea; els articles 8, 12 i 19 de la Declaració universal dels drets humans; els articles 8, 10, 13 i 14 del Conveni europeu de drets humans; i finalment, l'article 7 del Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals.

Respecte a la normativa elaborada per la Unió Europea destaquem el Reglament 2016/679, de 27 d'abril del 2016 relativa a la protecció general de les dades; la Directiva 2016/2102, de 26 d'octubre del 2016 sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic; també el Reglament 2018/1725, de 23 d'octubre de 2018, relatiu a la protecció de dades tractades per institucions, òrgans i organismes de la Unió; la Directiva 2019/882, de 17 d'abril del 2019 relativa als requisits d'accessibilitat dels productes i serveis; i finalment, la Proposta de Directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial (AI Liability Directive).

Així mateix, el dret a la no discriminació ha donat lloc a l'adopció de textos jurídics específics que protegeixen a col·lectius susceptibles de veure els seus drets vulnerats a conseqüència de la discriminació estructural que pateixen. Els esmentats inclouen la Convenció per a l'eliminació de totes les formes de discriminació racial, la Convenció per a l'eliminació de totes les formes de Discriminació contra les Dones o la Convenció sobre els Drets de les Persones amb Discapacitats, entre d'altres.

Igualment, el principi de justícia i equitat es correspon amb l'article 10 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, relatiu a la igualtat i no la discriminació. Aquest precepte requereix l'adopció de mesures destinades a superar les desigualtats per aconseguir resultats justos i equitatius.

D'acord amb l'informe explicatiu del Conveni marc⁵⁹, l'article 10 comporta l'adopció de mesures que garanteixin el respecte de totes les obligacions, tant internacionals com pròpies del dret domèstic de cada estat o regió, relacionades amb la protecció envers la discriminació, especialment pel que fa a la identificació, mitigació i eliminació de tota mena de baixos. D'altra banda, els autors del Conveni marc han expressat que l'article 10 no només requereix abstenir-se de perjudicar a persones concretes, sinó que comporta l'adopció de mesures per tal de superar les desigualtats estructurals i històriques, les quals han de fonamentar-se en els punts de vista de les persones afectades.

Així com, l'article 18 Conveni marc preveu de manera específica l'obligació de prendre en consideració les necessitats i riscos específics dels sistemes d'IA per als drets dels infants i les persones amb discapacitat, especialment pel que fa a l'educació digital i a la prevenció de l'ús d'intel·ligència artificial per a facilitar la generació de pornografia, l'abús sexual i l'explotació sexual dels menors⁶⁰.

Tot i la rellevància d'aquesta matèria, un estudi portat a terme per l'Agència de Drets Fonamentals de la Unió Europea (FRA)⁶¹ a diversos països de la UE, incloent-hi l'Estat espanyol, va revelar que la majoria de les persones desenvolupadores i usuàries d'IA no havien portat a terme una avaluació detallada en relació amb el potencial discriminador de l'automatització de processos de decisió.

Resulta crucial adoptar mesures d'avaluació, previsió, mitigació i eliminació d'aquells factors que puguin resultar en una discriminació envers alguna persona o col·lectiu. Només d'aquesta manera es pot garantir complir els requisits per la **AI Act**, així com el dret a la no discriminació, contemplat als instruments esmentats, que resulten igualment vinculants i de caràcter obligatori.

Per tal d'evitar aquestes situacions, és recomanable que les dades usades pels sistemes d'IA es recopilin comptant amb la participació dels grups d'interès, permetent que els seus integrants els

⁵⁹ Consell d'Europa (2024) Informe explicatiu del Conveni Marc del Consell d'Europa sobre intel·ligència Artificial, Drets Humans, Democràcia i Estat de Dret. Disponible a: <https://rm.coe.int/1680afae67> (consultada el 20 de juliol de 2024).



⁶⁰ *Idem*.

⁶¹ FRA (2021) Encertar el futur. Intel·ligència Artificial i drets fonamentals. Disponible a: <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights> (consultada el 21 de novembre de 2023).

que defineixin les seves característiques, i disposin d'un nivell de desagregació suficient per identificar possibles desigualtats.⁶²

Finalment, amb l'objectiu de facilitar la mitigació dels biaixos, a més de comptar amb la participació dels grups afectats, sabem que cal promoure la diversitat i la multidisciplinària dels equips que treballen en algorismes i sistemes d'IA. No obstant, fins i tot amb equips diversos, no podem esperar que aquesta diversitat sigui suficient per identificar punts cecs i mitigar els biaixos. Cal implicar persones d'àmbits que no siguin necessàriament de la IA, especialment de les ciències socials i les humanitats, així com experts del domini que entenen els aspectes i complexitats d'un problema en el qual ha d'operar un sistema d'IA.

2.1. Inclusió i diversitat

Nº	Pregunta
2.1.1  	<p>Heu establert mesures d'inclusió i equitat com provar els resultats del vostre sistema d'IA per a diferents grups afectats?</p> <p>Aquesta pregunta fa referència als articles 9, 10.3, 15.3, 27.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act), relatius a les mesures de gestió de riscos, la governança de dades, la resiliència i robustesa dels sistemes d'IA, l'avaluació d'impacte dels drets fonamentals per a sistemes d'IA d'alt risc i la promoció de codis de conducta d'aplicació voluntària per a persones o grups vulnerables.</p> <p>La pregunta també es relaciona amb els articles 10 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, que versen sobre la Igualtat i no discriminació i el marc de gestió de riscos i impactes. Juntament amb el dret humà a la no discriminació, consagrat a l'article 14 del Conveni europeu de drets humans, l'article 21 de la Carta de drets fonamentals de la UE, l'article 26 del Pacte internacional de drets civils i polítics i l'article 7 de la Declaració universal dels drets humans.</p> <p>A més, la pregunta també està relacionada l'apartat Specific safeguards to ensure non-discrimination when using de l'informe Getting The Future Right, Artificial Intelligence And Fundamental Rights de la FRA.</p> <p>Finalment, la pregunta es fonamenta en https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::u-smarcdef_0000377897&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_4bc33956-d665-48ad-92af-57ae532c98ef%3F_%3D377897eng.pdf&locale=es&multi=true&ark=/ark:/48223/pf0000377897/PDF/377897eng.pdf l'apartat de Fairness and non-discrimination de les recomanacions sobre ètica en la Intel·ligència Artificial</p>

⁶² ACNUDH (2018) Un enfocament basat en els drets humans per a les dades: no deixar ningú enrere en l'Agenda 2030 per al Desenvolupament Sostenible. Disponible a: <https://shorturl.at/r5hCL> (consultada el 20 de novembre de 2023).

[d'UNESCO](#), i està relacionada amb l'apartat [Fairness del AI Ethics Assessment de GSMA](#).

Exemple: El lloc web per sol·licitar un passaport al Regne Unit funciona amb un sistema automàtic que detecta les fotografies que no compleixen les normes del Ministeri d'Interior. D'acord amb una investigació portada a terme per la [BBC](#), aquest sistema desaprova el 22% de les dones amb pell fosca davant el 9% de desaprovació d'homes amb pell clara.

2.1.2*



Us heu assegurat que el vostre sistema d'IA no utilitza variables o "proxies" que poden ser injustament discriminatòries?

Aquesta pregunta fa referència [als articles 9, 15.3 27.1, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les mesures de gestió de riscos, la resiliència i robustesa dels sistemes d'IA, l'avaluació d'impacte dels drets fonamentals per a sistemes d'IA d'alt risc, les obligacions des proveïdors de sistemes de propòsit general de risc sistèmic i la promoció de codis de conducta d'aplicació voluntària per a persones o grups vulnerables. i la promoció de codis de conducta d'aplicació voluntària per a persones o grups vulnerables.

A més, la pregunta es fonamenta en [l'article 10 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la Igualtat i no discriminació, així com el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#).

En aquest sentit, la pregunta també està relacionada l'apartat [Specific safeguards to ensure non-discrimination when using de l'informe Getting The Future Right, Artificial Intelligence And Fundamental Rights](#) de la FRA.

Finalment, destaquem [l'apartat de Fairness and non-discrimination de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#) i està relacionada amb [l'apartat Fairness del AI Ethics Assessment de GSMA](#).

Exemple: D'acord amb [l'American Civil Liberties Union i el Human Rights Data Analysis Group](#), l'eina de cribratge familiar, *Allenghey* (Estats Units) per poder decidir les denúncies de negligència i abús infantil accepta més denúncies relacionades amb famílies negres que aquelles relatives amb famílies blanques. A més, el sistema etiqueta de major risc les llars on resideix una persona amb discapacitat que aquelles on no.

2.1.3



Heu avaluat si el vostre sistema d'IA s'adapta a un ampli espectre de preferències i habilitats individuals, incloent-hi persones usuàries que requereixen tecnologies d'assistència?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria d'accessibilitat.

A més, la pregunta es fonamenta en [l'article 10 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la Igualtat i no discriminació, així com el dret humà a la no discriminació,

consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), i [l'article 26 del Pacte internacional de drets civils i polítics](#).

Destaquem també les recomanacions contingudes a l'apartat de [Diversity, Non-discrimination and Fairness: Accessibility and Universal Design d'ALTAI](#), i està relacionada amb [l'apartat Fairness del AI Ethics Assessment de GSMA](#).

Exemple: El disseny del sistema facilita la lectura, per exemple, escollint un color de font que es distingeixi bé del fons i una mida adequada per a no cansar la vista.

2.1.4

Dins del vostre equip de treball, s'inclouen dones que garanteixin la diversitat d'opinions dins del procés de disseny i implementació del sistema d'IA?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de diversitat dels equips de desenvolupament.

A més, la pregunta es fonamenta en [l'article 10 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la Igualtat i no discriminació.

Està relacionada amb les recomanacions contingudes a [Diversity, Non-discrimination and Fairness: Accessibility and Universal Design d'ALTAI](#) i a [l'apartat Fairness del AI Ethics Assessment de GSMA](#).

Finalment, destaquem també el principi [Participation del document A Human Rights-Based Approach To Data de l'ACNUDH](#).

2.1.5

Dins del vostre equip de treball s'inclouen persones de diversos orígens o cultures que garanteixin la diversitat d'opinions dins del procés de disseny i implementació del sistema d'IA?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de diversitat dels equips de desenvolupament.

A més, la pregunta es fonamenta en [l'article 10 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la Igualtat i no discriminació.

D'altra banda, està relacionada amb les recomanacions contingudes a [Diversity, Non-discrimination and Fairness: Accessibility and Universal Design d'ALTAI](#) i a [l'apartat Fairness del AI Ethics Assessment de GSMA](#).

Pel que fa a l'aproximació basada en drets humans, també està relacionada amb el principi [Participation del document A Human Rights-Based Approach To Data de l'ACNUDH](#).

2.1.6

Dins del vostre equip de treball s'inclouen persones de diferents disciplines de coneixement més enllà de la informàtica i l'enginyeria?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de diversitat dels equips de desenvolupament.

I està relacionada amb les recomanacions contingudes a [Diversity, Non-discrimination and Fairness: Accessibility and Universal Design d'ALTAI](#) i a [l'apartat Fairness del AI Ethics Assessment de GSMA](#).

2.1.7



La vostra organització promou i fomenta una cultura organitzativa on la diversitat, l'equitat i la inclusió (DEI per les seves sigles en anglès) són elements prioritaris?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de diversitat dels equips de desenvolupament.

A més, la pregunta es fonamenta en [l'article 10 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la Igualtat i no discriminació.

Està també relacionada amb les recomanacions contingudes a [Diversity, Non-discrimination and Fairness: Accessibility and Universal Design d'ALTAI](#) i a [l'apartat Fairness del AI Ethics Assessment de GSMA](#).

2.1.8



La vostra organització té coneixement o forma part d'associacions o entitats que fomenten la DEI per avançar en polítiques d'IA responsable?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de diversitat dels equips de desenvolupament.

A més, la pregunta es fonamenta en [l'article 10 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la Igualtat i no discriminació.

I està relacionada amb les recomanacions contingudes a [Diversity, Non-discrimination and Fairness: Accessibility and Universal Design d'ALTAI](#) i a [l'apartat Fairness del AI Ethics Assessment de GSMA](#).

2.1.9



El vostre sistema d'IA compta amb mesures per a augmentar l'accessibilitat o recolzar-ne l'ús per a persones vulnerables?

Aquesta pregunta es basa [els articles 16 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre les obligacions de les persones proveïdores dels sistemes d'alt risc i els codis de conducta destinats a garantir la fiabilitat de la IA.

En aquest sentit, la pregunta està relacionada amb [l'article 4 de la Directiva 2019/882, de 17 d'abril del 2019 \[Directiva sobre els requisits d'accessibilitat dels productes i serveis\]](#) i [l'article 4 de la Directiva 2016/2102 del Parlament Europeu i](#)

[del Consell, de 26 d'octubre de 2016, sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils dels organismes del sector públic.](#)

La pregunta també es fonamenta en [els articles 10 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació i sobre els drets de les persones amb discapacitat i dels infants; [l'article 26 de la Carta de drets fonamentals de la UE](#) relatiu a la integració de les persones amb discapacitat; i [l'article 15 de la Carta social europea](#), sobre el dret de les persones amb alguna discapacitat a la integració social i la vida en comunitat.

A més, la pregunta està relacionada amb el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), i [l'article 26 del Pacte internacional de drets civils i polítics](#).

Exemples: Dins del [projecte Gameface](#) de Google està desenvolupant un sistema d'IA que permetrà als jugadors de videojocs amb limitació de moviments fer servir el ratolí mitjançant el reconeixement dels moviments del seu cap.

2.1.10*



Heu verificat si el vostre sistema d'IA pot influenciar negativament en processos democràtics i de presa de decisions a les institucions públiques?

Aquesta pregunta es basa en [als articles 9 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), sobre els sistemes de gestió de riscos i les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistèmic.

També es fonamenta en [els articles 5 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la integritat dels processos democràtics i respecte a l'estat de dret i el marc de gestió de riscos i impactes, així com en [l'article 21 de l'article 8 de la Declaració universal dels drets humans](#) el qual fa referència a l'apartat tercer a la importància de la voluntat del poble com a base del poder públic remarcant que s'expressa mitjançant eleccions electorals periòdiques per sufragi universal i igual amb vot secret i lliure.

Exemple: L'empresa [Smartmatic](#) ha implementat sistemes d'IA per a facilitar el recompte de vots electoral mitjançant algoritmes que escanegen i processen les butlletes electorals i recompte dels vots.

2.2. Identificació i mitigació de biaixos

Nº

Pregunta

2.2.1*



Heu implementat mesures que permetin mitigar els possibles biaixos estadístics en el vostre sistema d'IA, siguin originats en les dades d'entrenament o a posteriori?

Aquesta pregunta fa referència [als articles 9, 10.3, 15.3, 53, 55.1, 72 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu

a les mesures de gestió de riscos, la gestió de dades, la resiliència i robustesa dels sistemes d'IA, les obligacions de les persones proveïdores de sistemes de propòsit general, el seguiment post-comercialització dels sistemes d'alt risc, i la promoció de codis de conducta d'aplicació voluntària en matèria de grups vulnerables.

Així mateix, la pregunta es basa en [l'article 4.3 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

A més, es fonamenta en [els articles 10, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes. Juntament amb el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#).

En aquest sentit, també està relacionada l'apartat [Specific safeguards to ensure non-discrimination when using de l'informe Getting The Future Right, Artificial Intelligence And Fundamental Rights de la FRA](#) i l'apartat de [Diversity, Non-discrimination and Fairness d'ALTAI](#).

Exemple: Des del 2013 la Universitat d'Austin utilitzava un algoritme d'IA anomenat *GRADE* per a avaluar les sol·licituds per accedir als estudis de doctorat del departament de ciències de la computació. El 2020 van deixar d'utilitzar aquest sistema davant del risc que els seus resultats presentessin un biaix discriminatori, ja que havia estat entrenat amb dades històriques que en si mateixes podrien manifestar preferències injustes per determinats grups.

Aquest exemple està documentat a: [Uni revealed it killed off its PhD-applicant screening AI](#).

2.2.2*



Heu establert mecanismes que permetin mitigar els possibles biaixos de classificació en el vostre sistema d'IA, siguin per categories canviant o inadequades segons el context sociocultural?

Aquesta pregunta fa referència [als articles 9, 10.3, 15.3, 53, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les mesures de gestió de riscos, la gestió de dades, la resiliència, robustesa dels sistemes d'IA, les obligacions de les persones proveïdores de sistemes de propòsit general i la promoció de codis de conducta d'aplicació voluntària en matèria de grups vulnerables.

Així mateix, la pregunta es basa en [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

A més, la pregunta es fonamenta en [els articles 10, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes. Juntament amb el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta](#)

[de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#).

La pregunta també està relacionada amb el principi [Self-identification del document A Human Rights-Based Approach To Data](#) de l'ACNUDH l'[apartat de Diversity, Non-discrimination and Fairness](#) d'ALTAI.

Exemple: Per tal de garantir la mitigació de biaixos es pot recopilar dades de manera equilibrada i una de les tècniques és el submostratge aleatori o *Random Undersampling*. Consisteix en reduir la mida de la classe de majoritària i així s'igualava amb la classe minoritària. En el següent enllaç hi trobareu informació: <https://www.sciencedirect.com/science/article/pii/S1877050919313456> i <https://ieeexplore.ieee.org/document/9078901>.

2.2.3*



Heu adoptat mesures que permetin mitigar possibles biaixos cognitius en la fase de disseny o implementació del vostre sistema d'IA (e.x. el biaix de confirmació) ?

Aquesta pregunta fa referència [als articles 9, 10.3, 15.3, 53, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les mesures de gestió de riscos, la gestió de dades, la resiliència i robustesa dels sistemes d'IA, les obligacions de les persones proveïdores dels sistemes de propòsit general i la promoció de codis de conducta d'aplicació voluntària en matèria de grups vulnerables.

A més, la pregunta es fonamenta en [els articles 10, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes. Juntament amb el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#).

Finalment també fa referència a l'[apartat de Diversity, Non-discrimination and Fairness](#) d'ALTAI.

Exemple: La creació del lloc laboral de personal tècnica expert en ètica i diversitat, encarregada de realitzar avaluacions crítiques per identificar biaixos en les diferents fases del sistema. Com per exemple han fet les empreses multinacionals *Qantas* amb un Responsable de privacitat i ètica de dades o el Director d'innovació responsable i Gerent de la innovació responsable a *Facebook*.

Aquest exemple està documentat a: [15 AI Ethics Leaders Showing The World The Way Of The Future](#).

2.2.4*



Heu realitzat una avaluació d'impacte dels possibles biaixos del vostre sistema d'IA per saber si podria reforçar discriminacions, estereotips o prejudicis envers persones vulnerables (e.x. persones amb discapacitat, minories ètniques o individus d'edat avançada) ?

Des de la perspectiva jurídica la pregunta es fonamenta en [els articles 9, 10.3, 15.3, 27.1, 53, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les mesures de gestió de riscos, la governança de dades, la resiliència i robustesa dels sistemes d'IA, l'avaluació de

l'impacte dels sistemes d'alt risc sobre drets fonamentals, i la promoció de codis de conducta d'aplicació voluntària en matèria de grups vulnerables.

A més, la pregunta es fonamenta en [els articles 10, 12, 16 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la fiabilitat dels sistemes d'IA, el marc de gestió de riscos i impactes i els drets de les persones amb discapacitat i dels infants. Juntament amb el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#).

En aquest sentit, la pregunta també està relacionada amb l'apartat [Setting Minimum Requirements for Identifying and Assessing Fundamental Rights Impacts](#) de l'[Informe Towards meaningful fundamental rights impact assessments under the DSA d'Accessnow](#) i el [European Center for Not-for-Profit Law](#). Així com, guarda relació amb l'apartat [Potential for Abuse of the Algorithmic Equity Toolkit](#) d'ACLU i l'apartat [2.2.4. Justice](#) d'AIEIG.

Un exemple d'aquest tema el podem trobar a la següent publicació de *ForHumanity*: <https://forhumanity.center/independent-audit-of-ai-systems/>

Exemple: L'auditoria *ForHumanity* elabora normes per codificar la llei i establir millors pràctiques per tal de mitigar els riscos per als humans. Aquest exemple està documentat a: [Independent Audit of AI Systems](#).

2.2.5*

El vostre sistema d'IA per a la identificació biomètrica remota compleix els estàndards de classificació d'alt risc que tracten els biaixos relacionats amb l'edat, l'ètnia, la raça, el sexe o les discapacitats?

Aquesta pregunta està relacionada amb [els articles 9, 10, 15, 27.2, 53.1, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les mesures de gestió de riscos, la governança de dades, la resiliència i robustesa dels sistemes d'IA, l'avaluació d'impacte dels sistemes d'alt risc sobre els drets fonamentals, les obligacions de les persones proveïdores de sistemes de propòsit general, i els codis de conducta d'aplicació voluntària.

A més, la pregunta es fonamenta en [l'article 4.3 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

A més, la pregunta està relacionada amb [els articles 10, 12, 16 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la fiabilitat dels sistemes d'IA, el marc de gestió de riscos i impactes i els drets de les persones amb discapacitat i dels infants. Juntament amb el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#).

En aquest sentit, la pregunta també està relacionada l'apartat [Specific safeguards to ensure non-discrimination when using de l'informe Getting The Future Right, Artificial Intelligence And Fundamental Rights de la FRA](#).

Exemple: La realització de proves sistemàtiques per avaluar el rendiment del sistema en subgrups demogràfics diversos.

2.2.6*



El vostre sistema d'IA incorpora mesures per mitigar els biaixos del conjunt de dades, especialment aquells que podrien perpetuar la discriminació o afectar la salut i la seguretat, alhora que s'adhereixen a les pràctiques de preservació de la privadesa d'acord amb els requisits de la legislació de la Unió?

Des de la perspectiva jurídica la pregunta es fonamenta en [els articles 9, 10.3, 15.3, 27.1, 53, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les mesures de gestió de riscos, la governança de dades, la resiliència i robustesa dels sistemes d'IA, l'avaluació de l'impacte dels sistemes d'alt risc sobre drets fonamentals, i la promoció de codis de conducta d'aplicació voluntària en matèria de grups vulnerables.

Així mateix, la qüestió es basa en [l'article 32 del Reglament de la UE sobre protecció de les persones físiques en relació amb el tractament de dades personals](#) que versa sobre la seguretat de les dades personals.

A més, la pregunta es fonamenta en [els articles 10, 11, 12, 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la privacitat i protecció de dades personals, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes; el dret humà a la no discriminació, garantit a [l'article 14 del Conveni europeu de drets humans](#), [l'article 26 del Pacte internacional de drets civils i polítics](#) i [l'article 7 de la Declaració universal dels drets humans](#); el dret humà a la privacitat reconegut a [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#); [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals; i [l'article 7 del Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals](#), que versa sobre la seguretat de les dades.

A més, fa referència a [l'apartat de Diversity, Non-discrimination and Fairness d'ALTAI](#).

Exemple: Google *Fitbit* és una aplicació de salut i benestar que utilitza tècniques de mostreig aleatori i representatiu. Tot i que s'ha evidenciat que les dades recollides haurien de ser encara més representatives, per la qual cosa han iniciat un procés de cerca de persones investigadores.

Aquest exemple està documentat a: [12 examples of employee wellness software and apps](#), [NIH Fitbit Study Reveals Need for Diversity in Research](#) i [Fitbit looks to close diversity gap in research with new Health Equity Research Initiative](#).

2.2.7*



Les mesures de detecció i correcció de biaix al vostre sistema d'IA, inclòs el tractament de categories especials de dades personals, compleixen la normativa que garanteix la protecció de dades? (Reglament (UE) 2016/679, Directiva (UE) 2016/ 680, i el Reglament (UE) 2018/1725)

Aquesta pregunta es fonamenta en [els articles 9, 10.3, 15.3, 27.1, 53, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#)

, relatius a les mesures de gestió de riscos, la governança de dades, la resiliència i robustesa dels sistemes d'IA, l'avaluació de l'impacte dels sistemes d'alt risc sobre drets fonamentals, i la promoció de codis de conducta d'aplicació voluntària en matèria de grups vulnerables.

La pregunta també està relacionada amb [l'article 4.3 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Així com, [l'article 9 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#), [l'article 10 de la Directiva 2016/680, de 27 d'abril de 2016, \[Directiva de protecció de dades amb fins de prevenció, investigació, detecció, enjudiciament o execució d'infraccions penals\]](#), i [l'article 10 del Reglament 2018/1725, de 23 d'octubre de 2018, \[Reglament de protecció de dades tractades per institucions, òrgans i organismes de la Unió\]](#).

D'altra banda, la pregunta es basa en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la privacitat i protecció de dades personals. Juntament amb el dret humà a la privacitat, consagrat a [l'article 8 del Conveni europeu de drets humans](#), [l'article 17 del Pacte internacional de drets civils i polítics](#), [l'article 7 de la Carta de drets fonamentals de la UE](#), així com [l'article 8](#) del mateix text legal, relatiu al dret a la protecció de dades personals.

En aquest sentit, la pregunta també està relacionada amb l'apartat [Specific safeguards to ensure non-discrimination when using de l'informe Getting The Future Right, Artificial Intelligence And Fundamental Rights](#) de la FRA.

Exemple: Els sistemes de reconeixement facial permeten incorporar mecanismes de seguretat per a detectar l'accés no autoritzat al sistema. No obstant, es tracta d'una eina que entra en conflicte amb la tutela del dret a la intimitat i que, a més, s'ha evidenciat que no és tan segura com es pensava.

Aquest exemple està documentat a: [Facial recognition in security systems: How they work and what they could contribute to the security posture](#).

2.2.8* **El vostre sistema d'IA incorpora mecanismes de seguretat en cas d'anomalies o accions fora dels límits predeterminats, mitigant així els riscos per a la seguretat i els drets fonamentals?**



Aquesta pregunta es basa en els [articles 14, 15, 27.1, 53.1, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la vigilància humana, la resiliència i robustesa dels sistemes d'IA, l'avaluació de l'impacte dels sistemes d'alt risc sobre drets fonamentals, i la promoció de codis de conducta d'aplicació voluntària en matèria de grups vulnerables.

Així mateix, la pregunta està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Finalment, la pregunta es fonamenta en [els articles 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: La implementació d'un sistema de control basat en regles i límits predefinitos, de manera que si el sistema detecta una activitat que supera els paràmetres establerts, com ara un accés no autoritzat o un comportament inusual de la IA, es pot activar una funció d'interrupció immediata que atura totes les operacions i notifica immediatament al personal de seguretat.

2.2.9* **S'adverteix a les persones usuàries del vostre sistema d'IA d'alt risc contra el biaix d'automatització, especialment quan el sistema proporciona informació o recomanacions per a les decisions preses per persones?**

La pregunta es fonamenta en [els articles 9.4, 13.3, 27.1, 53.1, 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a les mesures de gestió de riscos, la transparència i comunicació d'informació a les persones usuàries, l'avaluació del impacte dels sistemes d'alt risc sobre els drets fonamentals i les obligacions de les persones proveïdores dels sistemes de propòsit general. Així com en [l'article 4 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

A més, la pregunta es fonamenta el dret a la informació reconegut a [l'article 19 del Pacte internacional de drets civils i polítics](#), [l'article 11 de la Carta de drets fonamentals de la UE](#), [l'article 10 del Conveni europeu de drets humans](#) i [l'article 19 de la Declaració universal dels drets humans](#); i el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), i [l'article 26 del Pacte internacional de drets civils i polítics](#).

Exemple: Hi ha empreses que estan duent a terme anuncis i comunicacions relatius a que el seu sistema d'IA està esdevenint més intel·ligent que la intel·ligència humana i això comporta la conseqüència directa per a les persones usuàries de confiar plenament amb el resultat proporcionat i no verificar-los. És un exemple *Rufus* que és el nou *chatbot* d'Amazon assistent de compres i tal i com anuncia l'empresa, la rapidesa i intuïció són el seu punt fort.

Aquest exemple està documentat a: [Amazon Enters Chatbot Fray With Shopping Tool](#).

2.2.10* **Heu implementat mesures per abordar i mitigar el risc de sortides esbiaixades i bucles de retroalimentació, especialment per als sistemes que continuen aprenent després del desplegament?**

Aquesta pregunta es basa en [els articles 9, 15.3, 27.1, 55.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre els sistema de gestió de riscos, la solidesa dels sistemes d'IA, les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistèmic, l'avaluació de l'impacte dels sistemes d'alt risc sobre els drets fonamentals i el seguiment postmercat dels sistemes d'alt ric.

Així mateix, la pregunta es relaciona amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil](#)

[extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

A més, la pregunta es fonamenta en [els articles 10, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: Doteu el vostre sistema d'un avís que us alerti quan es produeixin sortides esbiaixades i bucles de retroalimentació.

2.2.11* **Podeu proporcionar informació detallada sobre les dades i els recursos computacionals utilitzats per a la formació, les proves i la validació del vostre sistema d'IA, inclosa la procedència de les dades, les metodologies de curació i les mesures adoptades per detectar la inadequació i els biaixos de les dades**

Aquesta pregunta fa referència [als articles 10, 53, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la governança de dades, les obligacions de les persones proveïdores dels sistemes de propòsit general, i els codis de conducta d'aplicació voluntària.

Així mateix, està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

D'altra banda, la pregunta es fonamenta en [els articles 8, 12 14 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió, la fiabilitat dels sistemes d'IA, els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA i el marc de gestió de riscos i impactes.

També està relacionada amb [la Secció 1 del capítol IV del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que regula les obligacions legals dels responsables del tractament de dades i el seu règim de responsabilitat. Així mateix, la pregunta es basa en les recomanacions contingudes a [l'apartat de Privacy and Data Governance d'ALTAI](#).

Exemple: La revisió regular de les dades d'entrada i la retroalimentació dels resultats així com la introducció de controls per ajustar i corregir el comportament del model en temps real.

7.2.3. Principi 3: Seguretat i no maleficència

Els sistemes d'IA han de ser robustos i segurs per evitar riscos de seguretat, ja que les conseqüències dels seus resultats o d'un mal ús poden ser molt negatius i afectar a nivell individual i col·lectiu. La regulació juga un paper fonamental en aquest àmbit, ja que estableix normes clares per a la seguretat i maneig de dades. En aquest sentit, les organitzacions han de

complir amb estrictes mesures de control i estar subjectes a mecanismes d'auditoria i supervisió per part d'autoritats competents. Això garanteix, quan s'identifiquen problemes de seguretat, que es prenguin les accions adequades per protegir tant la tecnologia com els drets dels individus afectats.

Quan parlem de la seguretat dels sistemes d'IA, no només ens referim a garantir que la tecnologia sigui segura des d'un punt de vista tècnic (*security*), sinó també assegura que aquests sistemes no vulnerin els drets humans ni comprometin la seguretat pública (*safety*) en la seva implementació. Així doncs, els sistemes d'IA s'han de dissenyar amb la intenció de no causar dany a les persones, i han de ser sotmesos a proves regulars per garantir que no generen cap risc. Per assolir-ho, és essencial que les organitzacions rebin i integrin l'assessorament d'autoritats legals i comitès d'ètica, assegurant que les dades utilitzades en els sistemes d'IA es gestionen de manera segura i responsable, sense perjudicar els individus involucrats.

Aquest principi proposa que els sistemes d'IA haurien de funcionar de manera fiable d'acord amb el propòsit previst. Les preguntes d'aquest apartat provenen majoritàriament de les seccions relatives a responsabilitat, traçabilitat i robustesa tècnica dels diferents instruments i recomanacions consultades, i troben la seva referència normativa als articles 9 a 17, 27, 50, 53, 55, 72 i 95 de la normativa sobre intel·ligència artificial (**AI Act**).

La normativa internacional és rellevant destacar l'article 1, 3, 7 i 8 de la Carta de drets fonamentals de la Unió Europea; i l'article 14 del Conveni europeu de drets humans.

El principi de seguretat i no maleficència està relacionat amb l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, sobre la fiabilitat dels sistemes d'IA. En la seva virtut, és necessari prendre mesures que promoguin la seguretat, validesa i confiança en els sistemes d'IA, de manera que es garanteixin estàndards de seguretat, precisió, qualitat i robustesa durant tot el seu cicle de vida, i desenvolupar sistemes que siguin segurs des del disseny.

Tal com s'especifica a l'informe explicatiu del Conveni⁶³, per tal d'assolir la fiabilitat dels sistemes d'IA, també esdevé indispensable adoptar mesures que abordin requisits previs funcionals, com ho són la qualitat, exactitud, pertinença, integritat i seguretat de les dades.

Respecte a la normativa elaborada per la Unió Europea destaquem el Reglament 2016/679, de 27 d'abril del 2016 relativa a la protecció general de les dades; i també, la Proposta de Directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial (AI Liability Directive).

Aquest principi és indispensable per prevenir la lesió de drets, puix que la seva manca pot provocar un error en el funcionament del sistema dels que se'n derivin importants conseqüències. Entre els possibles escenaris, s'inclou l'ús indegut intencional i la manipulació del sistema a través



⁶³ Consell d'Europa (2024) Informe explicatiu del Conveni Marc del Consell d'Europa sobre Intel·ligència Artificial i Drets Humans, Democràcia i Estat de Dret. Disponible a: <https://rm.coe.int/1680afae67> (consultada el 20 de juliol de 2024).

de la pirateria maliciosa, la qual cosa podria desembocar en situacions de discriminació, violació de la privacitat, i fins i tot danys físics i psicològics⁶⁴.

En altres casos, el risc pot sorgir de problemes de precisió del mateix sistema, arribant a comportar conseqüències tan greus com la pèrdua de la vida. Aquest és el cas dels sistemes automàtics de conducció dels vehicles Tesla, als quals s'atribueixen 736 accidents de trànsit als Estats Units des del 2019, entre ells, 17 van ser mortals⁶⁵.

Així doncs, s'observa com la seguretat és un principi vinculat de manera transversal a tots els drets que puguin arribar a ser afectats per un sistema d'IA, inclosos, entre d'altres, el dret a la vida i la integritat física i mental, el dret a la llibertat i la seguretat, el dret a la igualtat i la no discriminació, el dret a la privacitat, i el dret a la llibertat d'expressió i a la informació, així com els principis de la Democràcia i l'Estat de Dret⁶⁶.

3.1. Funcionament del sistema

Nº	Pregunta
3.1.1*  	<p>Les persones que han dissenyat el vostre sistema d'IA han proporcionat orientació sobre com interpretar i respondre a les mètriques generades pel propi sistema?</p> <p>Aquesta pregunta fa referència als articles 13.3, 14.4 i 53.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act), relatius a la transparència, la vigilància humana, i les obligacions de les persones proveïdores de sistemes de propòsit general.</p> <p>Per l'altra banda, la pregunta es fonamenta en els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA.</p> <p>També té relació amb subapartat de Human Oversight d'ALTAI.</p> <p>Exemple: El <i>chatbot Tay</i> de Microsoft creat per a interactuar amb les persones joves a la xarxa social X no va durar actiu ni 24 hores ja que va desenvolupar respostes racistes i xenòfobes. És un exemple de com la manca de protocols sobre com evitar biaixos i discriminacions dissenyats per a les persones que supervisen les respostes d'aquestes eines.</p>

⁶⁴ Comitè ad hoc sobre Intel·ligència Artificial del Consell d'Europa (2020) Cap a la regulació dels sistemes d'IA. Disponible a: <https://shorturl.at/gjOzl> (consultada el 10 de desembre de 2023).

⁶⁵ Siddiqui, F i Merrill B. J. (2023) 17 víctimes mortals i 736 accidents: peatge impactant del pilot automàtic de Tesla. Disponible a: <https://www.washingtonpost.com/technology/2023/06/10/tesla-autopilot-crashes-elon-musk/> (consultada el 20 d'octubre de 2023).

⁶⁶ Comitè ad hoc sobre intel·ligència artificial del Consell d'Europa (2021) Intel·ligència artificial, drets humans, democràcia i estat de dret. Disponible a: <https://shorturl.at/pakCw> (consultada el 7 de novembre de 2023).

Aquest exemple està documentat a: [Twitter converteix un compte robot en un usuari racista i sexista en 24 hores](#) i [Tay aprèn el que no toca](#).

3.1.2

Heu informat sobre el nivell de precisió i seguretat del vostre sistema d'IA?

Aquesta pregunta es basa en [l'article 13.2 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la transparència.

D'altra banda, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA.

Exemple: Aquests sistemes han de ser molt precisos degut a la col·lisió amb drets fonamentals com és el cas de l'oficina de Control de Duanes i Protecció Fronterera dels EEUU qui ha desenvolupat el sistema de control fronterera [IBIS](#). Aquest sistema té la finalitat d'identificar possibles amenaces a la seguretat del país com detectant inconsistències en la informació proporcionada per els viatgers, identificar passaport fals o perfils de risc basats en comportament passats.

3.1.3*

Heu informat sobre com les accions de les persones usuàries poden influir en el rendiment del sistema?

Aquesta pregunta es basa en [els articles 13.2, 27.1 i 55 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistemàtic.

D'altra banda, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA.

Exemple: El cercador Google és el més utilitzat mundialment i per tant, influeix en les cerques futures que realitzen les persones usuàries ja que s'entrena amb moltes cerques.

Aquest exemple està documentat a: [Google controla el 90% de las búsquedas](#) i [El futuro de las búsquedas en 2023: Google se vuelve multimodal](#).

3.1.4*

Heu establert mecanismes de supervisió i control (intern o extern) per assegurar-vos que el vostre sistema d'IA funciona tal i com es pretén?

Aquesta pregunta fa referència a [els articles 9, 14, 17, 27.1, 55.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les mesures de gestió de riscos, a la vigilància humana, al sistema de gestió de qualitat, a la avaluació de l'impacte dels sistemes d'alt risc sobre els drets fonamentals, a les obligacions de les persones proveïdores dels sistemes de propòsit general de risc sistemàtic i al seguiment postmercat dels sistemes d'alt risc.

D'altra banda, la pregunta es fonamenta en [els articles 8, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de](#)

[dret](#), que versen sobre la transparència i supervisió, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Així mateix, està relacionat amb [l'apartat d'Accountability d'ALTAI](#).

Exemple: Contractar el serveis d'una empresa totalment externa perquè realitzi auditories independents amb el fi d'avaluar la precisió i eficàcia del sistema d'IA.

3.1.5*



Coneixeu els possibles comportaments i escenaris que el vostre sistema d'IA mai hauria de transgredir per garantir la seguretat i preservar la no maleficència?

Aquesta pregunta fa referència [als articles 9.2, 13.3, 27.1 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius al sistema de gestió de riscos, la transparència, l'avaluació de l'impacte dels sistemes d'alt risc sobre els drets fonamentals i les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistemàtic.

Així mateix, la pregunta està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Per l'altra banda, la pregunta es fonamenta en [els articles 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Finalment, destaquem [l'apartat de Technical Robustness and Safety d'ALTAI](#).

Exemple: Un sistema d'IA intenta accedir il·legalment a sistemes o dades protegides o exposar vulnerabilitats sense notificar adequadament als responsables de la seguretat.

3.2. Traçabilitat per a la gestió del risc

Nº Pregunta

3.2.1*



El vostre sistema ha passat per una avaluació dels seus possibles impactes sobre la salut, la seguretat i els drets de les persones?

Aquesta pregunta es basa en [l'article 9.2, 27.1, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la gestió de riscos, i l'avaluació de l'impacte dels sistemes d'IA sobre els drets fonamentals, les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistèmic i els codis de conducta d'aplicació voluntària.

Per l'altra banda, la pregunta s'inspira en [els articles 8 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de](#)

[dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i el marc de gestió de riscos i impactes.

D'altra banda, dona resposta a les demandes de més de 60 organitzacions de la societat civil que es van dirigir a les institucions europees agrupades en el [European Center for Not-for-Profit Law \(ECNL\)](#), la [Unió de Llibertats Civils per Europa \(Liberties\)](#) i el [Fòrum cívic Europeu \(ECF\)](#) en la seva carta oberta titulada [The AI Act Must Protect the Rule of Law](#).

Així com [l'apartat I, punt 1.4 de l'Informe sobre avaluacions d'impacte dels Drets Fonamentals en relació amb la Llei de Serveis Digitals d'AN i ECNL](#), sobre el compliment del marc normatiu dels drets fonamentals i [l'apartat II](#) per a l'avaluació de l'impacte sobre aquests.

Exemple: Amazon va fer servir un sistema de selecció de currículums per a les candidatures a diferents llocs de treball dins la seva empresa. Això no obstant, l'algoritme d'aquest sistema descartava a les dones en el procés de selecció de personal. Aquest exemple està documentat a: [El algoritmo de Amazon al que no le gustan las mujeres](#) i en general: [Algoritmos y discriminación de género en la selección de personal](#).

3.2.2

Heu establert o adoptat un protocol general de traçabilitat de les dades per a la gestió del risc del vostre sistema d'IA?

Aquesta pregunta fa referència a [l'article 12.2 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre l'enregistrament del funcionament dels sistemes d'IA.

Per l'altra banda, la pregunta es fonamenta en [els articles 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

També té relació amb el [subapartat de Traceability d'ALTAI](#).

Exemple: Una empresa que utilitza un sistema d'IA en el seu procés de presa de decisions comercials implementa un protocol que inclou la recopilació i l'emmagatzematge de dades d'entrada i sortida del sistema, així com la documentació de les decisions preses, per comprovar com aquest ha afectat a les seves decisions i identificar com minimitzar riscos de cara al futur.

3.2.3*

El vostre sistema d'IA compta amb mitjans per identificar i avaluar els riscos sorgits del seu ús?

Aquesta pregunta es basa en [els articles 9.2, 27.1, 55.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la gestió de riscos, l'avaluació de l'impacte dels sistemes d'alt risc sobre les drets fonamentals, les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistèmic i la vigilància postmercat.

D'altra banda, la pregunta es fonamenta en [els articles 8, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de](#)

[dret](#), que versen sobre la transparència i supervisió, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: L'empresa *Risilinc* utilitza IA per avaluar i traçar els riscos associats a la cadena de subministrament de diferents empreses i així valorar el rendiment de les persones proveïdores.

Aquest exemple està documentat a: [SUPPLIER EVALUATION: SUPPLIER RISK SCORECARD](#).

3.2.4*

El vostre sistema d'IA compta amb mitjans per identificar i avaluar els riscos sorgits amb les dades recollides després d'entrar en funcionament?

Aquesta pregunta es basa en [els articles 9.2, 15.3, 27.1, 55.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la gestió de riscos, la resiliència, l'avaluació de l'impacte dels sistemes d'alt risc sobre les els drets fonamentals, les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistèmic i la vigilància post-comercialització.

Per l'altra banda, la pregunta es fonamenta en [els articles 8, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: El Banc Interamericà de Desenvolupament, ha implementat els sistema d'IA [Alía](#) per a determinar la elegibilitat de les persones per a rebre assistència social i beneficis governamentals.

Aquest sistema, un cop entra en funcionament, ha de recopilar dades sobre les decisions d'elegibilitat i assignació preses per a identificar i avaluar els riscos associats. Llavors es realitzen avaluacions regulars d'impacte social per comprovar si el sistema afecta desproporcionadament uns certs grups de persones sol·licitants.

Aquest exemple està documentat a: [ALÍA | Project | IDEO.org](#)

3.2.5*

El vostre sistema d'IA compta amb mitjans que permeten l'adopció de mesures apropiades i específiques per eliminar o mitigar els riscos detectats?

Aquesta pregunta es basa en [els articles 9.2, 15.3, 27.1, 55.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la gestió de riscos, la resiliència, l'avaluació de l'impacte dels sistemes d'alt risc sobre els drets fonamentals, les obligacions de les persones proveïdores de sistemes de propòsit general de risc sistèmic i la vigilància post-comercialització.

Per l'altra banda, la pregunta es fonamenta en [els articles 8, 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió, la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: Una empresa de xarxes socials ha desenvolupat un sistema d'IA per a la detecció de contingut inapropiat en la seva plataforma, però que comporta un risc de falsos positius que podria causar l'eliminació errònia de contingut legítim. Per això, l'empresa implementa un mecanisme de revisió humana.

3.2.6

Heu informat sobre els riscos residuals (aquells que no han pogut ser eliminats o corregits després d'haver pres totes les mesures possibles) ?

Aquesta pregunta es basa [l'article 9.4 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la gestió de riscos.

D'altra banda, la pregunta es fonamenta en [els articles 8, 14 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió, els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA i el marc de gestió de riscos i impactes.

3.2.7*

Heu avaluat els possibles riscos o danys que provocaria que el vostre sistema d'IA fes prediccions inexactes en els escenaris previstos?

Aquesta pregunta fa referència a [els articles 9.5 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a l'avaluació de riscos i a les obligacions de les persones proveïdores de sistemes de propòsit general d'alt risc.

Per l'altra banda, la pregunta es fonamenta en [els articles 8 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i el marc de gestió de riscos i impactes.

Així com, als [apartats de *Technical Robustness and Safety* i d'*Accountability* d'ALTAI](#).

Exemple: El programa [PredPol](#), utilitzat per departaments policials dels EEUU, realitza prediccions sobre la zones on considera més probable que es cometí un delicte.

3.2.8

Heu considerat els possibles riscos o danys que provocaria si el vostre sistema d'IA s'utilitzés per a altres usos més enllà dels previstos?

Aquesta pregunta fa referència [als articles 9.5 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a l'avaluació de riscos i a les obligacions de les proveïdores de sistemes de propòsit general d'alt risc.

Per l'altra banda, la pregunta es fonamenta en [els articles 8 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i el marc de gestió de riscos i impactes.

Així mateix, la pregunta guarda relació amb l'apartat [Potential for Abuse de l'Algorithmic Equity Toolkit d'ACLU](#) i també amb als [apartats de *Technical Robustness and Safety* i d'*Accountability* d'ALTAI](#).

Exemple: El [Washington Post](#) ha fet ressò de l'estafa de 3.000 dòlars canadencs que va patir una parella per part d'algú que els va trucar fent-se passar pel seu net utilitzant un sistema d'IA per clonar la veu d'aquest, al·legant que estava a la presó i necessitava els diners per a la fiança.

3.2.9*

Heu avaluat que, en cap cas, les dades que recolliu, genereu o utilitzeu per al funcionament del vostre sistema d'IA no poden utilitzar-se per discriminar persones de forma negativa?

Aquesta pregunta fa referència als [els articles. 9.5, 10, 27.1, 50.2, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI](#)

[Act](#)), relatius a l'avaluació de riscos; a la governança de dades; l'avaluació de l'impacte dels sistemes d'alt risc sobre els drets fonamentals; les obligacions de les persones proveïdores de sistemes d'identificació biomètrica i reconeixement d'emocions; sistemes de propòsit general de risc sistèmic; i la promoció de codis de conducta d'aplicació voluntària en matèria de no discriminació.

Així mateix, la pregunta està relacionada amb [l'article 9 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#), que prohibeix i limita el processament de categories especials de dades personals.

D'altra banda, la pregunta es fonamenta en [els articles 10 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació i el marc de gestió de riscos i impactes, així com en el dret humà a la igualtat i la no discriminació, consagrat a [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#), [l'article 7 de la Declaració universal dels drets humans](#), i [l'article 14 del Conveni Europea de Drets Humans](#).

Finalment, la pregunta guarda relació amb l'apartat [Potential for Abuse de l'Algorithmic Equity Toolkit d'ACLU](#) i amb el [subapartat de Data Governance d'ALTAI](#).

Exemple: Una [investigació portada a Terme per la Universitat de Toronto, el Vector Insitute i el assachusetts Institute of Technology](#) ha posat en manifest que els conjunts de dades utilitzats per entrenar models d'IA per identificar lesions de tòrax en radiografies presenten biaixos basats en el gènere, la raça i factors socioeconòmics, la qual cosa comprometrà els resultats de la IA.

3.3. Mecanismes de seguretat

Nº	Preguntes
----	-----------

3.3.1	El vostre sistema està dotat de mesures per garantir la resistència davant d'errors sorgits de la seva interacció amb altres sistemes?
-------	---

Aquesta pregunta es basa en [l'article 15.3 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la solidesa i ciberseguretat dels sistemes d'IA.

Així mateix, la pregunta està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

D'altra banda, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA.

Exemple: Una agència governamental utilitza un sistema d'IA per a analitzar dades de ciutadans. Si hi ha una interacció inapropiada amb sistemes externs, el sistema d'IA

podria recopilar informació personal sense consentiment, infringint els drets fonamentals de privacitat. Per a prevenir això, l'agència estableix protocols d'accés a dades i utilitza tallafocs de seguretat per a protegir la privacitat dels ciutadans.

3.3.2*

El vostre sistema compta amb mesures de mitigació de possibles biaixos o intents de manipulació derivats de les dades d'entrada durant el seu funcionament?

Aquesta pregunta es basa en [els articles 15.3 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la solidesa dels sistemes d'IA.

Així mateix, la pregunta està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

D'altra banda, la pregunta es fonamenta en [els articles 12 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la fiabilitat dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: El 2016 Microsoft va llençar al mercat un *ChatBot* anomenat *Tay* destinat a interactuar amb gent jove a xarxes socials. A les poques hores de ser posada en funcionament un grup de persones usuàries van manipular el sistema amb dades d'entrada perquè genera missatges islamofòbics i supremacistes. En conseqüència, Microsoft va desactivar el sistema un dia després de la seva posada en funcionament. Aquest exemple està documentat a: [Tay, la robot racista y xenòfoba de Microsoft](#).

3.3.3

Poden les persones usuàries controlar fins a quin punt estan exposats i revocar el consentiment en qualsevol moment sense que això comprometi el rendiment del sistema d'IA?

Aquesta pregunta fa referència a [l'article 17 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu al sistema de gestió de qualitat dels sistemes d'IA.

Així mateix, la pregunta es fonamenta en [els articles 7, 11 i 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la dignitat humana i autonomia individual, la privacitat i protecció de dades personals i la fiabilitat dels sistemes d'IA.

D'altra banda, està relacionada amb als [apartats de Technical Robustness and Safety i d'Accountability d'ALTAI](#), al [punt 5, Constrained Autonomy, de la Declaració de Barcelona](#), i està relacionada amb el principi [Participation del document A Human Rights-Based Approach To Data de l'ACNUDH](#).

Exemple: Un sistema d'IA s'utilitza en una xarxa de trànsit intel·ligent per a optimitzar la gestió del trànsit i reduir la congestió en una ciutat. El fet que alguns conductors retiren el seu consentiment no hauria de suposar un error en el sistema que suposi un risc per al trànsit.

3.3.4

Heu establert mesures per examinar la precisió del vostre sistema d'IA de forma contínua per conèixer si aquest està fent una quantitat inacceptable de prediccions inexactes?

Aquesta pregunta fa referència [als articles 12.2, 17 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius als registres, al sistema de gestió de qualitat dels sistemes d'IA i a la vigilància post-comercialització del sistemes d'IA d'alt risc.

Per l'altra banda, la pregunta es fonamenta en [els articles 8 i 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió i la fiabilitat dels sistemes d'IA.

D'altra banda, al [subapartat de Traceability d'ALTAI](#). De la mateixa manera, la pregunta guarda relació amb l'apartat [Accuracy & Error in Algorithmic Systems del l'Algorithmic Equity Toolkit d'ACLU](#).

Exemple: Els sistemes d'IA de traducció automàtica poden efectuar traduccions inexactes o poc precises que haurien d'estar documentades, tot i que és difícil que hi hagi registres ja que es tracta com a part de la política de privadesa. Tot i que, Google Translate és una eina que ha rebut crítiques per dur a terme prediccions inexactes. Aquest exemple està documentat a: [Google Translate: ¿cuáles son los riesgos de esta herramienta y cómo se usa correctamente?](#) i [¿Qué grado de precisión tiene Google Translate?](#).

3.4. Protecció enfront d'atacs

Nº Preguntes

3.4.1*

Heu avaluat els riscos i la vulnerabilitat del vostre sistema d'IA per garantir la seva seguretat, integritat i resiliència davant de diferents formes d'atac?

Aquesta pregunta fa referència [als articles 15.4 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la resiliència i seguretat dels sistemes d'IA i les obligacions de les persones proveïdores dels sistemes de propòsit general de risc sistemàtic.

Així mateix, la pregunta està relacionada amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Per l'altra banda, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA.

D'altra banda, la pregunta també es basa en [l'apartat de Technical Robustness and Safety d'ALTAI](#).

Exemple: Implementar mesures de seguretat, com a sistemes de *firewall* i actualitzacions de seguretat regulars, per a garantir la seguretat i integritat de vehicles autònoms en la carretera.

Aquest exemple està documentat a: [¿Por qué es necesario el firewall en entornos corporativos?](#) i [LA IMPORTANCIA DE CONTAR CON UN FIREWALL.](#)

3.4.2

Heu portat a terme una avaluació de protecció que garanteixi que els conjunts de dades que utilitza el vostre sistema d'IA no han estat prèviament compromesos o piratejats?

Aquesta pregunta fa referència a [l'article 15.4 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la resiliència i seguretat dels sistemes d'IA.

Així com [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Per l'altra banda, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA

La pregunta també es basa en [l'apartat de Technical Robustness and Safety d'ALTAI.](#)

Exemple: Abans d'implementar una IA generativa que creï obres visuals, caldria verificar la integritat i autenticitat de les dades contingudes a les biblioteques d'imatges utilitzades com a referència.

7.2.4. Principi 4: Responsabilitat i retiment de comptes

La responsabilitat ha esdevingut un tema central en l'avanç dels usos ètics de la IA, ja que existeix el temor que les organitzacions puguin desviar la culpa o eludir la seva responsabilitat en sistemes d'IA. Quan parlem de responsabilitat, ens referim inicialment a la responsabilitat moral, que inclou tant la gestió i ús responsable de les dades dels usuaris com la responsabilitat dels actors involucrats en el desenvolupament i la implementació d'un sistema d'IA. Les organitzacions han de ser plenament conscients dels problemes que poden derivar-se d'un ús inadequat de dades i ser responsables de les conseqüències perjudicials que puguin produir com a resultat d'això.

Però la responsabilitat també és legal i la regulació juga un paper crucial en aquests termes. Les organitzacions han d'establir mecanismes interns i externs que garanteixen la responsabilitat i el retiment de comptes. La regulació exigeix que els sistemes d'IA siguin clars i transparents en l'atribució de la responsabilitat legal, de manera que sempre pugui identificar-se qui és responsable en qualsevol etapa del cicle de vida del sistema, ja sigui una persona física o una entitat jurídica. Aquests mecanismes de control són fonamentals per evitar que es dilueixi la responsabilitat en cas de falles o errors.

A més, el principi de retiment de comptes inclou la supervisió humana dels sistemes d'IA. Tot i que en alguns contextos es pot cedir un cert grau de control a aquests sistemes, les persones han de continuar enviant els responsables últims de les decisions preses i dels possibles danys causats. Això significa que la culpa no pot ser atribuïda als sistemes o eines d'IA, sinó que recau en els individus o entitats que els gestionen i els utilitzen. La regulació ha de garantir que hi hagi mecanismes clars per assignar la responsabilitat legal i ètica, assegurant que els danys no quedin sense conseqüències.

Així doncs, aquest principi planteja que els responsables de les diferents fases del cicle de vida del sistema d'IA haurien de ser identificables i responsables dels resultats dels sistemes d'IA, i que s'hauria d'habilitar la supervisió humana en aquests. Així mateix, sabem que l'anomenat *hype* o *ressò* de la IA s'està produint avui en molts productes, generalment per una qüestió d'atraure interès i finançament, però aquesta pràctica no tan sols és contra productiva per les organitzacions que la practiquen degut al seu descrèdit sinó que també suposa un greuge per la manca d'eficàcia i pels impactes esbiaixats o discriminatoris que poden tenir alguns dels sistemes als quals s'atribueixen capacitats que no tenen. És per aquesta raó que quan promocioneu una IA, cal tenir en compte alguns aspectes importants.

En aquest mateix sentit, encoratjar a les persones de les organitzacions a prioritzar les consideracions de promoció de la diversitat, equitat i inclusió (DEI) en cada pas de desenvolupament o aplicació d'algorismes o sistemes d'IA ajuda a mitigar biaixos coneguts i desconeguts. No obstant, els biaixos només els podem mitigar i no pas eliminar i, per tant, les organitzacions han de mantenir un estàndard d'aplicabilitat al voltant del funcionament dels seus sistemes d'IA així com de transparència al voltant de possibles deficiències o inconvenients.

Les preguntes d'aquest apartat provenen majoritàriament de les seccions relatives a vigilància humana, responsabilitat i gestió de riscos dels diferents instruments i recomanacions consultades i a la literatura acadèmica, i troben la seva referència normativa als articles 11, 13, 14, 17, 27, 53, 55, 72 i 95 de la **AI Act**.

Aquest principi es fonamenta en l'article 9 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, titulat *rendiment de comptes i responsabilitat*, d'acord amb el qual els estats haurien de prendre mesures per garantir la responsabilitat i el retiment de comptes en relació amb els perjudicis causats per un sistema d'IA, tant si les persones que ostenten la responsabilitat són individus com si són organitzacions o entitats.

Aquestes inclouen mesures de caràcter judicial, fins i tot l'exigència de responsabilitat penal; de naturalesa administrativa, incloent-hi la possibilitat de sol·licitar la reversió de procediments i decisions; i la imposició d'obligacions i responsabilitats específiques als operadors, com per exemple que les empreses que utilitzin IA comptin amb un sistema de reclamacions intern⁶⁷.

⁶⁷ Consell d'Europa (2024) Informe explicatiu del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret. Disponible a: <https://rm.coe.int/1680afae67> (consultada el 20 de juliol de 2024).

D'altra banda, el principi de responsabilitat i retiment es troba fortament relacionat amb el dret humà a un remei efectiu davant la vulneració de drets i llibertats, d'acord amb el qual s'ha d'assegurar la disponibilitat i accessibilitat a recursos efectius en cas que alguna persona vegi vulnerats els seus drets.

El Conveni marc recull aquest dret en l'article 14. D'acord amb el seu informe explicatiu, aquest dret no es limita a la disponibilitat de procediments mitjançant els quals reclamar la responsabilitat pels perjudicis patits, sinó que, a conseqüència de l'opacitat i complexitat tècnica dels sistemes d'IA, existeix l'obligació prèvia de facilitar informació rellevant del sistema per tal que les persones interessades puguin fonamentar correctament les seves queixes⁶⁸.

El dret a un recurs efectiu ha estat reconegut per moltes altres normes internacionals, incloent-hi els articles 5 i 13 del Conveni europeu de drets humans; els articles 8 i 47 de la Carta de drets fonamentals de la UE; l'article 2 del Pacte internacional de drets civils i polítics; i els articles 3 i 8 de la Declaració universal dels drets humans; i finalment, l'article 9 del Pacte internacional de drets civils i polítics.

Tampoc el dret a un remei efectiu no es limita a possibles recursos judicials, sinó que també comprèn l'existència d'altres tipus de mecanismes, tant davant institucions públiques com privades. Per exemple, en els casos de vulneració de drets relacionats l'ús d'internet, el Consell d'Europa ha manifestat que *"Per a obtenir un remei, no s'ha de recórrer necessàriament a l'acció legal immediatament [...] Es poden obtenir remeis eficaços directament de proveïdors de serveis d'Internet, autoritats públiques i/o institucions nacionals de drets humans"*⁶⁹.

D'aquesta manera, s'observa que tant les institucions públiques com les privades participen en la protecció dels drets i les llibertats de les persones a les institucions públiques. Per aquest motiu resulta essencial que tota entitat compti amb mitjans per reparar les vulneracions causades. En aquest sentit, no només caldrà oferir mitjans de denúncia i reclamació, sinó que les persones desenvolupadores, comercialitzadores i usuàries d'un sistema d'IA hauran de fer-se responsables dels resultats lesius que puguin derivar-se de la seva utilització, implementant mesures preventives⁷⁰ i de control humà⁷¹. Per aquest motiu el Conveni marc reconeix la rellevància de garantir mesures de vigilància humana (article 15), i l'adopció d'un marc de gestió de riscos i impactes per tal d'identificar, avaluar, prevenir i mitigar els riscos i impactes per als drets humans, la democràcia i l'estat de dret derivats del sistema d'IA (article 16).

Respecte a la normativa elaborada per la Unió Europea destaquem el Reglament 2016/679, de 27 d'abril del 2016 relativa a la protecció general de les dades; i també, la Proposta de Directiva del

⁶⁸ *Idem*.

⁶⁹ Consell d'Europa (2014) Recomanació CM/Rec (2014)6 del Comitè de Ministres dels Estats membres sobre una Guia de drets humans per a usuaris d'internet. Disponible a: <https://perma.cc/C5UP-K9HF> (consultada el 13 de desembre de 2023).

⁷⁰ FRA (2020) Empreses i drets humans – Accés als recursos. Disponible a: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-business-human-rights_en.pdf (consultada el 25 de novembre de 2023).

⁷¹ Consell de Seguretat de Nacions Unides (2023) La comunitat Internacional ha d'enfrontar-se urgentment a la nova realitat de la intel·ligència artificial generativa: el Consell de Seguretat debat dels riscos i beneficis. Disponible a: <https://press.un.org/en/2023/sc15359.doc.htm> (consultada el 13 de novembre de 2023).

Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial (AI Liability Directive).

4.1. Control

Nº	Preguntes
<p>4.1.1</p> <p>●</p>	<p>Us heu assegurat que les persones involucrades en el control tenen una comprensió adequada de la presa de decisions que efectua el vostre sistema d'IA?</p> <p>Aquesta pregunta fa referència a l'article 14 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act), relatiu a la vigilància humana de sistemes d'IA.</p> <p>Per l'altra banda, la pregunta es fonamenta en l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, que versa sobre la transparència i supervisió dels sistemes d'IA.</p> <p>També es relaciona amb les recomanacions contingudes al toolkit d'ICO sobre riscos i protecció de dades en la IA.</p> <p>Exemple: Garantir aquesta formació és fonamental per a poder garantir un bon control del sistema d'IA. Aquest requisit va lligat amb la capacitat de finançament i per això, moltes petites empreses "startups" poden trobar-se amb aquest repte. Aquest exemple està documentat a: Falta de capacitación y conocimientos evitan que startups despeguen i Innovación y startups: retos y oportunidades.</p>
<p>4.1.2</p> <p>●</p>	<p>Heu definit clarament els límits del nivell de control o participació humana dins del vostre sistema d'IA?</p> <p>Aquesta pregunta fa referència a l'article 14 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act), relatiu a la vigilància humana de sistemes d'IA, així com l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial (AI Liability Directive), relativa a la presumpció de culpa dels danys provocats per una IA.</p> <p>Per l'altra banda, la pregunta es fonamenta en l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, que versa sobre la transparència i supervisió dels sistemes d'IA.</p> <p>D'altra banda, al subapartat de Human Oversight d'ALTAI, i Accuracy & Error in Algorithmic Systems del l'Algorithmic Equity Toolkit d'ACLU, així com amb l'apartat Human Agency & Oversight del AI Ethics Assessment de GSMA.</p> <p>Exemple: MasterCard ha implementat sistemes d'IA generativa per a preveure la detecció de frau que poden patir llurs targetes de crèdit o debit. Es tracta d'un mecanisme per a fixar els límits del nivell de control internament així com, garantir la confiança de la seva clientela.</p>

Aquest exemple està documentat a: [Mastercard lanzará su propia IA generativa para ayudar a detectar el fraude.](#)

4.1.3*

El vostre sistema d'IA compta amb una eina que permeti a les persones encarregades del seu control intervenir en les decisions d'aquest?

Aquesta pregunta es basa en [els articles 14.1 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la vigilància humana dels sistemes d'alt risc i les obligacions de les persones proveïdores dels models generals de risc sistèmic.

Així com [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Des de la perspectiva dels drets humans, la pregunta es fonamenta en [l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la transparència i supervisió dels sistemes d'IA.

Exemple: Heu elaborat un sistema d'IA que permet a les persones encarregades del seu control intervenir en la seva revisió manual, correcció o opció de rebuig.

4.1.4*

És possible modificar, eliminar o revertir les decisions preses pel vostre sistema d'IA quan aquestes no hagin resultat suficientment adequades o exactes per tal d'eliminar o mitigar un efecte perjudicial?

Aquesta pregunta es basa en [els articles 14.1 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la vigilància humana dels sistemes d'alt risc i les obligacions de les persones proveïdores dels models generals de risc sistèmic, així com [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Des de la perspectiva dels drets humans, la pregunta es fonamenta en [els articles 8 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i el marc de gestió de riscos i impactes.

Exemple: El 2018 un sistema automatitzat va acomiadar al Sr. Ibrahim Diallo i li va denegar l'accés a al lloc de feina i totes les eines necessàries pel desenvolupament de les seves tasques a conseqüència d'un error. En la decisió no van participar persones humanes, i la seva cap no tenia la possibilitat per revertir la decisió presa per la IA. L'empresa no va ser capaç de solucionar el problema fins a 3 setmanes després de l'esdeveniment, durant les quals el Sr. Diallo no va rebre cap mena de retribució. Aquest exemple està documentat a: [The man who was fired by a machine.](#)

4.1.5

La persona encarregada de controlar les decisions preses pel vostre sistema d'IA compta amb la capacitat necessària per a exercir aquestes funcions?

Aquesta pregunta es basa en [l'article 14.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la vigilància humana.

Per l'altra banda, la pregunta es fonamenta en [l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la transparència i supervisió dels sistemes d'IA.

Exemple: Una empresa que ofereix a la persona encarregada de controlar les decisions en primer lloc, requisits de formació i experiència per a accedir al lloc de feina i posteriorment, garanteix la formació i desenvolupament continu, així com avaluar el compliment ètic del sistema.

4.1.6



La documentació del vostre sistema d'IA proporciona detalls complets sobre la seva supervisió i mesures de supervisió humana per garantir un desplegament informat i segur?

Aquesta pregunta es basa en [els articles 11 i 14.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la documentació tècnica dels sistemes d'IA i la vigilància humana.

Per l'altra banda, la pregunta es fonamenta en [els articles 8 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA.

Exemple: Informació detallada sobre els protocols de monitoratge continu, els mecanismes de detecció d'anomalies i les vies per a la intervenció humana en cas de necessitat.

4.2. Retiment de comptes

Nº

Preguntes

4.2.1



Heu determinat qui és legalment responsable de les accions i/o decisions que pren el vostre sistema d'IA durant tot el seu cicle de vida?

Aquesta pregunta fa referència [als articles 17.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre els sistema de gestió de qualitat dels sistemes d'alt risc i les obligacions de monitoratge post-comercialització.

Així mateix, trobem relació amb [la Secció 1 del capítol IV del Reglament General de Protecció de Dades \(GDPR\) del Parlament Europeu i el Consell de la UE](#), que versa sobre les obligacions legals dels responsables del tractament de dades i amb la [proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#).

D'altra banda, la pregunta està relacionada amb [l'article 9 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la responsabilitat i el retiment de comptes pels perjudicis derivats de l'ús de la IA. Així mateix, la pregunta es fonamenta en el dret a un recurs efectiu, reconegut a [l'article 13 del Conveni europeu de drets humans](#), [l'article 47 de la Carta de drets fonamentals de la UE](#), [l'article 2.3 del Pacte internacional de drets civils i polítics](#), i [l'article 8 de la Declaració universal dels drets humans](#).

També afegim l'estudi [Talkin'&Bout AI Generation: Copyright and the Generative-AI Supply Chain](#), sobre la cadena de decisions relacionades amb una IA generativa en relació amb els drets d'autor, així com la guia [Artificial Intelligence Contractual Clauses de Society for Computers & Law \(SCL\) AI Group](#).

La [checklist ètica del Protocol del Canadà proposada per Mörch et. al.](#) i al [principi de Responsibility and accountability de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#).

Exemple: La preocupació entre empreses i persones usuàries per a saber quina part és responsable de les decisions preses pel sistema d'IA, així com les conseqüències que se'n derivin es un tema de discussió doctrinal com recull aquesta revista [ELDerecho](#).

4.2.2



Heu avaluat de quina manera el vostre sistema d'IA influeix en els processos de presa de decisions de la vostra organització?

Aquesta pregunta fa referència [als articles 14 i 17 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la vigilància humana i la gestió de qualitat dels sistemes d'alt risc. Tant les mesures de supervisió humana per al desenvolupament del propi sistema com la importància de dotar la IA de sistemes de gestió de qualitat són dos elements per a poder garantir que s'efectua el retiment de comptes en la influència per a la presa de decisions.

Així com, [l'apartat d'Accountability d'ALTAI](#).

4.2.3



Heu establert mecanismes de revisió periòdica sobre responsabilitat i retiment de comptes amb els diferents agents involucrats en el desenvolupament i ús del vostre sistema d'IA?

Aquesta pregunta fa referència [als articles 14 i 17 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la vigilància humana i la gestió de qualitat dels sistemes d'alt risc.

D'altra banda, la pregunta està relacionada amb [l'article 9 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la responsabilitat i el retiment de comptes pels perjudicis derivats de l'ús de la IA. Així mateix, la pregunta es fonamenta en el dret a un recurs efectiu, reconegut a [l'article 13 del Conveni europeu de drets humans](#), [l'article 47 de la Carta de drets fonamentals de la UE](#), [l'article 2.3 del Pacte internacional de drets civils i polítics](#), i [l'article 8 de la Declaració universal dels drets humans](#).

Així com, [l'apartat d'Accountability d'ALTAI](#).

Exemple: Google cancel·la el seu Comitè d'Ètica sobre IA una setmana després de crear-lo per opinions conflictives dels seus integrants.

Aquest exemple està documentat a: [Google cancela su Comité para regular la Ética de la Inteligencia Artificial tan solo una semana después de su creación.](#)

4.2.4

Proporcioneu informació sobre si el sistema compta amb mesures de vigilància humana i qui és la persona responsable de les mateixes?

Aquesta pregunta es fonamenta en [l'article 13 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la transparència.

La pregunta també està relacionada amb [els articles 8, 9 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA i la responsabilitat i el retiment de comptes i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA.

Així mateix, la pregunta es fonamenta en el dret a un recurs efectiu, reconegut a [l'article 13 del Conveni europeu de drets humans](#), [l'article 47 de la Carta de drets fonamentals de la UE](#), [l'article 2.3 del Pacte internacional de drets civils i polítics](#), i [l'article 8 de la Declaració universal dels drets humans](#).

Exemple: Un sistema d'IA que compta a la seva pàgina web d'un portal de transparència, servei d'atenció al client i comunicació proactives amb les persones usuàries.

4.3. Figures de protecció

Nº	Preguntes
4.3.1	<p>Heu pres mesures per facilitar la demostració del compliment de la legislació vigent incloent-hi, per exemple, la Llei de Protecció de Dades (GDPR) ?</p> <p>Aquesta pregunta fa referència als articles 11, 13, 17.1 i 43 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act), relatius a la documentació tècnica, la transparència i comunicació d'informació a les persones usuàries, el sistema de gestió de qualitat dels sistemes d'alt risc i les avaluacions de conformitat.</p> <p>Està relacionada amb la Secció 1 del capítol IV del Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades] que regula les obligacions legals dels responsables del tractament de dades i el seu règim de responsabilitat.</p> <p>Així mateix, la pregunta està relacionada amb l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, que versa sobre la transparència i supervisió dels sistemes d'IA.</p> <p>Finalment està també relacionada amb al subapartat de Data Governance d'ALTAI i el toolkit d'ICO sobre riscos i protecció de dades en la IA.</p>

Exemple: *Cambridge Analytica* és una empresa de consultoria política que va recopilar i utilitzar dades personals de milers de persones usuàries de Facebook sense el seu consentiment per a influir en campanyes electorals i processos democràtics. Aquest exemple està documentat: [Cambridge Analytica, la gran fuga de dats](#).

4.3.2

Heu determinat una o més figures de protecció envers la persona usuària del vostre sistema d'IA com per exemple, la figura del Síndic de Greuges?

Aquesta pregunta fa referència [als articles 17.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre el sistema de gestió de qualitat i el monitoratge post-comercialització dels sistemes d'IA.

La pregunta també està relacionada amb [l'article 9 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la responsabilitat i el retiment de comptes pels perjudicis derivats de l'ús de la IA. Així mateix, la pregunta es fonamenta en el dret a un recurs efectiu, reconegut a [l'article 13 del Conveni europeu de drets humans, l'article 47 de la Carta de drets fonamentals de la UE, l'article 2.3 del Pacte internacional de drets civils i polítics, i l'article 8 de la Declaració universal dels drets humans](#).

Finalment està també relacionada amb al subapartat el [subapartat de Risk Management d'ALTAI](#).

4.3.3

Heu establert formes de reparació o compensació en cas que ocorri algun mal o impacte advers de responsabilitat a través de pòlisses d'assegurances, mitjans monetaris adequats i/o altres formes de compensació?

Aquesta pregunta fa referència a [l'article 27.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a l'avaluació de l'impacte de sistemes d'alt risc sobre drets fonamentals i també amb la [proposta legislativa \(AI Liability Directive\) de la Comissió Europea, sobre responsabilitat per danys de la intel·ligència artificial](#).

La pregunta també està relacionada amb [els articles 9 i 14 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la responsabilitat i el retiment de comptes i els recursos per a les vulneracions dels drets humans derivades dels sistemes d'IA. Així mateix, la pregunta es fonamenta en el dret a un recurs efectiu, reconegut a [l'article 13 del Conveni europeu de drets humans, l'article 47 de la Carta de drets fonamentals de la UE, l'article 2.3 del Pacte internacional de drets civils i polítics, i l'article 8 de la Declaració universal dels drets humans](#).

Finalment està també relacionada amb al [subapartat de Risk Management d'ALTAI](#) i coincideix amb l'apartat [Accountability del AI Ethics Assessment de GSMA](#).

Exemple: Una empresa que amb el servei d'una assegurança de responsabilitat civil, reserva de fons o garanties financeres, inclou fons de responsabilitat ambiental o sistemes d'indemnització per danys personals com a fórmules de compensació del seu sistema d'IA.

4.4. Capacitats de la IA

Nº	Preguntes
----	-----------

4.4.1	Heu pres mesures per garantir que no esteu exagerant les capacitats o el que pot fer el vostre sistema d'IA?
-------	---

Aquesta pregunta es fonamenta en [els articles 13.3, 14.4 i 53.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i la vigilància humana dels sistemes d'alt risc i les obligacions de les persones proveïdores dels models de propòsit general.

Finalment, destaquem la [publicació *Keep your AI claims in check* de la Federal Trade Commission](#) d'Estats Units.

Exemple: Al següent anunci podem veure com el titular que utilitza la companyia d'assegurances Mapfre fa referència a una hipèrbole de les aptituds de la IA atribuint-li tota la responsabilitat del futur.

Aquest exemple està documentat: [Intel·ligència artificial: el futuro es ahora](#).

4.4.2	Heu pres mesures per garantir que la vostra organització no promet que un sistema d'IA fa alguna cosa millor que un producte que no sigui IA sense proporcionar evidències?
-------	--

Aquesta pregunta fa referència [als articles 13.3, 14.4 i 53.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i la vigilància humana dels sistemes d'alt risc i les obligacions de les persones proveïdores dels models de propòsit general.

També està relacionada amb la [publicació *Keep your AI claims in check* de la Federal Trade Commission](#) d'Estats Units.

Exemple: En una pàgina web de venda d'electrodomèstics anuncia la perfecció que assoleix un robot de cuina en prepara una recepta en comparació amb un restaurant concret.

4.5. Promoció d'una cultura de l'ètica i responsabilitat relacionada amb la IA

Nº	Preguntes
----	-----------

4.5.1	La vostra organització té un codi ètic per l'ús responsable de la IA?
-------	--

Des de la perspectiva jurídica, aquesta pregunta es fonamenta en [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre els codis de conducta d'aplicació voluntària.

La pregunta també està relacionada amb [l'article 9 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que

versa sobre la responsabilitat i el retiment de comptes pels perjudicis derivats de l'ús de la IA.

Exemple: La vostra organització crea un codi amb directrius sobre com utilitzar la IA de manera responsable d'acord amb criteris ètics. En aquest sentit destaquem [l'Institut de responsabilitat de la IA](#), una organització global i sense ànim de lucre dedicada a permetre la IA responsable, que compta amb diversos recursos perquè les organitzacions puguin assolir aquest fi.

4.5.2

La vostra organització incentiva al seu personal a promoure una IA responsable a través d'un/a responsable d'ètica de la IA en la mateixa organització?

Des de la perspectiva jurídica, aquesta pregunta es fonamenta en [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre els codis de conducta d'aplicació voluntària.

La pregunta també està relacionada amb [l'article 9 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la responsabilitat i el retiment de comptes pels perjudicis derivats de l'ús de la IA.

Així mateix, està relacionada amb les [Recomanacions ètiques de la IA de l'UNESCO](#) on es fa un recull de valors i principis en l'ús de la IA destacant com a cabdal la responsabilitat.

Exemple: Un dels nous llocs de feina que implicarà la IA és la creació de la figura del responsable d'ètica que haurà de desenvolupar les tasques de control de les fases i contingut del sistema així com, dur a terme accions per a incentivar a la resta de persones treballadores. Poques empreses l'han començat a implantar, però si que s'ha descrit les funcions d'aquest.

Aquest exemple està documentat: [What Does An AI Ethics Officer Do?](#)

4.5.3

Considerem que la IA responsable és una prioritat de la vostra organització i això es reflecteix en els objectius dels sistema d'IA així com en les revisions del seu rendiment?

Des de la perspectiva jurídica, aquesta pregunta es fonamenta en [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre els codis de conducta d'aplicació voluntària.

La pregunta també està relacionada amb [l'article 9 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la responsabilitat i el retiment de comptes pels perjudicis derivats de l'ús de la IA.

Així mateix, està relacionada amb les [Recomanacions ètiques de la IA de l'UNESCO](#) on es fa un recull de valors i principis en l'ús de la IA destacant com a cabdal la responsabilitat.

4.5.4 **Us heu assegurat que el vostre sistema d'IA, quan s'utilitza per decidir sobre l'elegibilitat de serveis públics o privats, aborda de manera responsable les implicacions per als drets i el benestar de les persones?**

Aquesta pregunta es fonamenta en [als articles 27.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen l'avaluació de l'impacte dels sistemes d'alt risc sobre els drets fonamentals i els codis de conducta d'aplicació voluntària.

Així mateix, està relacionada amb [les Recomanacions ètiques de la IA de l'UNESCO](#) on es fa un recull de valors i principis en l'ús de la IA destacant com a cabdal la responsabilitat.

Exemple: Implementar controls per evitar prejudicis injustos i realitzar proves exhaustives per garantir que les decisions siguin respectuoses amb els drets humans i el benestar de les persones usuàries.

7.2.5. Principi 5: Privacitat

La privacitat és percep com un valor fonamental relacionat amb la protecció i el tractament de les dades, la personalització de la informació, la transparència i la supervisió dels processos. Les aplicacions d'IA, pel fet de requerir grans quantitats de dades, plantegen un risc per a la privacitat. Per aquest motiu, és indispensable que la privacitat es consideri com un element integrat des del disseny mateix dels sistemes d'IA. Això significa que les persones usuàries han de tenir un control efectiu i accés directe a les dades que es recopilen sobre ells, i a més, han de proporcionar un consentiment informat per a l'ús d'aquestes dades.

La privacitat no només és tracta d'una qüestió tècnica, sinó d'un dret que ha de ser protegit per garantir la dignitat i autonomia de les persones. Per aquesta raó, a més de garantir els drets de privacitat i la protecció de dades, els sistemes d'IA han d'assegurar una gestió adequada de les dades, establint mecanismes de governança que legitimen l'accés i l'ús d'aquestes. En aquest context, la regulació té un paper clau per assegurar que la privacitat sigui considerada un dret humà fonamental. Això implica que els desenvolupadors i les organitzacions que utilitzen sistemes d'IA han de prioritzar la protecció de les dades personals dels usuaris, veient la privacitat no només com un requisit tècnic, sinó com un valor ètic i legal indispensable.

En aquest apartat de la privacitat, cal subratllar que, sempre que sigui possible, la recollida i l'ús de dades personals ha de ser mínim, limitant-se a allò que sigui estrictament necessari i pertinent per a la finalitat del sistema d'IA. Aquesta pràctica no només protegeix els drets dels individus, sinó que també fomenta la confiança en l'ús d'aquestes tecnologies, assegurant que la privacitat sigui respectada en totes les fases del procés.

Les preguntes d'aquest apartat provenen majoritàriament de les seccions relatives a privacitat i governança de dades dels diferents instruments i recomanacions consultades. La referència a la **AI Act** es fonamenta amb els articles 10, 13, 17, 27, 50, 55, 72 i 95.

Tot i que l'accés a la informació, la desagregació de les dades i fins i tot la compartició de dades amb altres entitats tenen una importància cabdal per al desenvolupament i traçabilitat dels sistemes d'IA, aquestes activitats no s'han de portar a terme de manera que es malmetí la intimitat de les persones, sobretot si es troben afectades dades de característiques sensibles (com per exemple ètnia, identitat de gènere o estat de salut)⁷². Per aquest motiu, és necessari que les dades utilitzades pels sistemes d'IA, siguin dades d'entrenament o recollides a posteriori, siguin governades de manera que es protegeixi la privacitat de les persones afectades, incloent-hi el dret dels individus a controlar les seves dades⁷³.

En aquest sentit, l'article 11 del Conveni marc sobre intel·ligència artificial i drets humans, democràcia i l'estat de dret contempla el principi de privacitat i protecció de dades personals, en virtut del qual resulta essencial prendre mesures per garantir que la privacitat i les dades dels individus siguin protegits, d'acord amb la normativa internacional i domèstica aplicable a la matèria.

Si bé el dret a la privacitat (les persones han de poder tenir el control sobre la informació relativa a elles mateixes, qui l'obté, i per a què s'utilitza) i el dret a la protecció de dades (tutela de dades categoritzades com sensibles) estan estretament vinculats, han estat comunament reconeguts mundialment com dos drets separats⁷⁴. La privacitat ha estat reconeguda com a dret humà o fonamental a diversos instruments, inclosos l'article 12 de la Declaració universal dels drets humans; els articles 8 i 14 del Conveni europeu de drets humans; els articles 17 i 26 del Pacte internacional de drets civils i polítics; i els articles 7, 8, 21 i 26 de la Carta de drets fonamentals de la UE; l'article 15 de la Carta social europea;

D'altra banda, segons Supervisor Europeu de Protecció de Dades, la protecció de dades consisteix en "*protegir qualsevol identificació relativa a una persona física (viva) identificada o identificable, incloent noms, dates de naixement, fotografies, seqüències de visió, adreces de correu electrònic i números de telèfon*"⁷⁵. Al contrari que la privacitat, la protecció de dades no ha estat reconeguda com un dret humà en si mateix. Tot i això, es tracta d'un element essencial per a la garantia d'altres drets que sí han estat categoritzats com a tal. Per aquest motiu, el Consell d'Europa va aprovar el Conveni per a la protecció de les persones respecte al tractament automatitzat de dades de caràcter personal (Conveni 108).

La Regulació 2022/868, de 30 de maig del 2022 relativa a la governança de dades ha comportat opinions controvertides, ja que si bé molts actors afirmen haver sotmès els seus sistemes a avaluacions d'impacte en la protecció de dades en compliment de la normativa comunitària en la

⁷² ACNUDH (2018) Un enfocament de les dades basades en els drets humans: no deixar a ningú endarrere en l'Agenda 2030 per al Desenvolupament Sostenible. Disponible a: [GuidanceNoteonApproachtoData.pdf\(ohchr.org\)](#) (consultada el 20 de novembre de 2023).

⁷³ Comitè ad hoc sobre intel·ligència artificial del Consell d'Europa (2021) Intel·ligència artificial, drets humans, democràcia i estat de dret: Introducció. Disponible a: <https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a> (consultada el 7 de novembre de 2023).

⁷⁴ European Data Protection Supervisor (2023) Protecció de dades. Disponible a: [Data Protection | European Data Protection Supervisor \(europa.eu\)](#) (consultada el 26 de novembre de 2023).

⁷⁵ European Data Protection Supervisor (2023) Protecció de dades. Disponible a: [Data Protection | European Data Protection Supervisor \(europa.eu\)](#) (consultada el 26 de novembre de 2023).

matèria, aquests rarament preveuen l'impacte sobre els drets⁷⁶. En conseqüència, les mesures comunament preses fins ara no resulten suficients per garantir que el sistema d'IA és respectuós des d'un punt de vista ètic.


Tenint en compte l'articulat del Reglament 2016/679, de 27 d'abril del 2016 relatiu a la Protecció de Dades de la UE i la Directiva 2016/680, de 27 d'abril del 2016 relativa a la protecció de dades amb fins de prevenció, investigació, detecció, enjudiciament o execució d'infraccions penals és convenient esmentar la responsabilitat en la qual incorrerien les persones. Es a dir, si en l'ús d'un sistema d'IA de bot conversacional centrat en la usabilitat i el diàleg com podria ser el *Chat GPT* hi aboquessin dades de naturalesa sensible o personal. Aquestes dades serien registrades pel propi sistema d'IA per tal d'autogenerar-se i, per tant, perdrien llur naturalesa de privades o reservades perquè serien utilitzades en futurs usos del sistema.

Recordar doncs que les dades determinades com a personals o sensibles tenen la naturalesa de Drets fonamentals de les persones i gaudeixen d'una protecció jurídica reforçada. Així doncs, la seva lesió o vulneració implica incorre en responsabilitat penal⁷⁷. Es per això que també hem referenciat el Reglament 2018/1725, de 23 d'octubre del 2018, relatiu a la protecció de dades tractades per institucions, òrgans i organismes de la UE. Altrament, l'àmbit territorial d'aplicació del Reglament és efectiu fins i tot si les dades són tractades més enllà del territori de la Unió Europea.

D'altra banda, en base aquesta regulació i conflicte, la doctrina ha creat el terme "responsabilitat proactiva" per tal de garantir la protecció i privadesa de les dades personals en totes les fases d'un sistema des que s'inicia llur ús. A més a més, es exigida a tots els agents que poden interactuar amb les mateixes i la tutela implica el tractament, consideració, anonimització i finalment, avaluar-ne l'impacte.

Recordar doncs que les dades determinades com a personals o sensibles tenen la naturalesa de Drets fonamentals de les persones i gaudeixen d'una protecció jurídica reforçada. Així doncs, la seva lesió o vulneració implica incorre en responsabilitat penal⁷⁸ i l'àmbit d'aplicació del Reglament és efectiu fins i tot, si les dades són tractades més enllà del territori de la Unió Europea.

5.1. Protecció de la privacitat

Nº	Preguntes
5.1.1* 	Heu establert mecanismes de protecció de dades per tal que les dades de caràcter personal siguin tractades amb el grau de protecció legalment

⁷⁶ FRA (2021) Encertar amb el futur. Intel·ligència artificial i drets fonamentals.

Capítol VIII: recursos, responsabilitats i sancions, Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques respecte al tractament de dades personals i la lliure circulació d'aquestes dades. Disponible a: [*Getting the future right. Artificial intelligence and fundamental rights\(europa.eu\)](https://eur-lex.europa.eu/eli/reg/2016/679/oj) (consultada el 21 de novembre de 2023).

Capítol VIII: recursos, responsabilitats i sancions, Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques respecte al tractament de dades personals i la lliure circulació d'aquestes dades.

requerit i així evitar-ne el mal ús, alteració, pèrdua o sostracció per part de tercers?

Aquesta pregunta fa referència [als articles 10.5, 50.3 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la governança de dades i les obligacions dels sistemes de reconeixement d'emocions, categorització biomètrica i de propòsit general de risc sistemàtic. Legalment també destaquem [l'article 32 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre la seguretat de les dades personals.

La pregunta també es basa en [l'article 21 de la Regulació 2022/868, de 30 de Maig del 2022 \[Llei Europea sobre la Governança de dades\]](#), sobre els requisits específics per a protegir els drets i els interessos de les persones interessades i titulars de dades perquè respecta a les seves dades.

Així mateix, la pregunta està relacionada amb [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals; i [l'article 7 del Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals](#), que versa sobre la seguretat de les dades.

En aquest sentit, la qüestió guarda relació amb el principi [Privacy del document A Human Rights-Based Approach To Data](#) de l'ACNUDH, les recomanacions contingudes al [toolkit d'ICO sobre riscos i protecció de dades en la IA](#) i està relacionada amb l'apartat [Privacy and Security de l'AI Ethics Assessment de GSMA](#).

Exemple: D'acord amb la [Comissió Federal de Comerç dels EEUU](#) (FTC per les seves sigles en anglès) *Ring*, la filial de càmeres de seguretat d'Amazon, compta amb laxes mesures de seguretat que han permès a pirates informàtics prendre el control de diversos comptes. A més, el sistema permet que els seus empleats tinguin accés als vídeos privats dels consumidors.

5.1.2*

Heu establert mecanismes de protecció de dades per tal que les dades de caràcter personal subministrades per la persona interessada no siguin venudes, llogades ni cedides, sense el seu consentiment?

Aquesta pregunta fa referència [als articles 10.5, 17.1 50.3 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i el sistema de gestió de qualitat dels sistemes d'alt risc, així com les obligacions dels sistemes de reconeixement d'emocions, categorització biomètrica i de propòsit general de risc sistemàtic.

La pregunta també està relacionada amb [els articles 6 i 7 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versen sobre la licitud del tractament de dades i el consentiment dels afectats, i [l'article 21 de la Regulació 2022/868, de 30 de Maig del 2022 \[Llei Europea sobre la Governança de dades\]](#), sobre els requisits específics per a protegir els drets i els interessos de les persones interessades i titulars de dades perquè respecta a les seves dades.

Així mateix, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i, sobre el dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals; i [l'article 7 del Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals](#), que versa sobre la seguretat de les dades. [17 del Pacte internacional de drets civils i polítics](#), sobre el Dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals; i [l'article 7 del Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals](#), que versa sobre la seguretat de les dades.

En aquest sentit, la qüestió guarda relació amb el principi [Privacy del document A Human Rights-Based Approach To Data de l'ACNUDH](#) i les recomanacions contingudes al [toolkit d'ICO sobre riscos i protecció de dades en la IA](#).

Exemple: L'empresa *Meta* va ser multada el maig de 2023 per violar la Llei de Protecció de Dades incomplint amb la sol·licitud del consentiment de deure de protecció de les dades personals, tal com s'explica als següents articles: [This article is more than 4 months old Facebook owner Meta fined €1.2bn for mishandling user information](#), [Meta Fined \\$1.3 Billion for Violating E.U. Data Privacy Rules](#) i [Meta slapped with record \\$1.3 billion EU fine over data privacy](#).

5.1.3*

Heu establert processos per mantenir o millorar la privacitat i la protecció de dades al llarg del cicle de vida del vostre sistema d'IA?

Aquesta pregunta fa referència [als articles 10.5, 17.1, 50.3, 55.1 i 72 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i el sistema de gestió de qualitat dels sistemes d'alt risc, les obligacions dels sistemes de reconeixement d'emocions, categorització biomètrica i de propòsit general de risc sistemàtic, així com el seguiment post-comercialització.

Destaquem també [l'article 32 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre la seguretat de les dades personals.

Així mateix, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; i [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

En aquest sentit, la qüestió guarda relació amb el principi [Privacy del document A Human Rights-Based Approach To Data de l'ACNUDH](#), les recomanacions contingudes a [l'apartat 2.2.3. Privacy d'AIEIG](#) i a l'apartat de [Privacy and Data Governance d'ALTAI](#).

Exemple: El [sistema VEIL.AI](#) desenvolupat per l'empresa finlandesa homònima, sintetitza i anonimitza dades sensibles en matèria sanitària per donar lloc a un millor ús per a la investigació, el desenvolupament i la innovació.

Aquest exemple està documentat a: [Finnish health tech startup receives capital for better use of GDPR-free data.](#)

5.1.4*



Heu establert un mecanisme a través del qual una persona pot sol·licitar que la seva informació personal sigui eliminada?

Aquesta pregunta fa referència [als articles 10.5, 17.1 i 50.3 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i els sistema de gestió de qualitat dels sistemes d'alt risc, així com les obligacions de les persones proveïdores dels sistemes de reconeixement d'emocions i categorització biomètrica.

Altres normes a destacar són [l'article 17 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre el dret a la supressió o dret a l'oblit, i [l'article 21 de la Regulació 2022/868, de 30 de Maig del 2022 \[Llei Europea sobre la Governança de dades\]](#), sobre els requisits específics per a protegir els drets i els interessos de les persones interessades i titulars de dades perquè respecta a les seves dades.

Així mateix, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals; i [l'article 8 del Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals](#), que versa sobre les garanties de la persona afectada.

Finalment destaquem les recomanacions contingudes a [l'apartat 2.2.3. Privacy d'AIEIG](#) i a l'apartat de [Privacy and Data Governance d'ALTAI](#).

Exemple: El producte d'Amazon, [Amazon Rekognition](#), reconeix les emocions de les persones que apareixen a les imatges que analitza i n'estableix categories biomètriques.

Les persones usuàries tenen el dret de poder sol·licitar l'eliminació de les seves dades personals, ja sigui mitjançant una adreça de correu electrònic, assistència telefònica, sol·licitud per escrit o sistema de tiquets o incidències.

5.1.5*



Heu establert un protocol per obtenir el consentiment abans d'iniciar qualsevol processament o anàlisi a través del vostre sistema d'IA?

Aquesta pregunta fa referència [als articles 10.5, 17.1, 50.3 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i els sistema de gestió de qualitat dels sistemes d'alt risc, així com les obligacions de les persones proveïdores de sistemes de categorització biomètrica, reconeixement d'emocions i de propòsit general de risc sistemàtic.

Altres normes destacables són, [l'article 7 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#), que versa sobre les condicions per al consentiment de la persona afectada, i [l'article 21 de la Regulació 2022/868, de 30 de Maig del 2022 \[Llei Europea sobre la Governança de dades\]](#), sobre els requisits

específics per a protegir els drets i els interessos de les persones interessades i titulars de dades perquè respecta a les seves dades.

Així mateix, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; i [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

En aquest sentit, la pregunta també està relacionada amb el principi [Privacy del document A Human Rights-Based Approach To Data](#) de l'ACNUDH, a les recomanacions contingudes al [toolkit d'ICO sobre riscos i protecció de dades en la IA](#).

Exemple: El govern de Corea va lliurar aproximadament 170 milions d'imatges facials de persones coreanes i estrangeres, sense llur consentiment, a una empresa privada perquè desenvolupés una eina d'IA d'identificació biomètrica amb la finalitat de ser utilitzada pel control migratori.

Aquest exemple està documentat a: [El Gobierno entrega 170 millones de fotos de inmigrantes a una empresa de inteligencia artificial](#).

5.1.6*



La informació sobre el consentiment i la seva revocació és comprensible i accessible per totes les persones usuàries, incloent aquells que pertanyen a grups vulnerables, persones amb problemes d'accessibilitat o necessitats especials?

Aquesta pregunta fa referència [als articles 10.5, 13, 50.5 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades, les obligacions de les persones proveïdores dels sistemes de propòsit general, d'IA generativa, els sistemes de categorització biomètrica i de reconeixement d'emocions i altres sistemes que interactuïn amb persones físiques, i sobre els codis de conducta d'aplicació voluntària.

La pregunta també és fonamenta en [l'article 7 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre les condicions per al consentiment de la persona afectada.

Així mateix, la pregunta està relacionada amb [els articles 8, 11 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió dels sistemes d'IA, la privacitat i protecció de dades personals i els drets de les persones amb discapacitat i dels infants; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; i [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

Finalment, destaquem també les recomanacions contingudes a [l'apartat 2.2.3. Privacy d'AIEIG](#) i a l'apartat de [Privacy and Data Governance d'ALTAI](#).

5.1.7*



Exemple: El text en el qual s'informa sobre el consentiment per a l'ús de les dades i la seva revocació hauria d'utilitzar una construcció i llenguatge clara, i desitjablement anar acompanyat d'eines que permetin la seva lectura i comprensió amb persones amb diferents necessitats, com ara text vocal o àudio interactiu.

L'acceptació de les condicions en el vostre sistema d'IA implica la pèrdua de la privacitat de la persona usuària?

Aquesta pregunta fa referència [als articles 10.5, 17.1 i 50.3 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i el sistema de gestió de qualitat dels sistemes d'alt risc, i les obligacions de les persones proveïdores de sistemes de reconeixement d'emocions i de categorització biomètrica.

Així mateix, la pregunta també està relacionada amb [els articles 5, 25 i 32 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) sobre l'exigibilitat de la responsabilitat i llur amplitud; la previsió d'aquesta ja a la fase del disseny i durant el seu efecte; i l'obligatorietat d'anonimitzar i xifrar les dades personals, i [l'article 21 de la Regulació 2022/868, de 30 de Maig del 2022 \[Llei Europea sobre la Governança de dades\]](#), sobre els requisits específics per a protegir els drets i els interessos de les persones interessades i titulars de dades perquè respecta a les seves dades.

Per l'altra banda, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; i [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

Exemple: La Comissió Federal de Comerç dels Estats Units va descobrir que Amazon conservava els vídeos i les gravacions de veu recollides i informació de geolocalització relacionada amb els mateixos que havien estat enregistrades pels seus productes, *Ring* i *Alexa*, malgrat les peticions d'algunes persones usuàries perquè aquestes dades fossin eliminades.

Aquest exemple està documentat a: [Amazon to pay more than \\$30 million to settle FTC privacy complaints over Alexa and Ring.](#)

5.1.8*



El vostre sistema d'IA incorpora mesures per protegir la privadesa i prevenir la discriminació contra grups vulnerables?

Aquesta pregunta fa referència [als articles 10.5, 17.1, 27.1, 50.3, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i el sistema de la gestió de qualitat dels sistemes d'alt risc, l'avaluació de l'impacte del sistema d'alt risc sobre els drets fonamentals, les obligacions de les persones proveïdores de sistemes de reconeixement d'emocions, de categorització biomètrica i de propòsit general, i l'adopció de codis de conducta d'aplicació voluntària.

La pregunta també està relacionada amb [l'article 32 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre la seguretat de les dades personals.

Així mateix, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals; i en el dret Humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), [l'article 21 de la Carta de drets fonamentals de la UE](#), i [l'article 26 del Pacte internacional de drets civils i polítics](#).

En aquest sentit, la qüestió guarda relació amb el principi [Privacy del document A Human Rights-Based Approach To Data de l'ACNUDH](#), les recomanacions contingudes a [l'apartat 2.2.3. Privacy d'AIEIG](#) i [l'apartat de Fairness and non-discrimination de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#).

Exemple: Dos investigadors de la Universitat de Standford han desenvolupat un sistema d'identificació biomètrica que identifica la orientació sexual de les persones a partir de fotografies de la seva cara.

Aquest exemple està documentat a: [Researchers use facial recognition tools to predict sexuality lgbt groups arent happy](#).

5.1.9*



Us heu assegurat que el vostre sistema d'IA utilitza tècniques de preservació de la privadesa durant el seu desenvolupament?

Aquesta pregunta fa referència [als articles 10.5, 17.1, 50.3 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), de la Comissió Europea que versen sobre la governança de dades; el sistema de gestió de qualitat dels sistemes d'alt risc; les obligacions de les persones proveïdores de sistemes de reconeixement d'emocions; de categorització biomètrica; i de propòsit general de risc sistemàtic.

Així mateix, la pregunta està relacionada amb [l'article 32 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre la seguretat de les dades personals.

D'altra banda, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el Dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

En aquest sentit, la qüestió guarda relació amb el principi [Privacy del document A Human Rights-Based Approach To Data de l'ACNUDH](#) i les recomanacions contingudes a [l'apartat 2.2.3. Privacy d'AIEIG](#).

5.1.10*



Exemple: El risc que ha demostrat que plantegen les *Smart Toys* requereix que s'acompanyin de tècniques com l'anonimització de dades personals, la implementació de protocols de seguretat robustos i la incorporació de controls d'accés per limitar l'accés a la informació sensible només a personal autoritzat. Aquest exemple està documentat a:

<https://ticnegocios.camaravalencia.com/servicios/noticias/smart-toys/>.

Feu servir tècniques d'anonimat i xifratge per garantir la privadesa i la protecció de les dades personals en les operacions del vostre sistema d'IA (com el xifratge, l'anonimització o l'agregació) ?

Aquesta pregunta fa referència [als articles 10.5, 17.1, 50.3 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i el sistema de gestió de qualitat dels sistemes d'alt risc i les obligacions de les persones proveïdores de sistemes de reconeixement d'emocions, de categorització biomètrica i de propòsit general de risc sistemàtic.

Així mateix, la pregunta està relacionada amb [l'article 32 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre la seguretat de les dades personals.

D'altra banda, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

En aquest sentit, la qüestió guarda relació amb el principi [Privacy del document A Human Rights-Based Approach To Data de l'ACNUDH](#), les recomanacions contingudes a [l'apartat 2.2.3. Privacy d'AIEIG](#) i a l'apartat de [Privacy and Data Governance d'ALTAI](#).

Exemple: L'empresa *Afectiva* utilitza algoritmes d'aprenentatge automàtic avançats i visió per ordinador per detectar i analitzar les expressions emocionals de les persones a partir d'imatges de vídeo en temps real o capturades. Hauria de substituir tals dades identificatives per identificadors aleatoris en els conjunts de dades, tot i que aquesta informació no s'ha pogut trobar.

Aquest exemple està documentat a: <https://www.affectiva.com/>

5.1.11*



El disseny i el desplegament del vostre sistema d'IA garanteix l'accés igualitari i la no discriminació per a les persones amb discapacitat alhora que respecta la seva privadesa i dignitat?

Aquesta pregunta fa referència [als articles 10.5, 27.1, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la governança de dades; l'avaluació de l'impacte del sistemes d'alt risc sobre els drets fonamentals; les obligacions de les persones proveïdores dels models de propòsit general de risc sistemàtic; i als codis de conducta d'aplicació voluntària.

La qüestió també es fonamenta en [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA i [l'article 5 del Reglament](#)

[2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#) que versa sobre els principis del tractament de dades.

D'altra banda, la pregunta està relacionada amb [els articles 10, 11 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació, la privacitat i protecció de dades personals i els drets de les persones amb discapacitat i dels infants; [l'article 26 de la Carta de drets fonamentals de la UE](#) relatiu a la integració de les persones amb discapacitat i [l'article 15 de la Carta social europea](#) sobre el dret de les persones amb alguna discapacitat a la integració social i la vida en comunitat; el dret humà a la no discriminació, consagrat a [l'article 14 del Conveni europeu de drets humans](#), i [l'article 26 del Pacte internacional de drets civils i polítics](#); el dret humà a la privacitat, reconegut a [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#); [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals; i [l'article 7 del Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals](#), que versa sobre la seguretat de les dades.

Finalment, destaquem també l'apartat de [Right to Privacy, and Data Protection de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#).

Exemple: Incorporar funcionalitats d'accessibilitat com el suport per a tecnologies d'assistència i l'adaptabilitat de la interfície d'usuari, alhora que s'assegura que les dades personals de les persones amb discapacitat estiguin protegides mitjançant l'aplicació de tècniques de privacitat i seguretat adequades.

5.2. Governança de dades

Nº	Preguntes
----	-----------

5.2.1*	Heu establert un registre de la informació d'accés a les dades (personals o no) per identificar clarament quan, qui i amb quin propòsit ha accedit a les dades?
--------	--



Aquesta pregunta fa referència [als articles 10.5 i 50.3 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i les obligacions de les persones proveïdores de sistemes de reconeixement d'emocions i categorització biomètrica.

També és relaciona amb [l'article 30 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#), sobre el registre de les activitats de tractament. Així mateix, destaquem [l'article 20 de la Regulació 2022/868, de 30 de Maig del 2022 \[Llei Europea sobre la Governança de dades\]](#), sobre els requisits de transparència i el registre de les persones a les que se les ha permès el tractament de les dades.

Així mateix, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la

privacitat; i [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

Finalment, destaquem les recomanacions contingudes a l'apartat de [Privacy and Data Governance d'ALTAI](#).

5.2.2

Us heu assegurat que les persones que realitzen el processament i gestió de dades compten amb les competències necessàries i es mantenen al dia amb els nous desenvolupament per a comprendre i dur a terme la política de protecció de dades?

Aquesta pregunta fa referència [als articles 10 i 14 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a la governança de dades i la vigilància humana de sistemes d'IA.

Així mateix, la pregunta es fonamenta en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; i [l'article 8 de la Carta de drets fonamentals de la UE](#) la protecció de dades personals.

Destaquem també, les recomanacions contingudes a l'apartat de [Privacy and Data Governance d'ALTAI](#).

Exemple: La següent eina formativa de Certifai: [AI Data Annotation • CertifAI • Accredible • Certificates, Badges and Blockchain](#).

5.2.3

Heu establert els procediments per assegurar que els conjunts de dades siguin els adients i rellevants pel correcte rendiment i resultat previst del model?

Aquesta pregunta fa referència [als articles 10.3, 13.3 i 17.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades, la transparència i els sistema de gestió de qualitat dels sistemes d'alt risc.

Així mateix, la pregunta es relaciona amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

Per l'altra banda, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA.

Destaquem també les recomanacions contingudes a [l'apartat de Privacy and Data Governance d'ALTAI](#).

5.2.4*

Heu documentat el procés de recopilació i preparació de les dades pel vostre sistema d'IA?

Aquesta pregunta fa referència [als articles 10, 17.1 i 53.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la

governança de dades i el sistema de gestió de qualitat dels sistemes d'alt risc i les obligacions de les persones proveïdores dels sistemes de propòsit general.

Per l'altra banda, la pregunta es fonamenta en [els articles 8 i 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la transparència i supervisió i la fiabilitat dels sistemes d'IA.

Així mateix, la pregunta està relacionada amb la [Secció 1 del capítol IV del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#), que regula les obligacions legals dels responsables del tractament de dades i el seu règim de responsabilitat, així com [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#) relativa a la presumpció de culpa dels danys provocats per una IA.

Destaquem també, les recomanacions contingudes a [l'apartat de Privacy and Data Governance d'ALTAI](#).

Exemple: Una empresa que ha documentat en un protocol de manera definida els objectius, les necessitats i el procés de recopilació de les dades, la normalització i estandardització o el control de qualitat.

5.2.5

El conjunt de dades recopilades per entrenar el vostre sistema són adequades pel context en el qual serà utilitzat (per exemple, les dades són representatives del territori on s'utilitza el sistema) ?

Aquesta pregunta fa referència [als articles 10.4 i 17.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i el sistema de gestió de qualitat dels sistemes d'IA d'alt risc.

Així mateix, es relaciona amb [l'article 4.2 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relatiu a la presumpció de culpa dels danys provocats per una IA.

Per l'altra banda, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA.

Així mateix, la pregunta està relacionada amb el principi [Participation del document A Human Rights-Based Approach To Data de l'ACNUDH](#) i el principi [Participation del document A Human Rights-Based Approach To 2018/](#).

5.2.6

El vostre sistema d'IA està dissenyat per adherir-se als principis de minimització de dades i protecció de dades des del disseny i per defecte, tal com exigeixen les Lleis de Protecció de Dades?

Aquesta pregunta es fonamenta en [els articles 10.5 i 17.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la governança de dades i el sistema de gestió de qualitat, així com [l'article 4.3 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

A més, la pregunta està relacionada amb [els articles 5 i 25 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#), [l'article 10 i l'article 20 de la Directiva 2016/680, de 27 d'abril de 2016, \[Directiva de protecció de dades amb fins de prevenció, investigació, detecció, enjudiciament o execució d'infraccions penals\]](#). També [els articles 4 i 27 Reglament 2018/1725, de 23 d'octubre de 2018, \[Reglament de protecció de dades tractades per institucions, òrgans i organismes de la Unió\]](#), que versen sobre el tractament de categories especials de dades personals.

Així mateix, la pregunta es basa en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el Dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

Exemple: La recopilació i el processament de la menor quantitat de dades necessària per a l'objectiu previst.

5.2.7 ● **Heu implementat tecnologies que permeten entrenar el vostre sistema d'IA sense necessitat de transmetre o copiar dades en brut o estructurades, millorant així la privadesa de les dades?**

Aquesta pregunta es fonamenta en [l'article 10.5 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la governança de dades.

Així mateix, la pregunta està relacionada [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#) sobre el dret humà a la privacitat; i [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

Destaquem [el llibre blanc de la Comissió Europea sobre IA, un enfocament europeu d'excel·lència i confiança](#) on a l'apartat cinquè fixa alteratives de l'ús massiu de dades d'acord amb la normativa de la UE.

Exemple: El sistema *K-means clustering* (*Agrupament K-means*) és un algoritme d'aprenentatge no supervisat que agrupa dades en funció de similitud entre elles sense cap etiqueta prèvia i intenta trobar patrons o estructures.

Com veiem, l'aprenentatge no supervisat és un exemple de sistema d'IA que pot treballar amb dades sense etiquetar.

Aquest exemple està documentat a: [El algoritmo k-means aplicado a clasificación y procesamiento de imágenes](#) i [Algoritmo k-means: ¿Qué es y cómo funciona?](#).

5.2.8 ● **El vostre sistema d'IA limita la reutilització de dades personals sensibles i utilitza mesures avançades de seguretat i privadesa com la pseudonimització?**

Aquesta pregunta es fonamenta en [l'article 10.5 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la

governança de dades, així com [l'article 4.3 de la proposta de directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial \(AI Liability Directive\)](#), relativa a la presumpció de culpa dels danys provocats per una IA.

A més, la pregunta està relacionada amb [l'article 9 del Reglament 2016/679, de 27 d'abril 2016 \[Reglament general de protecció de dades\]](#), [l'article 10 del Reglament 2018/1725, de 23 d'octubre de 2018, \[Reglament de protecció de dades tractades per institucions, òrgans i organismes de la Unió\]](#) que versen sobre el tractament de categories especials de dades personals.

Així mateix, la pregunta es basa en [l'article 11 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la privacitat i protecció de dades personals; [l'article 12 de la Declaració universal dels drets humans](#), [l'article 8 del Conveni europeu de drets humans](#), i [l'article 17 del Pacte internacional de drets civils i polítics](#), sobre el dret humà a la privacitat; [els articles 7 i 8 de la Carta de drets fonamentals de la UE](#) sobre la privacitat i la protecció de dades personals.

Exemple: L'anàlisi de nòmina és un exemple de funcionalitat que analitza dades proporcionades per recursos humans que està anonimitzat. Aquesta funcionalitat l'inclou l'empresa ADP tal i com preveu a la seva política de privacitat i com també se'n fa ressò aquest article.

Aquest exemple està documentat a: [Política de Privacidad en ADP](#) i [¿Qué información pueden extraer las empresas gracias al Big Data?](#).

7.2.6. Principi 6: Autonomia

Les organitzacions que utilitzen sistemes d'IA han d'assegurar-se que el "principi de l'autonomia de la persona usuària sigui central en el funcionament dels seus sistemes. L'autonomia es refereix a la capacitat de les persones usuàries per exercir la seva llibertat com a individus davant els sistemes d'IA, eliminant la dependència d'aquests envers els models de presa de decisions automatitzades. En les societats democràtiques, l'autonomia es valora especialment ja que està vinculada a la protecció de la llibertat i a garantir que la IA s'utilitzi sense interferir ni perjudicar els individus.

Així doncs, els sistemes d'IA han de ser dissenyats per fomentar l'empoderament de les persones, permetent-los prendre decisions informades i promovent la protecció dels seus drets fonamentals. Això requereix que els sistemes estiguin dissenyats d'una manera que garanteixin la transparència, el consentiment clar en l'accés a la informació necessària perquè les persones entenguin com s'utilitzen les seves dades i puguin actuar en conseqüència. La regulació juga aquí un paper essencial, ja que ajuda a establir un marc de protecció per a l'autonomia de la persona usuària i assegura que les tecnologies no perjudiquin la seva llibertat ni els seus drets bàsics.

Per tant, aquest principi proposa garantir que els sistemes d'IA respectin els drets humans, la diversitat i l'autonomia de les persones. Les preguntes d'aquest apartat provenen majoritàriament de les seccions relatives a l'agència humana i autonomia dels diferents instruments i recomanacions consultades, i troben la seva referència normativa en els articles 9, 13, 14, 15, 27, 50, 55, 72 i 95 de la **AI Act**.

Segons el **Comitè ad hoc** del sobre Intel·ligència Artificial del Consell d'Europa, l'autonomia és la capacitat de cada individu per prendre decisions i requereix tenir a disposició informació suficient i fiable que permeti escollir de forma conscient⁷⁹. D'acord amb el Comitè, en termes de drets humans aquesta definició de l'autonomia no només es refereix al dret a la informació, sinó que es troba intrínsecament vinculada al concepte de dignitat humana, ja que un aspecte important de la dignitat és la capacitat d'autodeterminació, que es tradueix en la capacitat de prendre decisions lliurement.⁸⁰

És per aquest motiu que el Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret tracta aquests dos conceptes de manera conjunta a l'article 7, titulat *dignitat humana i autonomia individual*. D'acord amb aquest precepte, les parts del Conveni hauran d'adoptar mesures per tal que els sistemes d'IA respectin la dignitat humana i l'autonomia personal durant tot el seu cicle de vida. Tenint en compte la capacitat dels sistemes d'IA per a la imitació i manipulació, l'article 7 requereix l'adopció de garanties que permetin a les persones tenir control sobre l'ús i l'impacte de la intel·ligència artificial a les seves vides⁸¹.

Com s'ha explicat, l'autonomia permet a les persones prendre decisions lliurement. Per tant, també està relacionada amb el dret humà a la llibertat⁸², consagrat a l'article 5 del Conveni europeu de drets humans; l'article 3 de la Declaració universal dels drets humans; els articles 6 i 38 de la Carta de drets fonamentals de la Unió Europea; i l'article 9 del Pacte internacional de drets civils i polítics.

Els sistemes d'IA poden perjudicar l'autonomia de les persones que interactuen amb elles o amb els continguts que generen, per exemple, afavorint un sentiment de confiança excessiva en relació amb les decisions que adopta, sobretot quan el seu procés de presa de decisions no és prou transparent per a permetre a la persona usuària utilitzar el resultat del sistema de manera totalment conscient i informada⁸³. De fet, alguns sistemes, estan precisament dissenyats per generar imatges o sons falsos amb un alt grau d'autenticitat (*deepfake*), de manera que resulta gairebé impossible identificar-los com a contingut fictici si no es disposa d'informació contextual.

⁷⁹ Comitè ad hoc sobre intel·ligència artificial del Consell d'Europa (2020) Towards regulation of AI systems. Disponible a: <https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a> (consultada el 10 de desembre de 2023).

⁸⁰ Consell d'Europa (2024) Informe explicatiu al conveni marc del Consell d'Europa sobre la intel·ligència artificial i els drets humans, la democràcia i l'estat de dret. Disponible a: <https://rm.coe.int/1680afae67> (consultada el 20 de juliol de 2024).

⁸¹ *Idem*.

⁸² Comitè ad hoc sobre intel·ligència artificial del Consell d'Europa (2021) Intel·ligència artificial, drets humans, democràcia i estat de dret: Una Introducció. Disponible a: <https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a> (consultada el 7 de novembre de 2023).

⁸³ High-Level Expert Group on Artificial Intelligence (2020) La Llista d'Avaluació per a una Intel·ligència Artificial de Confiança. Disponible a: https://airegio.ems-carsa.com/nfs/programme_5/call_3/call_preparation/ALTAI_final.pdf (consultada el 7 de març de 2023).

És per aquesta raó que el Conveni marc determina que en les situacions en les quals un sistema d'IA informa o pren decisions que poden afectar els drets humans d'una persona, aquesta haurà de ser informada sobre el fet d'estar interactuant amb una IA (article 15.2). El risc és especialment elevat per a persones amb problemes d'accessibilitat o risc d'exclusió⁸⁴.

Per aquest motiu, cal adoptar mesures que permetin garantir que les persones que fan ús dels sistemes d'IA podran escollir sota el seu propi criteri i lliures d'influències entre totes les opcions possibles.

⁸⁴ Comitè ad hoc sobre intel·ligència artificial del Consell d'Europa (2020) Cap a la regulació dels sistemes d'IA. Disponible a: <https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a> (consultada el 10 de desembre de 2023).

6.1. Impacte en les capacitats de les persones usuàries

Nº

Preguntes

6.1.1



Heu establert un procés d'avaluació del vostre sistema d'IA per garantir que en cap cas disminueix el nombre d'eleccions possibles, ni tampoc l'obliga o força a prendre unes determinades decisions?

Aquesta pregunta fa referència a [l'article 13 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la transparència i comunicació d'informació a les persones usuàries.

Així mateix, la pregunta es fonamenta en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la dignitat humana i autonomia individual, així com en el dret a la llibertat, consagrat a [l'article 5 del Conveni europeu de drets humans, article 3 de la Declaració universal dels drets humans, l'article 6 de la Carta de drets fonamentals de la UE i l'article 9 del Pacte internacional de drets civils i polítics](#).

Finalment, destaquem les recomanacions contingudes al [subapartat Human Agency and Autonomy d'ALTAI](#), i està relacionada amb l'apartat [Human Agency & Oversight del AI Ethics Assessment de GSMA](#).

Exemple: El sistema [Workday](#) és un planificador de tasques quotidianes que ha integrat la IA per tal d'identificar oportunitats de creixement i aprenentatge dels empleats i reclutar nous talents de manera més ràpida i eficient. En aquesta funcionalitat ha de garantir que es tracta d'una eina que i no substitueix la capacitat de decisió de la persona usaria.

6.1.2*



Podeu assegurar que el vostre sistema d'IA, durant cap fase del seu cicle de vida, restringeix l'abast de les opcions d'estil de vida, creences, opinions, expressions o experiències personals?

Aquesta pregunta fa referència [als articles 13, 27.1, 55.1, 72 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i comunicació d'informació a les persones usuàries; l'avaluació de l'impacte sobre els drets fonamentals i el monitoratge post-comercialització dels sistemes d'alt risc, i els codis de conducta d'aplicació voluntària.

La pregunta també es fonamenta en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la dignitat humana i autonomia individual, així com en el dret a la llibertat, consagrat a [l'article 5 del Conveni europeu de drets humans, article 3 de la Declaració universal dels drets humans, l'article 6 de la Carta de drets fonamentals de la UE i l'article 9 del Pacte internacional de drets civils i polítics](#).

Finalment, destaquem el [punt 20 de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#), relatiu a la protecció de la diversitat i inclusió, i està relacionada amb [l'apartat Human Agency & Oversight del AI Ethics Assessment de GSMA](#).

6.1.3

Exemple: L'algoritme que utilitza [l'aplicació de cites *Coffee Meets Bagel*](#) recomana a les persones que en són usuàries els perfils de la mateixa ètnia que han indicat en el seu propi perfil. En conseqüència, l'aplicació restringeix la possibilitat de contactar amb persones d'una altra ètnia, fins i tot en els casos on les mateixes usuàries han indicat no tenir cap preferència al respecte.

Heu establert un protocol de comprovació sobre el vostre sistema d'IA que permeti certificar que ajuda les persones a prendre decisions millors i més informades d'acord amb els seus objectius?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que sobre els codis de conducta d'aplicació voluntària.

Per l'altra banda, la pregunta es fonamenta en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la dignitat humana i autonomia individual.

I està relacionada amb les recomanacions contingudes al [subapartat *Human Agency and Autonomy* d'ALTAI](#).

Exemple: Sistema d'IA ajuda a detectar i preveure el càncer de colon mitjançant la colonoscòpia, millorant la qualitat i disminuint els costos innecessaris. Gràcies a la qualitat del cribratge i la vigilància, mesurada per les taxes de detecció d'adenomes, millora la detecció assistida per ordinador en temps real.

Aquest exemple està documentat a: [How Artificial Intelligence Will Impact Colonoscopy and Colorectal Screening](#) i [Application of artificial intelligence in colorectal cancer screening by colonoscopy: Future prospects \(Review\)](#).

6.1.4*

Heu pres mesures per garantir que les persones que interactuen amb el vostre sistema siguin conscients que es tracta d'una IA?

Aquesta pregunta és fonamenta en [els articles 27.1, 50 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre l'avaluació de l'impacte sobre els drets fonamentals dels sistemes d'alt risc sobre les obligacions de les persones proveïdores de sistemes que interactuen amb persones, incloent sistemes d'IA generativa, de reconeixement d'emocions, categorització biomètrica i models de propòsit general, i els codis de conducta d'aplicació voluntària.

També es basa en [els articles 7, 8 i 15.2 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la dignitat humana i autonomia individual, la transparència i supervisió dels sistemes d'IA i el requisit de notificar a les persones quan estan interactuant amb un sistema d'IA. Juntament amb [l'article 38 de la Carta de drets fonamentals de la UE](#) relatiu a la protecció dels consumidors.

Exemple: Quan una usuària demana informació a [ChatGPT](#) sobre qüestions delicades, com per exemple dubtes relatius al seu estat de salut, el sistema d'IA informa que es tracta d'una intel·ligència artificial i no pot oferir els mateixos serveis que un professional de la matèria.

Després d'aquest aclariment proporciona la informació sol·licitada, però la persona usuària està millor posicionada per decidir si confiar en la resposta generada pel sistema, o bé plantejar la qüestió a una persona competent.

6.1.5



Heu establert els mecanismes per assegurar que totes les persones usuàries finals del sistema d'IA tenen prou capacitat i informació per a ser-ho, incloent-hi les persones amb problemes d'accessibilitat o que es troben en risc d'exclusió?

Aquesta pregunta fa referència [als articles 13, 27.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i la comunicació d'informació a les persones usuàries i l'avaluació de l'impacte sobre els drets fonamentals dels sistemes d'alt risc i als codis de conducta d'aplicació voluntària en matèria d'accessibilitat de persones amb discapacitat.

Per l'altra banda, la pregunta es fonamenta en [els articles 7, 8 i 18 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la dignitat humana i autonomia individual, la transparència i supervisió dels sistemes d'IA i els drets de les persones amb discapacitat i dels infants.

Finalment, la pregunta també està relacionada amb l'apartat de [Fairness and non-discrimination de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#), així com l'apartat [Policy Area 8: Education and research](#), del mateix document. de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO.

Exemple: L'organització benèfica *Scope*, ubicada a Gal·les, que treballa en l'àmbit de la igualtat i les discapacitats, compta amb una pàgina web que permet a les persones usuàries adaptar-ne l'accessibilitat ajustant la dimensió del text, el color, l'estil, la font i també el llenguatge emprat.

Aquest exemple està documentat a: [Website accessibility statement i 7 Grandiosos Ejemplos de Accesibilidad Web Para Inspirarte](#).

6.1.6*



El vostre sistema d'IA evita l'ús de tècniques manipulatives o subliminals que podrien perjudicar l'autonomia, la presa de decisions o les eleccions lliures d'un individu?

Aquesta pregunta fa referència [als articles 13, 27.1, 50.3, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i comunicació a les persones usuàries i l'avaluació de l'impacte sobre els drets fonamentals dels sistemes d'alt risc, les obligacions de les persones proveïdores de sistemes que poden generar o manipular contingut donant lloc a un *deepfake*, les obligacions de les persones proveïdores de models de propòsit general de risc sistemàtic i els codis de conducta d'aplicació voluntària.

Per l'altra banda, la pregunta es fonamenta en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la dignitat humana i autonomia individual.

Així com, [l'apartat de Fairness and non-discrimination and Policy Area 8: Education and research](#) de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO.

Exemple: *BlenderBot3* és un *chatbot* desenvolupat per Meta amb una memòria a llarg termini, la capacitat de cercar informació disponible a internet i programat per donar el que ha de ser percebut per les persones usuàries com a mostres d'empatia.

Aquest tipus de disseny pot portar a que les usuàries finals del sistema l'acabin percebut com a una persona real, arribant a confiar massa en els seus resultats.

Aquest exemple està documentat a: [Polémica con el chatbot de Meta: esta IA llama "manipulador" y "mala persona" a Zuckerberg](#) i [Facebook's new AI is already promoting antisemitism and hate speech](#).

6.1.7



El vostre sistema d'IA pot adaptar el seu nivell d'autonomia en funció de les preferències i requisits específics de la persona usuària?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre els codis de conducta d'aplicació voluntària.


També es basa en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la dignitat humana i autonomia individual, així com en el dret fonamental a la llibertat previst a [l'article 5 del Conveni europeu de drets humans](#), [l'article 3 de la Declaració universal dels drets humans](#), [l'article 6 de la Carta de drets fonamentals de la UE](#) i [l'article 9 del Pacte internacional de drets civils i polítics](#).

Exemple: La tècnica del disseny centrat en l'usuari es centra en les necessitats i preferències de les persones que utilitzen el sistema, de manera que aquestes queden més satisfetes del seu ús.

Aquest exemple està documentat a: [The dark side of artificial intelligence: manipulation of human behaviour](#) i [La IA y el diseño de interfaces de usuario](#).

6.2. Percepció del sistema

Nº	Preguntes
----	-----------

6.2.1* 	<p>Heu avaluat si el vostre sistema d'IA encoratja a les persones usuàries a desenvolupar una inclinació, simpatia o empatia que pugui portar a aquestes a sobreestimar les capacitats del mateix sistema?</p>
---	---


Aquesta pregunta fa referència [als articles 14.4, 27.1 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a les mesures de vigilància humana de sistemes d'IA.

Així mateix, la pregunta es fonamenta en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la dignitat humana i autonomia individual, així com en el dret a la llibertat, consagrat a [l'article 5 del Conveni europeu de drets humans, article 3 de la Declaració universal dels drets humans, l'article 6 de la Carta de drets fonamentals de la UE i l'article 9 del Pacte internacional de drets civils i polítics](#).

Així com, les recomanacions contingudes al [subapartat Human Agency and Autonomy d'ALTAI](#).

Exemple: En molts casos s'utilitzen imatges antropomòrfiques per a representar sistemes d'IA, com és el cas d'*Emmi*, l'assistent virtual que utilitza l'empresa Mediamarkt a la seva pàgina web. Aquesta practica pot generar en les persones usuàries una sensació de simpatia que comporta el risc de que sobreestimïn llurs capacitats.

Aquest exemple està documentat a: [Human-Like A.I. Is Deceptive and Dangerous i Mediamarkt Logo](#).

6.2.2* 	<p>Heu establert mesures per tal que, en cap cas, les operacions del vostre sistema d'IA puguin veure's com a opaques, enganyoses o manipuladores per a les persones usuàries?</p>
---	---

Aquesta pregunta fa referència [als articles 13, 27.2, 50, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre la transparència i comunicació d'informació a les persones usuàries i l'avaluació de l'impacte sobre els drets fonamentals dels sistemes d'alt risc, les obligacions de les persones proveïdores de sistemes d'IA generativa, categorització biomètrica, reconeixement d'emocions i propòsit general, així com altres sistemes que interactuïn amb persones, i els codis de conducta d'aplicació voluntària.

Així mateix, la pregunta es fonamenta en [els articles 7 i 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la dignitat humana i autonomia individual, i la transparència i supervisió dels sistemes d'IA, així com en el dret a la llibertat, consagrat a [l'article 5 del Conveni europeu de drets humans, article 3 de la Declaració universal dels drets humans, l'article 6 de la Carta de drets fonamentals de la UE i l'article 9 del Pacte internacional de drets civils i polítics](#).

Finalment, les recomanacions contingudes al [subapartat Human Agency and Autonomy d'ALTAI](#).

Exemple: Podeu dissenyar el vostre sistema per tal que en generar un resultat proporcioni també una explicació clara i comprensible sobre com ha arribat a aquest.

6.2.3

El vostre sistema d'IA manté un nivell de supervisió humana per gestionar la seva autonomia i adaptabilitat, garantint un funcionament segur i controlat després del desplegament?

Aquesta pregunta es fonamenta a [l'article 14 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la supervisió humana dels sistemes d'alt risc.

Per l'altra banda, la pregunta es basa en [l'article 8 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la transparència i supervisió dels sistemes d'IA.

Exemple: Una cadena hotelera vol instal·lar en les seves habitacions un sistema d'intel·ligència artificial que funciona com a assistent virtual. Els equips dels hotels on s'instal·li haurien de tenir i mantenir accés a un registre dels processos de decisió del sistema d'IA i ser capaços de verificar les decisions preses i corregir-les, si escau. Aquest exemple està documentat a: [Everyday Ethics for AI](#).

6.2.4

El vostre sistema d'IA té mecanismes per garantir que el seu grau d'autonomia està limitat per evitar comportaments no desitjats o d'alt risc?

Aquesta pregunta es basa a [l'article 14.3 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la vigilància humana dels sistemes d'alt risc.

Per l'altra banda, la pregunta es fonamenta en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la dignitat humana i autonomia individual.

Exemple: En el cas que el vostre sistema sigui un *chatbot* podeu limitar la seva actuació de manera que es negui a respondre a consultes relacionades amb la salut, que es tracta d'un àmbit categoritzat per la **AI Act** com d'alt risc, aconsellant a les usuàries, així mateix, que consultin a una persona professional.

6.2.5

Disposeu de mecanismes per garantir que l'autonomia del vostre sistema d'IA es mantingui en línia amb els objectius previstos i els requisits de seguretat?

Aquesta pregunta es fonamenta en [els articles 9.6 i 14.3 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre el sistema de gestió de riscos i la vigilància humana dels sistemes d'alt risc.

Per l'altra banda, la pregunta es basa en [l'article 7 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#) que versa sobre la dignitat humana i autonomia individual

Exemple: L'empresa *Fiddler AI* ha establert una associació estratègica amb Amazon que li permetrà vendre les seves tecnologies de monitoratge i explicabilitat de la IA als clients de *Amazon Web Services*, el servei de núvol d'Amazon. Aquest exemple està documentat a [toolify.ai](#).

6.2.6*



Heu avaluat i mitigat els riscos relacionats amb les capacitats i el grau d'autonomia del vostre sistema d'IA?

Aquesta pregunta es basa en [els articles 9 i 55.1 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre el sistema de gestió de riscos dels sistemes d'alt risc i les obligacions de les persones proveïdores de models de propòsit general.

Per l'altra banda, la pregunta es fonamenta en [els articles 7 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la dignitat humana i autonomia individual i el marc de gestió de riscos i impactes.

Exemple: Compteu amb una avaluació dels riscos del vostre sistema relatiu a llur autonomia i capacitat de manera periòdica.

6.2.7



El vostre model d'IA se sotmet a avaluacions de referència, especialment avaluant factors com la seva adaptabilitat a noves tasques i autonomia?

La pregunta es basa en [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la promoció de codis de conducta d'aplicació voluntària.

Exemple: Compteu amb una avaluació d'adaptació i autonomia del vostre sistema relatiu a tasques o situacions futures.

6.2.8



El vostre sistema d'IA, ja sigui autònom o com a part d'un producte, pot adaptar-se i aprendre del seu entorn sense comprometre la seguretat i els estàndards ètics?

Aquesta pregunta fa referència a [l'article 15.4 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versa sobre la resiliència i ciberseguretat dels sistemes d'alt risc.

Per l'altra banda, la pregunta es fonamenta en [l'article 12 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre la fiabilitat dels sistemes d'IA.

Així mateix, destaquem [el títol III sobre principis i valors de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#) que agrupa en quatre blocs aquells valors que haurien de ser respectats en el cicle de la vida del sistema d'IA i els prenem com a guia per a complir aquests estàndards ètics.

Exemple: El filtre *antispam* de *one.com* té la capacitat d'aprendre noves paraules clau i frases utilitzades en els correus brossa i aquells que poden contenir virus informàtics.

Aquest exemple està documentat a: one.com

7.2.7. Principi 7: Sostenibilitat

La sostenibilitat té dues perspectives: la socioeconòmica i la mediambiental. Pel que fa a la primera, el desenvolupament d'una IA sostenible implica establir models que permetin la comunicació i el control entre els sistemes d'IA, els desenvolupadors i la societat. Això és fonamental perquè és la societat que experimenta amb més intensitat les conseqüències, tant positives com negatives, de l'aplicació de la IA. Per aquest motiu, és evident la necessitat de sistemes de compensació i de certificació que garanteixin que els sistemes d'IA operin de manera segura i justa.

Des d'una perspectiva socioeconòmica, el desenvolupament sostenible de la IA destaca pel seu impacte sobre l'ocupació i les desigualtats socioeconòmiques. Si bé un dels majors temors és la pèrdua de llocs de treball a causa de l'automatització, també es preveu la creació de noves oportunitats laborals. No obstant això, aquest benefici potencial només serà possible amb una transició planificada que inclou la formació i la capacitat de persones amb les habilitats necessàries per treballar amb sistemes d'IA així com el reconeixement dels drets d'autoria i la seva conseqüent compensació. Si no s'aborden aquests temes de forma adequada, es podrien incrementar la vulnerabilitat econòmica de certs grups, especialment els creadors de contingut professional, limitant els seus ingressos i el seu accés al mercat laboral. Per tant, l'impacte econòmic de la implementació i ús de la IA ha de considerar aquests aspectes clau per assegurar un desenvolupament econòmic sostenible. La regulació, en aquest cas, és fonamental per establir polítiques que fomentin una transició justa cap a un futur laboral on la IA no esdevé un generador de desigualtats.

Des d'una perspectiva mediambiental, hi ha una creixent preocupació que les organitzacions utilitzin la IA de manera poc conscient des d'un punt de vista ambiental i incrementant la seva petjada ecològica. Així doncs, quan es detecten danys ecològics causats per l'ús i abús de la IA, les organitzacions han de prendre mesures immediates per aturar-los i explorar maneres d'utilitzar aquesta tecnologia sense afectar negativament el medi ambient. Així doncs, l'ús de la IA ha de ser respectuós amb l'eficiència energètica i contribuir a mitigar les emissions de gasos d'efecte hivernacle, assegurant que la seva petjada ecològica sigui mínima.

Les regulacions han de jugar un paper crucial en l'establiment d'estàndards per garantir que els sistemes d'IA no només redueixen les emissions, sinó que promoguin l'eficiència en l'ús de recursos, especialment aquells materials. Això inclou el disseny de sistemes d'IA que maximitzin l'eficiència energètica i minimitzin el desaprofitament, assegurant un ús sostenible de la tecnologia a llarg termini. Per aquest motiu, és fonamental que les organitzacions assumeixin la responsabilitat de garantir que l'ús de la IA sigui coherent amb els objectius de sostenibilitat mediambiental.

Per tant, aquest principi planteja que els sistemes d'IA haurien de beneficiar les persones, la societat i el medi ambient. Les preguntes d'aquest apartat provenen majoritàriament de les seccions relatives a l'impacte de la IA sobre els drets i el benestar ambiental dels diferents instruments i recomanacions consultades, i troben la seva referència normativa a l'article 27, 53, 55 i 95 de la **AI Act** relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat.

El principi de sostenibilitat està relacionat amb l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret, relatiu al marc de gestió de riscos i impactes. Aquest article imposa la obligació d'adoptar mesures per tal d'identificar, avaluar, preveure i mitigar els riscos que els sistemes d'IA plantegen sobre els drets humans, la democràcia i l'estat de dret. L'informe explicatiu afegeix que els marcs de gestió de riscos i impactes també hauran de valorar els riscos i impactes mediambientals sorgits dels sistemes d'IA, ençà que la preservació d'un medi ambient saludable està intrínsecament relacionada amb el gaudi dels drets humans⁸⁵.

Així mateix, a més de considerar els riscos potencials, també s'haurien de valorar els possibles beneficis i impactes positius que els sistemes avaluats poden comportar per a la societat en conjunt⁸⁶.

A més, el principi de sostenibilitat està relacionat amb l'article 13 del Conveni marc, que versa sobre la innovació segura, i anima als estats membres a establir ambients segurs i supervisats que permetin testejar els sistemes artificials abans de ser col·locats al mercat, per tal d'identificar i avaluar si el seu ús és respectuós per als drets humans, la democràcia i l'estat de dret.

Si bé els sistemes d'IA poden arribar a suposar un risc per als drets de les persones, en determinats casos el seu ús pot potenciar l'exercici d'aquests, sempre que es faci de manera ètica i responsable. Per exemple, l'Agència de Drets Fonamentals de la UE considera que, mentre que existeix la possibilitat que les decisions preses per una IA siguin discriminatòries per a algunes persones, la IA pot ser potencialment utilitzada per testejar i detectar comportaments discriminatoris per tal d'evitar-los⁸⁷.

Per aquest motiu, resulta important dissenyar i usar els sistemes d'IA prenent en consideració que aquests hagin de ser posats al servei de les persones. Amb aquesta finalitat, seria oportú comptar amb la participació dels grups sobre els quals es preveu utilitzar la IA en totes les fases del seu disseny i ús, ja que aquests són els millor posicionats per identificar les seves necessitats i de quina manera la IA podria afectar-les⁸⁸.

D'altra banda, el principi de sostenibilitat requereix avaluar l'impacte del sistema d'IA sobre el medi ambient. El 2021 el Consell de Drets Humans de les Nacions Unides va declarar que l'accés a un medi ambient saludable i sostenible és un dret universal a la seva Resolució 48/13 de 8

⁸⁵ Consell d'Europa (2024) Informe explicatiu sobre la Convenció Marc del Consell d'Europa sobre Intel·ligència Artificial i Drets Humans, Democràcia i Estat de Dret. Disponible a: <https://rm.coe.int/1680afae67> (consultada el 20 de juliol de 2024).

⁸⁶ *Idem*.

⁸⁷ FRA (2021) Fer que el futur sigui correcte. Intel·ligència Artificial i drets fonamentals. Disponible a: <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights> (consultada el 21 de novembre de 2023).

⁸⁸ ACNUDH (2018) Un enfocament basat en els drets humans sobre les dades: no deixar ningú enrere en l'Agenda 2030 per al Desenvolupament Sostenible. Disponible a: <https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf> (consultada el 20 de novembre de 2023).

d'octubre de 2021⁸⁹. A partir de la resolució del Consell de Dret Humans, altres organismes internacionals s'han pronunciat a favor del reconeixement d'aquest dret, com ara el Consell d'Europa⁹⁰ o la Unió Europea⁹¹, la qual, si bé ja mencionava la protecció al medi ambient a la seva Carta de Drets Fonamentals, no la definia com a un dret en si mateixa. Per la seva banda, l'Assemblea General de les Nacions Unides ha manifestat que la degradació del medi ambient i el canvi climàtic suposen una de les amenaces més greus i apressants als que s'enfronta la humanitat⁹².

Per aquest motiu, l'ús ètic de la IA requereix que els sistemes siguin respectuosos amb el medi ambient. A tal fi, la **AI Act** demana a la Comissió que sol·liciti a les organitzacions europees l'estandardització de processos d'informació i documentació per a millorar el rendiment dels sistemes d'IA, com per exemple desenvolupant sistemes energèticament eficients durant tot el seu cicle de vida⁹³.

Un dels reptes socials que afronten les IA és el debat entorn de la propietat intel·lectual, i especialment les generatives. La propietat intel·lectual és tracta d'un element del dret a la propietat privada, que es tracta d'un dret humà protegit pel Dret Internacional, com per exemple els articles 1 i el 14 de la Conveni europeu de drets humans. De fet, la propietat intel·lectual està reconeguda com un dret fonamental en si mateixa a l'article 17 de la Carta de drets fonamentals de la UE i del qual també destaquem els articles 21 i 31 al 34.

Respecte a la normativa internacional, és rellevant per aquest principi els articles 1 a 30 de la Carta social europea; els articles 7, 22 a 25 de la Declaració universal dels drets humans; l'article 26 del Pacte internacional de drets civils i polítics; i finalment, els articles 6 a 8 i 11 del Pacte internacional de drets econòmics, socials i culturals.

Com s'ha explicat prèviament, les IA en la fase de desenvolupament utilitzen dades per entrenar-se. Per exemple, els sistemes d'intel·ligència artificial que produeixen imatges com DALL-E o *Midjourney*, han requerit d'un gran nombre d'imatges per "aprendre" a crear-ne una de manera autònoma.

⁸⁹ Consell de Drets Humans de les Nacions Unides (2021) Resolució A/HRC/48/L.23/Rev.1: El dret humà a un medi ambient sense riscos, net, saludable i sostenible. Disponible a: <https://press.un.org/en/2022/ga12437.doc.htm> (consultada el 7 de desembre de 2023).

⁹⁰ Consell d'Europa (2022) El Comitè de Ministres fa una crida als estats membres perquè reconeguin el dret a un medi ambient net, saludable i sostenible com un dret humà. Disponible a: <https://www.coe.int/en/web/portal/-/committee-of-ministers-calls-on-member-states-to-recognise-the-right-to-a-clean-healthy-and-sustainable-environment-as-a-human-right> (consultada el 4 de desembre de 2023).

⁹¹ Parlament Europeu (2021) Un dret universal a un medi ambient saludable. Disponible a: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698846/EPRS_ATA\(2021\)698846_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698846/EPRS_ATA(2021)698846_EN.pdf) (consultada el 4 de desembre de 2023).

⁹² Assemblea General de les Nacions Unides (2022) Resolució A/76/L.75: El dret humà a un medi ambient net, saludable i sostenible. Disponible a: <https://digitallibrary.un.org/record/3983329?v=pdf> (consultada el 7 de desembre de 2023).

⁹³ Comissió Europea (2023) Artificial Intelligence – Preguntes i respostes. Disponible a: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683 (consultada el 14 de desembre de 2023).

A causa d'aquestes mecàniques, sorgeixen dubtes en relació amb les IA generatives i la propietat intel·lectual que podem englobar en dues qüestions: 1) si el contingut generat per la IA, és susceptible de ser protegit per les lleis de copyright i, en cas que així sigui, qui en seria el beneficiari; 2) i si els productes generats per un sistema d'IA poden infringir els drets d'autor en relació amb les dades protegides per copyright utilitzades per el seu entrenament.

En relació amb la primera qüestió, l'Organització Mundial del Comerç (OMPI) defineix aquest concepte com "*les creacions de la ment, com les invencions, les obres literàries i artístiques, i els símbols, noms i imatges utilitzats en el comerç*".⁹⁴ De manera similar, la Cort de Justícia de la UE ha considerat que poden gaudir de la protecció dels drets d'autor aquelles obres llur contingut determina elements que expressin la creació intel·lectual de l'autor.⁹⁵ En ambdós casos, sembla que, a priori, l'existència de drets d'autor sobre una producció requereix l'autoria humana.⁹⁶ En conseqüència, com a mínim de moment, els instruments normatius que contempnen la regulació relativa a la propietat intel·lectual no inclouen en la seva protecció les creacions no generades per una persona humana.⁹⁷

Tot i això, no es tracta d'un debat tancat. Hi ha qui argumenta, per exemple, que la IA emprada per crear una obra pot ser considerada com una eina utilitzada per a la persona que introdueix les instruccions. Ja que són el reflex de la creativitat de l'autor i podrien donar lloc a què el producte fos protegit per les lleis de copyright, de manera similar a un fotògraf que pren les decisions necessàries per dotar de caràcter artístic a les imatges que pren amb la càmera.⁹⁸

En relació amb la segona de les qüestions, com jo avançàvem, es planteja el dubte de si els productes de les IA generatives per a l'entrenament de les quals s'han utilitzat dades relatives a obres protegides pels drets d'autor, poden suposar la infracció de la legislació de propietat intel·lectual. En aquest sentit, el Servei de Recerca del Congrés d'Estats Units identifica dos potencials supòsits d'infracció de drets d'autor: mitjançant la creació de còpies de les dades utilitzades en el procés d'entrenament o generant productes que s'assemblen a obres existents.⁹⁹

En primer lloc, el procés d'entrenament suposa crear còpies de les dades utilitzades. Dins el marc comunitari, la Directiva 2001/29/CE del Parlament Europeu i del Consell, de 22 de maig de 2001, relativa a l'harmonització de determinats aspectes dels drets d'autor i drets afins en la societat de

⁹⁴ Organització Mundial de la Propietat Intel·lectual (s/d) Què és la propietat intel·lectual?. Disponible a: <https://www.wipo.int/about-ip/es/> (consultada el 17 de gener de 2024).

⁹⁵ Sentència del Tribunal de Justícia de la Unió Europea (Sala Quarta), assumpte C-5/08, de 16 de juliol de 2009. Disponible a: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A62008CJ0005> (consultada el 18 de gener de 2024).

⁹⁶ Guadamuz, A. (2017) Intel·ligència Artificial i *copyright*. Disponible a: https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html (consultada el 14 de gener de 2024).

⁹⁷ Hugenholtz, P. B. Quintais, J.P. (2021) Copyright i creacions artificials: Protegeix la legislació de drets d'autor de la UE les obres assistides per IA?. Disponible a: <https://link.springer.com/article/10.1007/s40319-021-01115-0> (consultada el 23 de gener de 2024).

⁹⁸ Congressional Research Service (2023) Intel·ligència Artificial Generativa i la llei de *Copyright*. Disponible a: <https://crsreports.congress.gov/product/pdf/LSB/LSB10922> (consultada el 17 de gener de 2024). En relació amb el cas *Midjourney vs Kristina Kashtanova* de la Oficina de *Copyright* d'Estats Units.

⁹⁹ *Ibidem*.

la informació¹⁰⁰, prohibeix els actes de reproducció, ja sigui directa o indirecta, i d'una part o la totalitat d'una obra sense autorització de l'autor. No obstant, la Directiva 2019/790 del Parlament Europeu i del Consell, de 17 d'abril de 2019, sobre els drets d'autor i drets afins en el mercat únic digital¹⁰¹, que ha entrat en vigor recentment, incorpora en el seu article quart una excepció a aquesta norma, per la qual no resultarien il·lícites les reproduccions i extraccions d'obres accessibles de manera legítima per a fins de mineria de textos i dades. En conseqüència, aquesta primera possibilitat no seria considerada una vulneració dels drets d'autor a la vista de l'ordenament jurídic comunitari¹⁰².

Pel que fa a la segona possibilitat, encara no existeix una resposta legal clara. Hem de tenir en compte que la reproducció d'elements originals d'una obra seguida per l'aportació pròpia de components d'originalitat suposa la creació del que s'anomena una obra derivada. A la Unió Europea, el dret a crear obres derivades forma part del conjunt de drets d'autor dels que es posseïdor la persona que ha creat l'obra en qüestió¹⁰³, per la qual cosa és una facultat exclusiva que ostenta la persona autora de l'obra i aquelles persones a les que ha autoritzat a tal fi¹⁰⁴.

No obstant, aquest dret pot contemplar excepcions. En aquest sentit, s'ha determinat que les parodies, obres que parteixen d'una idea ja existent, són respectuoses amb els drets d'autor sempre que es compleixin amb uns requisits¹⁰⁵. Sobre aquesta temàtica, els tribunals han dictaminat que es possible generar obres inspirades o similars a d'altres, sempre que no es puguin confondre entre si, i que no hi hagi risc de que el contingut no original pugui ser confós amb les obres original de la persona autora¹⁰⁶.

De manera similar, el Tribunal de Justícia de la UE ha explicat en el cas *Pelham*¹⁰⁷ que el dret a la propietat intel·lectual no és absolut, sinó que la seva protecció ha de ponderar-se en relació amb

¹⁰⁰ Directiva 2001/29/CE del Parlament Europeu i del Consell, de 22 de maig de 2001, relativa a l'harmonització de determinats aspectes dels drets d'autor i drets afins als drets d'autor en la societat de la informació. Disponible a: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2001-81549> (consultada el 17 de gener de 2024).

¹⁰¹ Directiva (UE) 2019/790 del Parlament Europeu i del Consell, de 17 de abril de 2019, sobre els drets d'autor i drets afins en el mercat únic digital i per la que es modifiquen les Directives 96/9/CE i 2001/29/CE. Disponible a: <https://www.boe.es/doue/2019/130/L00092-00125.pdf> (consultada el 17 de gener de 2024).

¹⁰² De Champris, B. (2023) *AI Act amenaçat per demandes de drets d'autor sense sentit*. Disponible a: <https://www.project-disco.org/european-union/ai-act-under-threat-from-pointless-copyright-demands/> (consultada el 25 de gener de 2024).

¹⁰³ Saluveer, A.L. (2014) *El concepte d'obres derivades en la legislació de drets d'autor europea en relació amb l'era digital: Llicències de programari lliure i de codi obert*. Disponible a: <https://lup.lub.lu.se/luur/download?func=downloadFile&recordId=4461961&fileId=4461970> (consultada el 25 de gener de 2024).

¹⁰⁴ Brey Rodríguez-Tembleque, M. (2023) *El Dret de transformació. Límits i obra derivada*. Disponible a: <https://app.vlex.com/#search/jurisdiction:ES/El+Derecho+de+transformaci%C3%B3n.+L%C3%ADmites+y+obra+derivada/vid/derecho-transformacion-limites-obra-972357282> (consultada el 25 de gener de 2024).

¹⁰⁵ Sentència de l'Audiència Provincial de Barcelona de 10 de Octubre de 2003.

¹⁰⁶ Tribunal de Justícia de la Unió Europea, Gran Sala, Cas C-201/13, *Johan Deckmyn i Vrijheidsfonds VZW v Helena Vandersteen i Altres*, de 3 de setembre de 2014. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62013CJ0201> (consultada el 25 de gener de 2024).

els altres drets fonamentals, incloent la llibertat de les arts, reconeguda a l'article 13 de la Carta de drets fonamentals de la UE. No obstant, la mateixa sentència indica quan s'hagi de reconèixer els elements de l'obra original inclosos en l'obra derivada, es tractarà d'un acte de reproducció en el sentit de l'article 2 de la Directiva 2001/29. Per tant, suposarà una infracció de la normativa en matèria de drets d'autor que no pot ser excusada per l'exercici de la llibertat de les arts.¹⁰⁸

Un altre possible excepció a les infraccions de copyright és el cas de les creacions independents doble, és a dir, una intel·ligència artificial crea de manera independent una obra que sigui idèntica totalment o parcialment a una obra ja existent. Per tal que un incident d'aquestes característiques no sigui considerat com a vulneració dels drets d'autor, recau sobre la persona propietària de l'obra més recent l'obligació de provar aquesta circumstància.¹⁰⁹

Com es pot observar, encara hi ha un gran nombre de qüestions obertes en relació amb les possibles vulneracions dels drets d'autor per l'ús de les IA generatives. Tot i que la **AI Act** ha volgut introduir algunes previsions sobre aquesta matèria, aquesta resulta insuficient per fer front a tots els possibles escenaris i les especialitats que a IA generativa suposa en relació amb la normativa vigent.

Per aquest motiu, i a falta d'una regulació més específica, s'haurà de contemplar cas per cas en quins supòsits les obres generades per una IA podran ser considerades vulneracions dels drets d'autor, quins subjectes són considerats responsables de tals infraccions, i fins i tot si els productes de les IA generatives seran susceptibles de ser protegits per la legislació en matèria de propietat intel·lectual. A tals efectes, caldrà esperar que aquests casos comencin a arribar als nostres tribunals per tal que el poder judicial desenvolupi jurisprudència en la matèria. En aquest sentit, als Estats Units ja han començat a sorgir els primers casos judicials sobre la qüestió, com per exemple la demanda interposada per les artistes Sarah Anderson, Kelly McKernan, i Karla Ortiz contra Stability AI, Midjourney i DeviantArt.¹¹⁰

¹⁰⁷ Tribunal de Justícia de la Unió Europea, Gran Sala, Cas C-476/17, Pelham GmbH, Moses Pelham i Martin Haas v. Ralf Hütter i Florian Schneider-Esleben, de 29 de juliol de 2019. Disponible a: <https://curia.europa.eu/juris/liste.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-476%252F17&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lqrec=en&lq=&page=1&cid=1983391> (consultada el 25 de gener de 2024).

¹⁰⁸ *Idem*.

¹⁰⁹ Nordemann J.B. (2024) Dret de la UE: IA generativa, infraccions de drets d'autor i responsabilitat – La meua aposta per un tema candent el 2024. Disponible a: <https://copyrightblog.kluweriplaw.com/2024/01/23/eu-law-generative-ai-copyright-infringements-and-liability-my-guess-for-a-hot-topic-in-2024/> (consultada el 25 de gener de 2024).

¹¹⁰ Francen, C. (2023) Midjourney, Stability AI i DeviantArt aconsegueixen una victòria en el cas de drets d'autor presentat per artistes, però la lluita continua. Disponible a: <https://venturebeat.com/ai/midjourney-stability-ai-and-deviantart-win-a-victory-in-copyright-case-by-artists-but-the-fight-continues/> (consultada el 29 de gener de 2023).

7.1. Desenvolupament sostenible

Nº

Preguntes

7.1.1*



Considerem que el vostre sistema d'IA té un impacte positiu en els drets laborals i/o en la qualitat del treball de les persones?

Aquesta pregunta fa referència [als articles 27.1, 55.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre l'avaluació de l'impacte dels sistemes d'alt risc sobre els drets fonamentals, les obligacions de les persones proveïdores dels sistemes de propòsit general de risc sistèmic, i la promoció de codis de conducta d'aplicació voluntària en matèria sostenibilitat.

Així mateix, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, així com els drets humans relatius al treball, incloent-hi el dret humà a les condicions de treball justes i equitatives, consagrats als [articles 22 a 24 de la Declaració universal dels drets humans](#), [els articles 31 a 34 de la Carta de drets fonamentals de la UE](#), [els articles 6, 7 i 8 de la del Pacte internacional de drets econòmics, socials i culturals](#) i [els articles 1 i ss de la Carta social europea](#).

Finalment, la pregunta es fonamenta en les demandes de [ECNL, Liberties i ECF a la Carta d'AI Act Must Protect the Rule of Law](#), així com el [punt 50 de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#), relatiu a l'avaluació ètica de l'impacte dels sistemes d'IA en relació amb els drets.

Exemple: S'han reportat casos en els que l'algoritme utilitzat per Amazon per monitorar a les persones encarregades de les entregues dels productes de companyia han acomiadat a alguna persona afirmant que el seu rendiment era baix sense tenir en consideració els obstacles del món real que la persona treballadora pot trobar-se per realitzar la feina. No obstant, a aquestes decisions es realitzen sense la intervenció ni la revisió d'una persona humana.

Aquest exemple està documentat en el següent enllaç: [Fired by Bot: Amazon Turns to Machine Managers And Workers Are Losing Out - Bloomberg](#).

7.1.2



Considerem que el vostre sistema d'IA millora la qualitat de vida de les persones usuàries a nivell individual i vetlla pel desenvolupament sostenible a nivell col·lectiu?

Aquesta pregunta fa referència [als articles 27 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre l'avaluació d'impacte dels sistemes d'alt risc sobre els drets fonamentals i el codis de conducta d'aplicació voluntària en matèria sostenibilitat.

Així mateix, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, juntament amb el dret a un nivell de vida adequat, reconegut a [l'article 25 de la Declaració universal dels drets humans](#) i [l'article 11 del Pacte internacional de drets econòmics, socials i culturals](#); el dret a la protecció contra la pobresa i l'exclusió social, consagrat a [l'article 30 de la Carta](#)

[social europea](#); i el dret a un medi ambient saludable declarat a la [Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

La pregunta també es relaciona amb [el punt 14 de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#), relatiu a la millora de la qualitat de vida per part dels sistemes d'IA.

Exemple: Dins del [projecte IKI](#) de Nacions Unides s'utilitza tecnologia d'IA per ajudar a preveure patrons meteorològics, de manera que les comunitats i les autoritats puguin planificar millor com adaptar-se i mitigar els efectes del canvi climàtic.

7.1.3



Heu tingut en compte l'accés social, incloent-hi la bretxa digital, en l'ús i implantació del vostre sistema d'IA?

Aquesta pregunta fa referència [als articles 27.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria d'accessibilitat.

Així mateix, la pregunta es fonamenta en [els articles 10 i 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versen sobre la igualtat i la no discriminació i el marc de gestió de riscos i impactes. Juntament amb el dret humà a la igualtat i la no discriminació, consagrat a [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#), [l'article 7 de la Declaració universal dels drets humans](#), i [l'article 14 del Conveni europea de drets humans](#).

Finalment, la pregunta està relacionada amb les recomanacions en matèria contractual contingudes a [The Ethics of AI Business Practices: A Review of 47 AI Ethics Guidelines, d'Attard-Frost et al.](#)

Exemple: Un estudi ha reportat que, mentre que un 53% d'estudiants britànics ja estan utilitzen eines d'IA com suport per als seus estudis, altres alumnes no tenen accés a les mateixes tecnologies, generant-se una bretxa digital. Per aquest motiu, l'informe resultant recomana a les institucions educatives que comencin a educar als alumnes sobre com fer servir la IA de manera correcta i proveir d'aquestes tecnologies a les persones que per si mateixes no hi poden accedir, per tal de reduir desigualtats entre l'alumnat.

Aquest exemple està documentat a: [Most students use AI for studies, digital divide emerges – Survey](#)

7.1.4



Heu abordat els punts cecs de l'anàlisi mitjançant la participació amb les parts interessades rellevants, per exemple comprovant les hipòtesis i discutint les implicacions del vostre sistema d'IA amb les comunitats afectades?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de *stakeholder participation*.

Així mateix, la pregunta està relacionada amb [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, així com el dret a la igualtat i la no discriminació, consagrat a [l'article 21 de la Carta de drets fonamentals de la UE](#), [l'article 26 del Pacte internacional de drets civils i polítics](#), [l'article 7 de la](#)

[Declaració universal dels drets humans](#) i [l'article 14 del Conveni europeu de drets humans](#).

Finalment destaquem els [apartats de *Fairness and non-discrimination i Multi-stakeholder and adaptive governance and collaboration* de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#) i l'apartat [Injustice in Algorithmic Systems de l'Algorithmic Equity Toolkit d'ACLU](#), així com en el principi [Participation del document A Human Rights-Based Approach To Data de l'ACNUDH](#).

Exemple: L'oficina regional de la Lliga Àrab de l'Organització Internacional del Treball està desenvolupant una plataforma propulsada amb IA que pugui ser utilitzada per ocupadors, persones en recerca de feina i formadors. El disseny del concepte es va dur a terme en estreta col·laboració amb tots els interessats rellevants, incloent la Camara de la Industria de Jordània, Consells d'habilitats del sector químic i de la confecció, així com diverses persones proveïdores de formació. Per a més informació sobre el projecte podeu consultar l'informe [United Nations Activities on Artificial Intelligence \(AI\)](#).

7.1.5



Us assegureu que existeixi una compensació justa i un tracte ètic a les persones implicades en l'etiquetatge de dades dels vostres sistemes d'IA?

La pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria.

Així mateix, la pregunta està relacionada amb els drets humans relatius al treball, incloent-hi el dret a les condicions de treball justes i equitatives, consagrats als [articles 22 a 24 de la Declaració universal dels drets humans](#), els [articles 31 a 34 de la Carta de drets fonamentals de la UE](#) i els [articles 6, 7 i 8 de la del Pacte internacional de drets econòmics, socials i culturals](#).

També està relacionada amb [el títol IV, actuació 10 sobre economia i treball de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#).

Exemple: Recompensar econòmicament a les persones implicades en l'etiquetatge de dades del vostre sistema i garantir que no seran utilitzades, o només ho seran amb total respecte dels requisits legals aplicables.

7.1.6*



Implementeu mesures per abordar problemes de drets d'autor i drets de propietat intel·lectual quan feu servir conjunts de dades externs en el vostre procés de desenvolupament d'IA?

Aquesta pregunta fa referència [als articles 53.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatius a les obligacions de les persones proveïdores dels models de propòsit general i la promoció de codis de conducta d'aplicació voluntària.

D'altra banda, la pregunta es relaciona amb la [Directiva 2001/29/CE, de 22 de maig del 2001 \[Directiva dels drets d'autor i drets afins en la societat de la informació i la Directiva 2019/790 del Parlament Europeu i del Consell, de 17 d'abril de 2019, sobre els drets d'autor i drets afins en el mercat únic digital\]](#).

A més, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes. Juntament amb el dret a la propietat intel·lectual, reconegut en [l'article 17.2 de la Carta de drets fonamentals de la UE](#), [l'article 1 del Protocol del Conveni europeu de drets humans per a la protecció dels drets humans i les llibertats fonamentals](#), i [l'article 17 de la Declaració universal dels drets humans](#).

Exemple: L'agència de fotografia i banc d'imatges nord americana *Getty Images* denuncia al sistema d'IA *Stable Diffusion* per l'escaneig il·legal de milions d'imatges del seu lloc web. Aquest exemple està documentat a:

[Getty Images is suing the creators of AI art tool Stable Diffusion for scraping its content](#) i [Adn](#).

7.1.7



Col·laboreu activament amb organitzacions laborals o sindicats per mitigar el possible desplaçament laboral causat per l'adopció de tecnologies d'IA a través de la requalificació de les persones treballadores afectades?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria sostenibilitat.

Així mateix, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, així com els drets humans relatius al treball, incloent-hi el dret humà a les condicions de treball justes i equitatives, consagrats [als articles 22 a 24 de la Declaració universal dels drets humans](#), [els articles 31 a 34 de la Carta de drets fonamentals de la UE](#), [els articles 6 i 7, de la del Pacte internacional de drets econòmics, socials i culturals](#), i [els articles 5 i 6 de la Carta social europea](#).

Finalment, la pregunta també es relaciona amb [el punt 50, i al títol IV, actuació 10 sobre economia i treball, de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#), sobre l'avaluació de l'impacte dels sistemes d'IA sobre els drets i el bon funcionament dels sistemes d'IA en matèria empresarial i laboral.

Exemple: L'11 de desembre de 2023 Microsoft i la federació sindical més gran dels EEUU, AFL-CIO, van [acordar una col·laboració](#) dins la qual els treballadors i els líders sindicals podran donar comentaris sobre la seva experiència treballant amb IA i les seves preocupacions sobre aquesta tecnologia als desenvolupadors i investigadors d'IA de Microsoft, mitjançant "cimeres laborals" entre el sindicat i Microsoft.

7.2. Impacte mediambiental

Nº Preguntes

7.2.1*

El vostre sistema d'IA és capaç d'enregistrar el seu consum d'energia i impacte ambiental durant tot el seu cicle de vida?

La pregunta fa referència [als articles 53.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre les obligacions de les persones proveïdores dels sistemes de propòsit general i els codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Així mateix, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, així com al dret d'un medi ambient saludable declarat a la [Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

Exemple: Un estudi titulat [Power Hungry Processing: Watts Driving the Cost of AI Deployment?](#) ha determinat que la creació d'una sola imatge mitjançant una IA generativa comporta, de mitja, la mateixa petjada de carboni que carregar al 100% la bateria d'un telèfon mòbil.

Per a més informació sobre aquesta qüestió podeu consultar els següents articles: [Crear una sola imatge amb intel·ligència artificial consumeix tanta energia com carregar un mòbil](#) i [Powering AI could use as much electricity as a small country](#).

7.2.2*

Heu avaluat l'eficiència energètica del vostre sistema d'IA tenint en compte el seu cicle de vida?

Aquesta pregunta fa referència [als articles 53.1 i 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), que versen sobre les obligacions de les persones proveïdores dels sistemes de propòsit general i els codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Així mateix, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, així com en el dret a un medi ambient saludable declarat a la [Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

Per l'altra banda, la pregunta està relacionada amb les recomanacions contingudes a [l'apartat d'Environmental well-being d'ALTAI](#) i amb la [Policy Area 5: Environment and Ecosystems de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#). Finalment, també es basa en l'apartat [Enviromental Wellbeing del AI Ethics Assessment de GSMA](#).

7.2.3

Heu establert mesures per incrementar l'eficiència energètica del vostre sistema d'IA a través de la supervisió que, per naturalesa, és més eficient amb les dades?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Així mateix, la pregunta es fonamenta en el dret a un medi ambient saludable declarat a la [Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

La pregunta també es relaciona amb les recomanacions contingudes a l'[apartat d'Environmental well-being d'ALTAI](#) i amb la [Policy Area 5: Environment and Ecosystems de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#), juntament amb l'[apartat Environmental Wellbeing del AI Ethics Assessment de GSMA](#).

Exemple: Existeixen sistemes d'IA que permeten identificar formes d'optimitzar el consums energètic.

Aquest exemple està documentat a: [Cómo la inteligencia artificial puede contribuir al ahorro energético](#).

7.2.4

Heu establert mesures per incrementar l'eficiència energètica del vostre sistema d'IA a través de la minimització de dades o de l'ús de dades sintètiques?

Aquesta pregunta fa referència a l'[article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Per l'altra banda, la pregunta es fonamenta en el dret a un medi ambient saludable declarat a la [Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

La pregunta també es relacionada amb les recomanacions contingudes a l'[apartat d'Environmental well-being d'ALTAI](#) i amb la [Policy Area 5: Environment and Ecosystems de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#).

Exemple: Existeixen sistemes d'IA que efectuen compressió de dades de vídeos per a reduir la quantitat d'aquestes sense comprometre la qualitat del contingut, com és el cas de *l'start-up Depp Render*.

Aquest exemple està documentat a: [Deep Render Says Its AI Video Compression Tech Will 'Save the Internet'](#) i <https://siliconcanals.com/es/noticias/AI-con-sede-en-Londres-startup-deep-render-secures-funding/>.

7.2.5

Heu establert mesures per incrementar l'eficiència energètica del vostre sistema d'IA transferint coneixement de dades riques a dominis de dades pobres?

Aquesta pregunta fa referència a l'[article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Per l'altra banda, la pregunta es fonamenta en el dret a un medi ambient saludable, declarat a la [Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

La pregunta també es relacionada amb les recomanacions contingudes a l'[apartat d'Environmental well-being d'ALTAI](#) i amb la [Policy Area 5: Environment and Ecosystems de les recomanacions sobre ètica en la Intel·ligència Artificial d'UNESCO](#).

Exemple: Un sistema d'IA on la transferència d'aprenentatge *zero-shot* es transfereix el coneixement d'un domini ric a un domini de dades pobres sense cap ajustament del mateix sistema i, per tant, es du a terme de manera automàtica.

7.2.6

Incorporeu una programació eficient energèticament i pràctiques de disseny sostenible als vostres sistemes d'IA, especialment quan tracteu amb el processament de dades a gran escala?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Així mateix, la pregunta es fonamenta en el dret a un medi ambient saludable, reconegut a [la Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

Per l'altra banda, la pregunta es relaciona amb les directrius de la UNESCO contingudes [al títol IV, actuació 5 sobre medi ambient i ecosistemes de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#) i a [Ethical Impact Assessment: A Tool of the Recommendation on the Ethics of Artificial Intelligence](#), així com l'apartat [Environmental well-being d'ALTAI](#).

Exemple: L'empresa de centre de dades *Switch* ha rebut diversos reconeixements pel seu model de disseny sostenible, arribant a rebre la màxima puntuació d'entre totes les empreses incloses a informe *Clicking Clean* de Greenpeace.

Aquest exemple està documentat a: [Clicking Clean: Who is winning the race to build a green internet?](#)

7.2.7

Heu implementat estratègies per reduir la petjada ambiental dels vostres sistemes d'IA, especialment quan manegeu conjunts de dades extensos?

Aquesta pregunta fa referència a relatiu a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Així mateix, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, i en el dret humà a un medi ambient saludable, reconegut en [la Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

Per l'altra banda les preguntes es relacionen amb [el títol IV, actuació 5 sobre medi ambient i ecosistemes de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#) i l'apartat [Environmental well-being d'ALTAI](#).

Exemple: A l'article [Cloud Storage vs. Hard Disk Drive \(HDD\): Which is Better for Data Security?](#) s'explica com emmagatzemar dades al núvol genera una major petjada mediambiental que si s'utilitza un disc dur.

7.2.8

Heu explorat l'ús de fonts d'energia renovables i pràctiques d'informàtica verda en el desplegament i l'operació dels teus sistemes d'IA per millorar la sostenibilitat?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Així mateix, la pregunta es fonamenta en el dret humà a un medi ambient saludable, reconegut a [la Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

Per l'altra banda, la pregunta està relacionada amb l'[apartat d'Environmental well-being d'ALTAI](#) i [el títol IV, actuació 5 sobre medi ambient i ecosistemes de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#).

Exemple: L'empresa [Autogrid](#) ofereix una plataforma que permet a les companyies elèctriques o els operadors comercials de xarxes optimitzar la gestió d'energia mitjançant algoritmes d'aprenentatge automàtic. D'aquesta manera és possible preveure la demanda i optimitzar les operacions de xarxa, minimitzant emissions i costos.

7.2.9

Col·laboreu amb organitzacions i iniciatives enfocades a promoure pràctiques d'IA sostenibles per reduir l'impacte ambiental de les tecnologies d'IA?

Aquesta pregunta fa referència a [l'article 95 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \(AI Act\)](#), relatiu a la promoció de codis de conducta d'aplicació voluntària en matèria de sostenibilitat ambiental.

Així mateix, la pregunta es fonamenta en [l'article 16 del Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#), que versa sobre el marc de gestió de riscos i impactes, i en el dret humà a un medi ambient saludable, reconegut en [la Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU](#).

Per l'altra banda, la pregunta es relaciona amb les directrius de la UNESCO contingudes [al títol IV, actuació 5 sobre medi ambient i ecosistemes de les recomanacions sobre ètica en la intel·ligència artificial d'UNESCO](#) i a [Ethical Impact Assessment: A Tool of the Recommendation on the Ethics of Artificial Intelligence](#), així com l'[apartat Environmental well-being d'ALTAI](#).

Exemple: La vostra empresa participa en associacions i/o trobades amb altres empreses per a promoure pràctiques d'IA sostenibles.

* Tot i que la categoria de risc limitat compren els sistemes de reconeixement d'emocions, d'identificació biomètrica, d'IA generativa i de models de propòsit general, les obligacions de transparència que es preveuen a la AI Act no són les mateixes per tots aquests sistemes, sinó que presenta règims diferenciats.

Per aquest motiu, recomanem prestar atenció a la justificació jurídica de les preguntes per tal d'assegurar si el vostre sistema de risc limitat es troba subjecte a les obligacions específiques que es reflecteixen en cadascuna de les qüestions.

8. GUIA PER CONTRACTES EN MATÈRIA D'IA:

Un dels grans reptes que planteja la Intel·ligència Artificial és l'atribució de responsabilitats per les conseqüències derivades de la implantació d'aquesta tecnologia. La **AI Act** ja compta amb disposicions en les quals es delimiten quins subjectes són els responsables de complir amb les exigències contemplades per la mateixa llei. En aquest sentit, els articles 24 a 29 de la **AI Act** europea preveuen les diferents obligacions per a les persones fabricants dels productes, les importadores, les distribuïdores, les usuàries i terceres persones.

Així mateix, la proposta de Directiva del Parlament Europeu i del Consell relativa a normes de Responsabilitat Civil Extracontractual a la Intel·ligència Artificial (AI Liability Directive) conté algunes previsions sobre la presumpció de culpa de diferents agents en matèria de responsabilitat extracontractual derivada de la infracció d'una norma de la **AI Act**.

No obstant això, és necessari establir uns criteris que ens permetin atribuir la responsabilitat d'actes que no només infringeixin la **AI Act** sinó que suposin una lesió de qualsevol disposició de l'ordenament jurídic, afavorint el rendiment de comptes i la seguretat jurídica.

És per aquesta raó que en aquest últim capítol hem afegit una guia, en base als set principis establerts en el qüestionari, en la que sintetitzem els requisits ètic-legals formulats de manera que reflecteixi quins aspectes haurien de ser considerats en la redacció de contractes sobre sistemes d'IA. Recaurà sobre les parts contractants determinar quina d'elles (sinó totes), seran responsables de cadascun d'aquests aspectes. D'aquesta manera, aspirem a que la guia serveixi com a una eina que permeti a les persones proveïdores i usuàries saber quin és el contingut esperable en contractes envers aquesta matèria.

Per a crear aquest nou apartat hem pres de referència l'informe fet per *Society for Computers & Law (SCL) AI Group* sobre *Artificial Intelligence Contractual Clauses*.¹¹¹, replicat les preguntes del **Model PIO** les quals s'han de respondre en funció de quin subjecte sigui en la utilització del sistema d'IA que s'indica.

Principi 1: Transparència i explicabilitat

1.1. Anàlisi preliminar de l'ús del sistema

Nº	Recomanació de clàusula
----	-------------------------

1.1.1	El sistema anirà acompanyat d'informació precisa sobre per a què s'utilitza així com la identitat i les dades de contacte de la persona proveïdora o representants.
-------	---

¹¹¹ Society for Computers & Law (SCL) AI Group – AI Clauses Projecte (octubre 2023). *Artificial Intelligence Contractual Clauses*. (Informe guia per a detallar la responsabilitat de proveïdors i clients en les relacions contractuals en el marc de sistemes d'IA). Disponible a: <https://www.scl.org/news/13004-society-for-computers-and-law-ai-group-launches-artificial-intelligence-contractual-clauses> (consultada el 17 d'octubre 2023).

- 1.1.2 Es garantirà que el procés de generació de resultats del sistema compleix amb els següents requisits:
- Està ben documentat i reproduïble per a detectar futurs problemes.
 - Utilitza el model més simple i intel·ligible en favor de la transparència.
 - Pren en consideració les competències i alfabetització en matèria d'intel·ligència artificial de totes les persones usuàries.
 - Realitza registres automàtics sobre el seu funcionament.

1.2. Explicabilitat

Nº	Recomanació de clàusula
----	-------------------------

- | | |
|-------|---|
| 1.2.1 | Es documentarà i es farà pública la següent informació relativa al sistema: <ul style="list-style-type: none"> • El seu procés de desenvolupament i les persones que hi han estat implicades. • La informació tècnica necessària per al seu ús. • Instruccions concises, clares i escrites en un llenguatge accessible, sobre el seu funcionament. • El procés pel qual el sistema arriba a un resultat determinat i els resultats previstos. • Les possibles limitacions del sistema. • Informació relativa a l'intercanvi i cessió de dades així com les vies i mecanismes que permeten a les persones interessades exercir els seus drets. |
| 1.2.2 | El sistema comptarà amb un mecanisme que permeti identificar el contingut que genera com a creació d'aquest. |
| 1.2.3 | Es prendran mesures per tal que el nivell de transparència i explicabilitat del sistema no suposi un risc per a la privacitat de les persones ni la mateixa seguretat del sistema. |

1.3. Traçabilitat i representativitat

Nº	Recomanació de clàusula
----	-------------------------

- | | |
|-------|---|
| 1.3.1 | En relació amb les dades utilitzades pel sistema, s'assegurarà el compliment dels següents requisits: <ul style="list-style-type: none"> • El sistema anirà acompanyat de documentació relativa al tipus de dades utilitzades, la seva procedència, i els canvis que han patit en cada fase del seu cicle de vida. • Es prendran mesures per verificar la representativitat i adequació de les dades utilitzades. • El sistema comptarà amb salvaguardes per verificar l'edat de les persones. |
| 1.3.2 | El registre d'arxius que genera el sistema d'IA serà conservat durant un termini mínim de sis mesos. |

1.4. Protocols de comunicació

Nº Recomanació de clàusula

- 1.4.1 El sistema disposarà de les següents eines de comunicació:
- Una funció que permeti a les persones usuàries realitzar comentaris sobre el seu funcionament.
 - Un sistema de notifikacions en cas d'incident greu o error.
- 1.4.2 S'establirà una política de participació de diferents grups d'interès (*stakeholders*) on s'inclouï les persones usuàries finals i/o receptores.

Principi 2: Justícia i equitat

2.1. Inclusió i diversitat

Nº Recomanació de clàusula

- 2.1.1 El sistema d'IA comptarà amb mesures d'inclusió i equitat, especialment en relació amb els següents aspectes:
- Testatge dels resultats del sistema per a diferents grups afectats.
 - Mesures d'augment de l'accessibilitat.
 - Mesures que recolzin el seu ús per part de persones en situació de vulnerabilitat.
 - Mesures per a garantir que el sistema s'adapta a un ampli espectre de preferències i habilitats individuals.
- 2.1.2 El sistema serà sotmès a una avaluació amb la finalitat de verificar que no utilitza variables o *proxies* injustament discriminatòries abans de la seva comercialització/utilització.
- 2.1.3 El grup de desenvolupament del sistema d'IA ha d'incloure persones de gènere no masculí, persones de diversos orígens o cultures i de diverses disciplines de coneixement (més enllà de la informàtica i l'enginyeria).
- 2.1.4 L'organització promourà una política organitzativa que tingui com a prioritat la diversitat, l'equitat i la inclusió.

2.2. Identificació i mitigació de biaixos

Nº Recomanació de clàusula

- 2.2.1 El sistema comptarà amb mesures i mecanismes per a detectar, corregir i mitigar possibles biaixos durant tot el seu cicle de vida.

Especialment, les mesures aniran adreçades als biaixos presents en:

- La fase de disseny o implementació.
- Les dades d'entrenament i posteriors.
- Categories canviant o inadequades.

- 2.2.2 Abans de la seva comercialització/utilització el sistema serà sotmès a una avaluació sobre l'impacte dels seus possibles biaixos, especialment aquells que podrien afectar els drets, salut o seguretat de les persones.
- 2.2.3 El sistema complirà amb els estàndards de classificació que tracten els biaixos relacionats amb l'edat, l'ètnica, la raça, el sexe o la discapacitat d'acord amb la normativa aplicable.
- 2.2.4 El sistema inclourà mecanismes de seguretat per tal de prevenir els següents incidents:
- Anomalies o accions fora dels límits predeterminats.
 - Sortides esbiaixades i bucles de retroalimentació.
- 2.2.5 Les mesures per a la detecció, correcció i mitigació de biaixos compliran amb la normativa aplicable en matèria de protecció de dades. En específic, es garantirà el compliment del Reglament (UE) 2016/679, la Directiva (UE) 2016/ 680, i el Reglament (UE) 2018/1725.
- 2.2.6 Es proporcionarà informació detallada sobre les dades i els recursos utilitzats per a prevenir i detectar la inadequació o els biaixos de les dades, així com el risc del biaix d'automatització.

Principi 3: Seguretat i no maleficència

3.1. Funcionament del sistema

Nº	Recomanació de clàusula
----	-------------------------

- | | |
|-------|---|
| 3.1.1 | <p>El sistema anirà acompanyat de la següent informació:</p> <ul style="list-style-type: none"> • El nivell de precisió i seguretat del sistema. • La manera i el grau d'influència que les accions de les persones usuàries poden tenir sobre el rendiment del sistema. • Els possibles comportaments i escenaris que mai hauria de transgredir per garantir la seguretat i preservar la no maleficència del sistema. • Els mecanismes de supervisió i control del sistema (tant intern com extern). |
| 3.1.2 | <p>Les persones que han dissenyat/dissenyaran el sistema, proporcionaran orientació sobre com interpretar i respondre les mètriques que generi.</p> |

3.2. Traçabilitat per a la gestió del risc

Nº	Recomanació de clàusula
----	-------------------------

- 3.2.1 Prèviament a la seva comercialització/utilització el sistema serà sotmès a una avaluació que incorpori els següents aspectes:
- Els possibles impactes del sistema sobre la salut, la seguretat i els drets de les persones afectades.
 - El risc que les dades recollides, generades o utilitzades pel sistema siguin emprades per discriminar a persones de manera negativa.
 - Els possibles riscos i danys que provocaria el sistema en cas de realitzar prediccions inexactes en els escenaris previstos.
 - Els riscos que comportaria utilitzar el sistema més enllà dels usos previstos.
- 3.2.2 El sistema comptarà amb un protocol general sobre traçabilitat de les dades per a la gestió del risc.
- 3.2.3 El sistema comptarà amb mitjans que permetin les següents funcions:
- Identificar, avaluar i adoptar mesures respecte als riscos sorgits del seu ús i de les dades recollides després d'entrar en funcionament.
 - Informar sobre els riscos residuals del sistema que no hagin pogut ser corregits ni mitigats.

3.3. Mecanismes de seguretat

Nº Recomanació de clàusula

- 3.3.1 El sistema comptarà amb les següents mesures:
- Mesures de resistència davant errors sorgits per la seva interacció amb altres sistemes o persones.
 - Mesures de resistència i mitigació d'errors sorgits d'intents de manipulació per persones no autoritzades.
 - Mesures d'examen continuu sobre la precisió de les decisions preses pel sistema.
- 3.3.2 Les persones usuàries del sistema d'IA podran controlar fins a quin punt hi estan exposades al mateix i revocar el seu consentiment en qualsevol moment sense que això comprometi el seu rendiment.

3.4. Protecció enfront d'atacs

Nº Recomanació de clàusula

- 3.4.1 Prèviament a la seva comercialització/utilització el sistema serà sotmès a una avaluació per a garantir la seva seguretat, integritat i resiliència davant de diferents formes d'atac.

- 3.4.2 Prèviament a la seva comercialització/utilització els conjunts de dades utilitzades pel sistema seran sotmesos a una avaluació per verificar que no han estat prèviament compromesos o piratejats.

Principi 4: Responsabilitat i retiment de comptes

4.1. Control

Nº	Recomanació de clàusula
4.1.1	Es prendran mesures per garantir que les persones involucrades en el control de les decisions preses pel sistema tinguin una comprensió adequada sobre el seu funcionament i comptin amb la capacitat necessària per exercir aquesta funció.
4.1.2	El sistema comptarà amb les eines que permetin a les persones encarregades del seu control intervenir, modificar, eliminar o revertir les decisions preses pel sistema.
4.1.3	El sistema anirà acompanyat d'informació i documentació relativa als següents aspectes: <ul style="list-style-type: none"> • Els límits dels mecanismes de control del sistema. • Les mesures de supervisió humana amb les que compta el sistema.

4.2. Retiment de comptes

Nº	Recomanació de clàusula
4.2.1	Prèviament a la utilització/comercialització del sistema es determinarà: <ul style="list-style-type: none"> • La persona legalment responsable de les accions i/o decisions que pren durant tot el seu cicle de vida. • La persona responsable de les mesures de vigilància humana del sistema.
4.2.2	L'organització adoptarà les següents mesures: <ul style="list-style-type: none"> • Portarà a terme una avaluació de cara a determinar la influència que el sistema suposa en la presa de decisions de l'organització. • Establirà mecanismes de revisió periòdica sobre la responsabilitat i el retiment de comptes amb els diferents agents involucrats en el seu desenvolupament i ús.

4.3. Figures de protecció

Nº	Recomanació de clàusula
4.3.1	L'organització prendrà les següents mesures: <ul style="list-style-type: none"> • Facilitar la demostració del compliment de la legislació vigent. • Formes de reparació o compensació en cas de perjudicis causats pel sistema.

- Determinar figures de protecció envers les persones usuàries i les persones afectades pel sistema.

4.4. Capacitació

Nº Recomanació de clàusula

- 4.4.1 L'organització es compromet a no realitzar cap afirmació que pugui conduir a sobre estimar les capacitats del sistema i que no sigui demostrable compartint dades i el codi d'aquest.

4.5. Promoció d'una cultura de l'ètica i responsabilitat relacionada amb la IA

Nº Recomanació de clàusula

- 4.5.1 L'organització desenvoluparà un codi ètic per a l'ús responsable de la intel·ligència artificial.
- Inclourà els següents punts:
- Promoció de l'ús responsable de la intel·ligència artificial per part del personal de l'organització.
 - Portar a terme la determinació dels objectius del sistema i la revisió del seu funcionament partint de la perspectiva de l'ús responsable de la intel·ligència artificial.
 - Adoptar mesures per assegurar que el sistema, en el procés de generar decisions, pren en consideració les implicacions sobre els drets i el benestar de les persones.

Principi 5: Privacitat

5.1. Protecció de la privacitat

Nº Recomanació de clàusula

- 5.1.1 Comptarà amb mecanismes de protecció de dades presents durant tot el seu cicle de vida encaminats a garantir els següents aspectes:
- Que les dades de caràcter personal siguin tractades d'acord amb el grau de protecció legalment requerit per tal d'evitar-ne el mal ús, l'alternació, la pèrdua, o la sostracció per part de tercers.
 - Que les dades subministrades per la persona interessada no siguin venudes, llogades, ni cedides sense el seu consentiment.
 - Que el sistema compta amb processos per a mantenir o millorar la privacitat i protecció de les dades durant tot el seu cicle de vida.
 - Que es fan servir tècniques d'anonimat, xifratge i agregació.
 - Que existeix un protocol per a obtenir el consentiment de les persones afectades abans d'iniciar qualsevol processament de dades a través del

El sistema, i la informació relativa a aquestes accions és comprensible i accessible per a totes les possibles persones usuàries, inclosos aquelles amb necessitats especials.

- Que existeix un mecanisme a través del qual la persona interessada pot sol·licitar que la seva informació sigui eliminada.

5.1.2 El sistema garantirà l'accés igualitari per a persones amb discapacitat i en situació vulnerable tot respectant la seva privadesa i dignitat.

5.2. Governança de dades

Nº	Recomanació de clàusula
----	-------------------------

5.2.1	El sistema comptarà amb un registre de la informació d'accés a les dades que permeti identificar clarament qui, quan i amb quin propòsit hi accedeix.
-------	---

5.2.2	Es prendran mesures per garantir que les persones responsables del processament i gestió de dades comptin amb les competències necessàries per a realitzar aquestes funcions i coneixements actualitzats sobre la matèria.
-------	--

5.2.3	De cara a garantir l'adequació i l'ús reposable de les dades utilitzades pel sistema es prendran les següents mesures: <ul style="list-style-type: none"> • S'establirà un procediment per assegurar que els conjunts de dades usats siguin adients i rellevants pel rendiment i resultat previst del sistema i que siguin adequades pel context en el qual s'utilitzarà. • El procés de recopilació i preparació de les dades usades serà documentat. • El sistema utilitzarà mesures de privadesa (com per exemple la pseudonimització de les dades) i limitarà la reutilització de les dades personals sensibles.
-------	---

5.2.4	El sistema està/ha estat dissenyat de manera que puguin garantir les següents qüestions: <ul style="list-style-type: none"> • El sistema s'adhereix als principis de minimització de dades i protecció de dades des del disseny i per defecte adherir-se als principis de minimització i protecció de dades. • El sistema pot ser entrenat sense la necessitat de transmetre o copiar dades en brut o estructurades.
-------	--

Principi 6: Autonomia

6.1. Impacte en les capacitats de les persones usuàries

Nº	Recomanació de clàusula
----	-------------------------

6.1.1	El sistema inclourà un procés d'avaluació per a garantir que no disminueix el nombre d'eleccions possibles i no obliga o força a prendre unes determinades decisions en general ni en cap fase del seu cicle de vida.
-------	---

- 6.1.2 El sistema anirà acompanyat d'un protocol de comprovació que permeti certificar que ajuda les persones a prendre decisions millors i més informades.
- 6.1.3 El sistema comptarà amb mecanismes que garanteixin els següents aspectes:
- Que les persones usuàries finals siguin conscients que interactuen amb una intel·ligència artificial i estan prou capacitades i informades per a fer-ho.
 - Que els resultats que generi siguin etiquetats d'alguna manera que permeti a les persones identificar que aquest contingut ha estat general per una intel·ligència artificial.
 - Que no posa en risc els nivells d'autonomia de les persones usuàries finals, evitant l'ús de tècniques manipulatives o subliminars i adaptant-se a les preferències i necessitats de la persona.

6.2. Percepció del sistema

Nº Recomanació de clàusula

- 6.2.1 El sistema comptarà amb mecanismes que garanteixin que les seves operacions siguin transparents, clares, sinceres i no encoratgen a les persones usuàries a sobreestimar les seves capacitats.
- 6.2.2 El sistema comptarà amb els següents mecanismes:
- Mesures de supervisió humana que possibilitin gestionar el seu grau d'autonomia i adaptabilitat.
 - Mecanisme de limitació del grau d'autonomia del sistema per a evitar comportaments no desitjats o d'alt risc.
 - Adaptar-se i aprendre del seu entorn sense comprometre la seguretat ni estàndards ètics.
- 6.2.3 El sistema serà sotmès a una avaluació per a identificar i mitigar els riscos de les seves capacitats i el seu grau d'autonomia, així com la seva adaptabilitat a noves tasques.

Principi 7: Sostenibilitat

7.1. Desenvolupament sostenible

Nº Recomanació de clàusula

- 7.1.1 Es garantirà que en el disseny, la implementació i l'ús el sistema s'han pres en consideració les limitacions i obstacles derivats de la bretxa digital i l'accés social no igualitari.
- 7.1.2 Abans de la seva comercialització i/o utilització, el sistema serà sotmès a una avaluació sobre els seus impactes als drets de les persones, la seguretat, la salut i el medi ambient. Aquesta avaluació pren especialment en consideració els següents àmbits:
- Impacte sobre els drets laborals.
 - Impacte sobre la qualitat de vida de les persones.
 - Impacte i riscos relatius al desenvolupament sostenible.

- Mesures de compensació justa i tracte ètic a les persones implicades en totes les fases del cicle de vida del sistema i dels afectats per la seva implementació i ús.

7.1.3 El sistema comptarà amb mesures que garanteixin el respecte i ús ètic de les dades protegides per la propietat intel·lectual. Entre aquestes mesures s'inclourà fer pública la informació relativa a les dades protegides per la legislació sobre propietat intel·lectual emprades pel sistema.

7.1.4 En el desenvolupament, la comercialització, la implementació i/o la utilització del sistema es compactarà amb la participació de parts interessades rellevants.

7.1.5 L'organització col·laborarà activament amb la representació laboral del seu personal per tal d'identificar, corregir i mitigar els possibles riscos que l'adquisició, implementació i/o ús del sistema puguin comportar per al benestar i els drets laborals de les persones treballadores.

7.2. Impacte mediambiental

Nº	Recomanació de clàusula
----	-------------------------

7.2.1	El sistema comptarà amb mecanismes que li permetin enregistrar el seu consum d'energia i impacte ambiental durant tot el seu cicle de vida.
-------	---

7.2.2	L'organització implementarà mecanismes i estratègies adreçades a millorar l'eficiència energètica del sistema i reduir la seva petjada ambiental, especialment quan s'utilitzen conjunts de dades extensos.
-------	---

7.2.3	Abans de la seva comercialització i/o utilització, el sistema serà sotmès a una avaluació en la qual s'adreci, com a mínim, els següents aspectes: <ul style="list-style-type: none"> • L'eficiència energètica del sistema. • Explorar l'ús de fonts d'energia renovables i pràctiques d'informàtica verda.
-------	--

9. BIBLIOGRAFIA

Access now & European Centre for Not-for-Profit Law (2023). *Towards meaningful fundamental rights impact assessments under the DSA*. (Informe d'avaluació de l'impacte dels Drets Fonamentals segons la Llei de Seguretat Digital). Disponible a: <https://www.accessnow.org/wp-content/uploads/2023/09/DSA-FRIA-joint-policy-paper-September-2023.pdf> (consultat el 19 de setembre de 2023).

ACCIÓ- Agència per la Competitivitat de l'Empresa en col·laboració amb el CIDAI. (2024) *La intel·ligència artificial a Catalunya*. (Informes tecnològics). Disponible a: <https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/la-intel·ligencia-artificial-a-catalunya> (consultada el 12 de desembre 2024).

ACNUDH (2011). Principis rectors sobre Empresa i Drets Humans. Disponible a: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusiness_hr_en.pdf (consultada el 23 de desembre de 2023).

ACNUDH (2018). Un enfocament basat en els drets humans per a les dades: no deixar ningú enrere en l'Agenda 2030 per al Desenvolupament Sostenible. Disponible a: <https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf> (consultada el 20 de novembre de 2023).

ACNUDH (2023) OHCHR i negocis i drets humans. Disponible a: <https://www.ohchr.org/en/business-and-human-rights> (consultada el 23 de desembre de 2023).

ADP. Disponible a: <https://es.adp.com/privacidad.aspx> (consultada el 12 de març de 2024).

Agència catalana de seguretat alimentària (2023) *Legislació sobre els organismes modificats genèticament*. Disponible a: <https://shorturl.at/xSSiu> (consultat el 6 de novembre de 2023).

Agència espanyola de protecció de dades. (2023) *Intel·ligència artificial: Transparència* (Informe en relació a l'encaix de la transparència en la normativa de la Intel·ligència Artificial). Disponible a: <https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-transparencia> (consultat el 25 de setembre de 2023).

Aquilar, R. (2024) Quin grau de processió té Google Translate? *Weglot*. Disponible a: <https://www.weglot.com/es/blog/how-accurate-is-google-translate> (consultada el 11 de gener de 2024).

Ahmed, A. (2023) El repte d'Apple en IA: analitzar les limitacions de Siri i els avenços dels rivals. *Digital information world*. Disponible a: <https://shorturl.at/ZbkPo> (consultada el 17 d'octubre de 2023).

Ahmed, M. (2020) TikTok: Trump diu que l'acord d'Oracle per a l'aplicació de vídeo “té la meua benedicció”. *BBC*. Disponible a: <https://www.bbc.com/news/technology-54349538> (consultada el 15 de febrer de 2024).

AI Ethics Impact Group (2020) De els principis a la pràctica. Un marc interdisciplinari per operacionalitzar l'ètica de la IA. Disponible a: <https://www.ai-ethics-impact.org/en> (consultada el 7 de març de 2023).

Allen Institute for Artificial Intelligence. (s.d). Our Team. Disponible a: [AllenNLP - Team — Allen Institute for AI \(allenai.org\)](https://allenai.org) (consultada el 15 de febrer de 2024).

Andrews, E.L. (2021) Volant a cegues: Les eines d'IA als hospitals no estan ben documentades. *HAI Stanford University Human-Centred Artificial Intelligence*. Disponible a: <https://hai.stanford.edu/news/flying-dark-hospital-ai-tools-arent-well-documented> (consultada el 10 d'octubre 2023).

Arthur, C. (2014) Tendències de la grip de Google : preveient la grip. *The Guardian*. Disponible a: [Google Flu Trends is no longer good at predicting flu, scientists find | Google | The Guardian](https://www.theguardian.com/technology/2014/mar/12/google-flu-trends) (consultada el 12 de març de 2024).

Asurion. (s.d.) L'Alexa escolta les converses que tenim a casa? Disponible a: [Is Alexa always listening to your conversations? | Asurion](https://www.asurion.com/press/2023/03/04/is-alexa-always-listening-to-your-conversations/) (consultada el 4 de març de 2023).

Assemblea General de les Nacions Unides (1948) Declaració universal dels drets humans. Disponible a: <https://shorturl.at/lfvgo> (consultada el 12 de novembre de 2023).

Assemblea General de les Nacions Unides (1966) Pacte internacional de drets civils i polítics. Disponible a: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (consultada el 8 de novembre de 2023).

Assemblea General de les Nacions Unides (1966) Pacte internacional de drets econòmics, socials i culturals. Disponible a: <https://www.ohchr.org/sites/default/files/cescr.pdf> (consultada el 8 de novembre de 2023).

Assemblea General de les Nacions Unides (1979) Convenció sobre l'eliminació de totes les formes de discriminació contra la dona. Disponible a: [A/RES/34/180: Convention on the Elimination of All Forms of Discrimination against Women \(un.org\)](https://www.un.org/en/convention-on-the-elimination-of-all-forms-of-discrimination-against-women) (consultada el 14 de desembre de 2023).

Assemblea General de les Nacions Unides (2022) Resolució A/76/L.75: El dret humà a un medi ambient net, saludable i sostenible. Disponible a: <https://tinyurl.com/mtu6tyhn> (consultada el 7 de desembre de 2023).

Attard-Frost, B., De los Ríos, A. & Walters, D.R. (2022). L'ètica de les pràctiques empresarials en IA: una revisió de 47 guies d'ètica en IA. Springer link. AI and Ethics. Disponible a: <https://doi.org/10.1007/s43681-022-00156-6> (consultada el 7 de març de 2023).

AutoGrid (s/d) Una plataforma para conservar, desplegar, gestionar y monetizar los recursos energéticos. Disponible a: <https://www.auto-grid.com/> (consultada el 11 de gener de 2024).

Aznar Domingo, A. & Domingues Villarroel, M.P. (2022) La responsabilitat civil derivada del uso de intel·ligència artificial. El Derecho. Disponible a: <https://elderecho.com/responsabilidad-civil-derivada-uso-inteligencia-artificial> (consultada el 20 de març de 2024).

Bach, M., Wener, A. & Palt, M. (2019) La proposta del mètode de submostreig per aprendre de conjunts de dades desequilibrats. ScienceDirect, volume 159. 125-134. Disponible a: <https://www.sciencedirect.com/science/article/pii/S1877050919313456> (consultada el 20 de juny de 2024).

Barcelona Declaration (2017) Declaració de Barcelona per al desenvolupament i ús adequat de la intel·ligència artificial a Europa, IIIA CSIC. Disponible a: <https://www.iiia.csic.es/barcelonadeclaration/> (consultada el 7 de març de 2023).

Bakiner, O. (2023) The promises and challenges of addressing artificial intelligence with human rights. Disponible a: <https://journals.sagepub.com/doi/full/10.1177/20539517231205476> (consultada el 15 de novembre de 2023).

BBC Mundo (2018) Les IA son sexistes i racistes? El debat està obert. Disponible a: <https://www.bbc.com/mundo/noticias-45823470> (consultada el 15 de febrer de 2024).

Bernadette, J. (2023) Com funciona Siri. Howstuffworks? Disponible a: <https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/siri4.htm> (consultada el 17 d'octubre de 2023).

Bertuzzi, Luca. (2023) Els responsables polítics de la UE han estat debatent algunes condicions de filtre que permetrien als desenvolupadors d'IA evitar complir amb el règim més estricte de la llei d'Intel·ligència Artificial de la UE. Però aquest compromís polític s'està trobant amb

problemes legals significatius. Euractiv. Disponible a: <https://tinyurl.com/3mn4b7ep> (consultada el 26 de setembre de 2023).

Bertuzzi, Luca. (2023) AI Act: Els principals eurodiputats revisen la classificació de l'alt risc, ignorant el dictamen jurídic negatiu. Euractiv. Disponible a: <https://tinyurl.com/3mn4b7ep> (consultada el 26 de setembre de 2023).

Boot, R. (2023). S'amplia l'ús de la IA per avaluar les sol·licituds de crèdit universal i reduir el frau. The Guardian. Disponible a: <https://www.theguardian.com/society/2023/jul/11/use-of-artificial-intelligence-widened-to-assess-universal-credit-applications-and-tackle> (consultada el 4 de març de 2024).

Boot, R. (2023) S'adverteix al RU de la falta de transparència en l'ús de la IA per examinar les sol·licituds de protecció social. The Guardian. Disponible a: <https://www.theguardian.com/politics/2023/sep/03/uk-warned-over-lack-transparency-use-ai-vet-welfare-claims> (consultada el 4 de març de 2024).

Bunting, G. (2023) Com la IA podria millorar els jocs per a les persones amb discapacitat. Wired. Disponible a: <https://www.wired.com/story/ai-make-gaming-better-accessibility/> (consultada el 20 de març de 2024).

Cad&Lan (s.d) Com la IA pot contribuir a l'estalvi energètic. Disponible a: <https://www.cadlan.com/noticias/ahorro-energetico-con-ia/> (consultada el 12 de març de 2024).

Calaway, A. (2021) IA i la lluita contra el tràfic de persones. Disponible a: <https://tinyurl.com/452jvt3n> (consultada el 23 de desembre de 2023).

Castilla Juárez, K. (2022) El dret humà al medi ambient: tard o insuficient? Disponible a: <https://tinyurl.com/4nabt8td> (consultada el 22 de gener de 2023).

Castillo del, C. (2023) Crear una sola imatge amb IA consumeix tanta energia com carregar un mòbil. elDiario.es. Disponible a: https://www.eldiario.es/tecnologia/crear-sola-imagen-inteligencia-artificial-consume-energia-cargar-movil_1_10748992.html (consultada el 15 de febrer de 2024).

CCMA (2016) Twitter converteix un compte robot en un usuari racista i sexista en 24 h. Disponible a: <https://www.ccma.cat/324/twitter-converteix-un-compte-robot-en-un-usuari-racista-i-sexista-en-24-hores/noticia/2720895/> (consultada el 20 de març de 2024).

CEPYME News. (s.d). Google treballa en la cerca de multimodals: què són i com funcionen. Disponible a: <https://cepymenews.es/busquedas-google-multimodal/> (consultada el 12 de març de 2024).

Comissari per als Drets Humans del Consell d'Europa (2023) IA i drets humans. Disponible a: <https://www.coe.int/en/web/commissioner/thematic-work/artificial-intelligence> (consultada el 7 de desembre de 2023).

Comissió Europea (2020) Explorant el potencial de la IA en la lluita contra l'abús infantil en línia. Disponible a: <https://digital-strategy.ec.europa.eu/en/library/exploring-potential-ai-fight-against-child-online-abuse> (consultada el 23 de desembre de 2023).

Comissió Europea (2021) Proposta de Reglament del Parlament Europeu i del Consell, normes harmonitzadores en matèria d'Intel·ligència Artificial (Artificial Intelligence Act) i modifica determinat actes legislatius de la UE. Disponible a: [resource.html \(europa.eu\)](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF) i https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (consultada el 4 de març de 2023).

Comissió Europea (2022) Proposta de Directiva del Parlament Europeu i del Consell per adoptar les normes de la responsabilitat civil extracontractual de la IA (AI Liability Directive). Disponible a: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0496 (consultada el 20 de març de 2023).

Comissió Europea (2023) European Data Governance Act (informe sobre l'impacte de la Llei de governança de dades). Disponible a: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act> (consultada el 26 de setembre de 2023).

Comissió Europea (2023) Intel·ligència artificial – Preguntes i respostes. Disponible a: [Artificial Intelligence – Q&As \(europa.eu\)](https://artificial-intelligence-q&as.europa.eu) (consultada el 14 de desembre de 2023).

Comitè ad hoc sobre intel·ligència artificial del Consell d'Europa (2021) Intel·ligència artificial, drets humans, democràcia i l'estat de dret. A Primer. Disponible a: <https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a> (consultada el 7 de novembre de 2023).

Comitè ad hoc sobre intel·ligència artificial del Consell d'Europa (2020) Towards regulation of AI systems. Disponible a: <https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a> (consultada el 10 de desembre de 2023).

Comitè sobre Intel·ligència Artificial del Consell d'Europa (2023) Projecte de Conveni marc intel·ligència artificial, drets humans, democràcia i l'estat de dret. Disponible a: <https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043> (consultada el 19 de desembre de 2023).

Consell d'Europa. Carta social europea (revisada) el 3 de maig 1996. Disponible a: [CETS 163 - European Social Charter \(Revised\) \(coe.int\)](https://rm.coe.int/t/t09/1680ade043/1680ade043.pdf) (consultada el 20 de setembre).

Consell d'Europa (1950) Conveni europeu de drets humans, modificat per les disposicions del Protocol nº 15 (STCE nº 213) a partir de la seva entrada en vigor l'1 d'agost del 2021 i del Protocol nº 14 (STCE nº 194) a partir de la seva entrada en vigor l'1 de Juny de 2010. Disponible a: [European Convention on Human Rights \(coe.int\)](https://rm.coe.int/t/t09/1680ade043/1680ade043.pdf) (consultada el 20 de setembre).

Consell d'Europa (1981) Conveni per a la Protecció de les Persones Respecte al Tractament Automatitzat de Dades de Caràcter Personal, fet a Estrasburg el 28 de gener de 1982. Disponible a: [CETS 108 - Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data \(coe.int\)](https://rm.coe.int/t/t09/1680ade043/1680ade043.pdf) (consultada el 15 de setembre de 2023).

Consell d'Europa (2022) El Comitè de Ministres demana als Estats membres que reconeguin el dret a un medi ambient net, sa i sostenible com un dret humà. Disponible a: [The Committee of Ministers calls on member states to recognise the right to a clean, healthy and sustainable environment as a human right - Human Rights and Rule of Law \(coe.int\)](https://rm.coe.int/t/t09/1680ade043/1680ade043.pdf) (consultada el 4 de desembre de 2023).

Consell d'Europa (2024) Informe Explicatiu del Conveni Marc del Consell d'Europa sobre intel·ligència artificial, drets humans, democràcia i l'estat de dret. Disponible a: <https://rm.coe.int/1680afae67> (consultada el 20 de juliol de 2024).

Consell d'Europa (2014) Recomanació CM/Rec (2014) 6 del Comitè de Ministres dels Estats membres sobre una Guia dels drets humans dels usuaris d'internet. Disponible a: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900-0016804d5b-31 (consultada el 13 de desembre de 2023).

Consell de Drets Humans de les Nacions Unides (2021) Resolució A/HRC/48/L.23/Rev.1: El dret humà a un medi ambient sense risc, net, saludable i sostenible. Disponible a: [The human right to a clean, healthy and sustainable environment : \(un.org\)](https://www.un.org/en/press/docs/2021/211215_ahrc48l23rev1.html) (consultada el 7 de desembre de 2023).

Consell de la Unió Europea (2024) Artificial intelligence (AI) act: El Consell dona llum verda definitiva a les primeres normes mundials sobre IA. Disponible a: <https://tinyurl.com/4xy55j5z> (consultada el 21 de maig de 2024).

Consell de Seguretat de Nacions Unides (2023) La comunitat internacional ha d'enfrontar-se urgentment a la nova realitat de la Intel·ligència Artificial Generativa, subratllant els oradors mentre el Consell de Seguretat debat els riscos i els avantatges. Disponible a: <https://press.un.org/en/2023/sc15359.doc.htm> (consultada el 13 de novembre de 2023).

Cosper, J. (2021) 7 grans exemples d'accessibilitat web per a inspirar-te. Dream host. Disponible a: <https://www.dreamhost.com/blog/es/grandiosos-ejemplos-accessibilidad-web/> (consultada el 20 de març de 2024).

Davis, W. (2023) Tesla sota investigació a Califòrnia sobre els problemes de seguretat del pilot automàtic i la publicitat enganyosa. The Verge. Disponible a: [Tesla under investigation in California over Autopilot safety issues and false advertising - The Verge](https://www.theverge.com/2023/3/4/tesla-under-investigation-in-california-over-autopilot-safety-issues-and-false-advertising) (consultada el 4 de març de 2024).

Depor. (2022). Google Translate: Avantatges, debilitats i com hem d'utilitzar-ho correctament aquesta eina poderosa. Disponible a: <https://tinyurl.com/3apwb3zy> (consultada el 15 de febrer de 2024).

Diaz, N. (2022) Epic revisa l'algoritme de la sepsis. Becker's Hospital Review. Disponible a: <https://tinyurl.com/jjy kz xkk> (consultada el 10 d'octubre 2023).

Ding, M. & Yan, J. & Chao, G. & Zhang, S. (2023) Una aplicació d'intel·ligència artificial fa el cribratge del càncer colorectal per colonoscòpia: perspectives de futur. (Article number: 199). Oncology Reports. Disponible a: <https://www.spandidos-publications.com/10.3892/or.2023.8636#> (consultada el 20 de març de 2024).

De Vries, A. (2023) La creixent empremta energètica de la IA. Joule. Disponible a: [https://www.cell.com/joule/fulltext/S2542-4351\(23\)00365-3](https://www.cell.com/joule/fulltext/S2542-4351(23)00365-3) (consultada el 22 de desembre de 2023).

Duffy, C. & Fung, B. (2023) Amazon pagarà més de 30 milions de dòlars per a resoldre les queixes de privacitat de la FTC sobre Alexia i Ring. CNN Business. Disponible a: <https://edition.cnn.com/2023/05/31/tech/amazon-ring-ftc-complaint/index.html> (consultada el 20 de març de 2024).

DW español. (s.d). Meta comparteix les dades dels seus usuaris. Disponible a: [Meta comparte los datos de sus usuarios – DW – 10/08/2023](https://www.dw.com/es/meta-comparteix-los-datos-de-sus-usuarios/a-63188888) (consultada el 15 de febrer de 2024).

El Economista (2023) La falta de capacitació i coneixements eviten que les startups s'enlairin. Disponible a: <https://tinyurl.com/378tx88n> (consultada el 15 de febrer de 2024).

Energy5. Disponible a: <https://energy5.com/es/guia-para-el-usuario-como-aumentar-la-inteligencia-humana-con-ia> (consultada el 7 de febrer de 2024).

Erdenesanaa, D. (2023) La intel·ligència artificial podria necessitar aviat tanta electricitat com tot un país. Disponible a: <https://www.nytimes.com/2023/10/10/climate/ai-could-soon-need-as-much-electricity-as-an-entire-country.html> (consultada el 22 de desembre de 2023).

EU Artificial Intelligence Act. (2024) Timeline of Developments. Disponible a: <https://artificialintelligenceact.eu/developments/> (consultada el 4 de juny de 2024).

EurekAlert! (2023) Alimentar la IA podria consumir tanta electricitat com un país petit. Disponible a: <https://www.eurekalert.org/news-releases/1003775> (consultada el 4 de març de 2024).

European Center for Not-for-Profit Law (2023). Civil society calls on EU legislators to ensure the AI Act protects the rule of law. (Informe d'avaluació de l'impacte dels drets fonamentals i la garantia d'aplicar la IA d'acord a la llei). Disponible a: <https://ecnl.org/news/civil-society-calls-eu-legislators-ensure-ai-act-protects-rule-law> (consultada el 3 d'octubre de 2023).

European Data Protection Supervisor (2023) Protecció de dades. Disponible a: [Data Protection | European Data Protection Supervisor \(europa.eu\)](https://www.edps.europa.eu/) (consultada el 26 de novembre de 2023).

European Union Agency for Fundamental Rights. (2020) Negocis i drets humans: Revisió de l'actuació i evolució de la UE. Disponible a: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-business-human-rights_en.pdf (consultada el 25 de novembre de 2023).

Feldman, S. (2023) El termini de la Fed arriba i marxa sense replica de Tesla a les preguntes sobre l'autopilot. Ars technical. Disponible a: <https://arstechnica.com/cars/2023/07/tesla-misses-deadline-to-inform-nhtsa-about-autopilot-problems/> (consultada el 10 d'octubre 2023).

Firewall en entorns corporatius. (s.d). Consultek: blog de seguretat informàtica. Disponible a: <https://blog.conzultek.com/ciberseguridad/firewall-en-entornos-corporativos> (consultada el 4 de març de 2024).

Floridi, L., Holweg, M., Taddeo, M., Amaya Silva, J., Mökander, J & Wen, Y. (2022) capAI – Procediment per avaluar la conformitat dels sistemes d'IA amb la AI Act. Disponible a: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4064091 (consultada el 13 d'octubre de 2023).

For Humanity (2016) Auditoria independent dels sistemes d'IA. Disponible a: <https://forhumanity.center/independent-audit-of-ai-systems/> (consultada el 12 de març de 2024).

FRA (2021) Getting the future right. Intel·ligència artificial i drets fonamentals. Disponible a: [*Getting the future right. Artificial intelligence and fundamental rights \(europa.eu\)](https://european-council.europa.eu/media/en/press-communications/intermediary/asset/116144) (consultada el 21 de novembre de 2023).

Generalitat de Catalunya (2023) Acord de Govern 53/2023, de 21 de març, pel qual s'aprova el Pla nacional per a l'erradicació de l'amiant a Catalunya 2023-2032. Diari Oficial de la Generalitat de Catalunya, 21 de març de 2023. Disponible a: <https://dogc.gencat.cat/ca/document-del-dogc/?documentId=955516> (consultada el 6 de novembre de 2023).

Gertchik, M., Jegede, T., Shah, T., Gutiérrez, A., Beiers, S., Shemtov, N., Xu, K., Samant, A., & Horowitz, A. (2023). Com la política oculta en un algoritme amenaça a les famílies d'aquest comtat de Pensilvania. ACLU. Disponible a: <https://www.aclu.org/news/womens-rights/how-policy-hidden-in-an-algorithm-is-threatening-families-in-this-pennsylvania-county> (consultada el 12 de març de 2024).

Godoy, J.D. (2020) La intel·ligència artificial pot reduir el consum d'energia dels edificis un 30%. El periòdic. Disponible a: <https://tinyurl.com/pkfvttf9> (consultada el 11 de gener de 2024).

Google. (s.d). Product Accessibility. Disponible a: [Accessibility in Our Products & Features — Google \(about.google\)](https://www.google.com/accessibility/) (consultada el 4 de març de 2024).

Granell Querol, A. (2021) Una pàgina web accessible i amable és possible. Museus i accessibilitats. Disponible a: <https://museusiaccessibilitat.blogspot.com/2021/11/una-pagina-web-accessible-i-amable-es.html> (consultada el 10 d'octubre del 2023).

¿Gratas, B. (2023) Perquè és important realitzar un monitoreig d'aplicacions i quines son les mètriques clau? Invagate. Disponible a: [¿Por qué es importante realizar un monitoreo de aplicaciones y cuáles son las métricas clave? \(invagate.com\)](https://invagate.com/por-que-es-importante-realizar-un-monitoreo-de-aplicaciones-y-cuales-son-las-metricas-clave/) (consultada el 20 de març de 2024).

Greenpeace (2017) Clicking Clean: Qui guanya amb la cura per a construir una internet verda? Disponible a: <https://shorturl.at/7wcdj> (consultada el 18 de juliol del 2024).

Hackett, M (2021) Fitbit cerca tancar l'esclatxa de la diversitat en la investigació amb una nova iniciativa d'investigació sobre equitat sanitària. Mobi health news. Disponible a: <https://tinyurl.com/2ky5ru37> (consultada el 20 de març de 2024).

Hacker, P., Naumann, F., Friedrich, T., Grundmann, S., Lehmann, A., & Zech, H. (2022.) AI Compliance – Reptes de l'aproximació entre la ciència de les dades i el dret. J. Ca14 (3) Article 21. Disponible a: <https://doi.org/10.1145/3531532> (consultada el 16 d'octubre de 2023).

Hawkins, D. (2017) Els investigadors utilitzen eines de reconeixement facial per predir la sexualitat, els grups LGTB no estan content. The Washington Post. Disponible a: <https://tinyurl.com/3jufnfww> (consultada el 11 de gener de 2024).

High-Level Expert Group on Artificial Intelligence (2020) Llista de l'avaluació de la IA fiable. Disponible a: <https://tinyurl.com/j48nxufs> (consultada el 7 de març de 2023).

Higuera, A. (2022) Polèmica amb el *chatbot* de Meta: aquesta IA diu “manipulador” i “mala persona” a Zuckerberg. 20 minutos. Disponible a: <https://tinyurl.com/ywyv8664> (consultada el 4 de març de 2024).

Hoseong, C. (2021) El govern va lliurar 170 milions de fotos facials d'entrada al país a una empresa d'IA (traducció coreà). Disponible a: <https://tinyurl.com/2cszdnk8> (consultada el 15 de febrer de 2024).

Ideo.org (2022) Un programa de serveis socials de migrants per a migrants. Reforça les xarxes de recolzament per a ajudar als immigrants a accedir als serveis que necessiten. Inter-American Development Bank (IDB). Disponible a: <https://www.ideo.org/project/alia> (consultada el 20 de juny de 2024).

Laird, J. (2023) *ChatGPT* La majoria de la gent no pot detectar les notícies falses. Tech.co. Disponible a: <https://tech.co/news/chatgpt-spotting-fake-news-impossible> (consultada l'11 d'octubre de 2023).

Lazer, D. & Keenedy, R. (2015) Podem aprendre de l'èpic fracàs de Google Flu Trends? Wired. Disponible a: <https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/> (consultada el 20 de març de 2024).

La importància de un Firewall (2022) Cointic: blog de Seguridad informática. Disponible a: <https://seguridadinformatica.cointic.com.mx/blog/> (consultada el 12 de març de 2024).

Lee, K. & Feeder Cooper, A. & Grimmelmann J., (2023) Parlant de la generació de la IA: els drets d'autor i la cadena de subministrament de la IA generativa. SSRN. Disponible a: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4523551 (consultada el 20 de setembre de 2023).

Llei Orgànica 3/1978, de 14 de desembre, de reforma de l'Estatut d'Autonomia per al País Vasco, BOE núm. 301, de 14 de desembre de 1978. Disponible a: <https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229> (consultada el 4 de desembre de 2023).

Lorenzo, A. (2024) Mastercard llança la seva pròpia IA generativa per ajudar a detectar el frau. El Economista. Disponible a: <https://www.economista.es/tecnologia/noticias/12651895/02/24/mastercard-lanzara-su-propia-ia-generativa-para-ayudar-a-detectar-el-fraude.html> (consultada el 4 de març de 2024).

IBM. (s.d) Watson documentation. IBM Cloud. Disponible a: <https://cloud.ibm.com/developer/watson/documentation> (consultada el 12 de març de 2024).

In Suit (2020) 10 consells sobre com fer accessible la teva pàgina web. Situable Inclusion. Disponible a: <https://www.insuit.net/es/como-hacer-accessible-pagina-web/> (consultada el 16 d'octubre de 2023).

Mac Blog (2020) Els avantatges i desavantatges de Siri. Medium. Disponible a: <https://tinyurl.com/7y79frjj> (consultada el 17 d'octubre de 2023).

Mac Gregor, K. (2024) La majoria dels estudiants utilitzen la IA per als seus estudis i sorgeix l'escletxa digital – Enquesta. University World News. Disponible a: [Most students use AI for studies, digital divide emerges – Survey \(universityworldnews.com\)](https://www.universityworldnews.com/2024/07/17/most-students-use-ai-for-studies-digital-divide-emerges-survey/) (consultada el 17 de juliol de 2024).

Made for minds (2023) Meta comparteix les dades dels usuaris. DW. Disponible a: <https://tinyurl.com/3py7ksnf> (consultada el 16 d'octubre de 2023).

Mantelero, A. (2022) Avaluació de l'impacte en els drets humans i la IA. Disponible a: https://link.springer.com/chapter/10.1007/978-94-6265-531-7_2 (consultada el 20 de novembre de 2023).

Mantelero, A. (2020) La regulació de la IA en el marc dels drets humans: una metodologia de full de ruta. Disponible a: <https://iris.polito.it/handle/11583/2861372> (consultada el 18 de gener de 2024).

Mañes, P. (2023) Reptes startups i com resoldre'ls. Startup Valencia. Disponible a: <https://startupvalencia.org/es/retos-startups-y-como-solventarlos/> (consultada el 11 de gener de 2024).

Mapfre (2021) Intel·ligència artificial: el futur és ara. Disponible a: [Inteligencia artificial: el futuro es ahora](https://www.mapfre.com/actualidad/inteligencia-artificial-el-futuro-es-ahora) (consultada el 15 de febrer de 2024).

Masterson, V. (2024) 9 maneres en les quals la IA ajuda a combatre el canvi climàtic. World economic forum. Disponible a: <https://www.weforum.org/agenda/2024/02/ai-combat-climate-change/> (consultada el 12 de març de 2024).

McCleary, W. (2022) Un estudi dels NIH sobre Fitbit revela la necessitat de diversitat en la investigació. HealthTech Insider. Disponible a: <https://healthtechinsider.com/2022/05/06/nih-fitbit-study-reveals-need-for-diversity-in-research/> (consultada el 15 de febrer de 2024).

Mediamarkt. Disponible a: <https://te-ayudamos.mediamarkt.es/> (consultada el 12 de març de 2024).

Mena Roa, M. (2021) Instagram comparteix amb tercers el 79% de les dades de les persones usuàries. Statista. Disponible a: <https://es.statista.com/grafico/24509/datos-personales-compartidos-con-terceros-por-aplicaciones-ios-seleccionadas/> (consultada l' 11 d'octubre de 2023).

Metingil, N. (2022) Una startup finlandesa de tecnologia sanitària rep capital per a millorar el seu us de dades lliure de GDPR. Artíclel startup. Disponible a: <https://arcticstartup.com/veil-ai-receives-convertible-loan-of-e1-3m/> (consultada el 4 de març de 2024).

Milmo, D. & O'Carroll, L. (2023) Meta, propietaria de Facebook, multada amb 1200 milions d'euros per gestionar malament la informació dels seus usuaris. The Guardian. Disponible a: <https://tinyurl.com/3d9mxkjm> (consultada el 20 de març de 2024).

Minevich, M. (2012) 15 líders en ètica de la IA mostren al món el camí del futur. Forbes. Disponible a: <https://www.forbes.com/sites/markminevich/2021/08/09/15-ai-ethics-leaders-showing-the-world-the-way-of-the-future/> (consultada el 20 de març de 2024).

Minevich, M. & Rossi, F. (2021) Perquè hauria de contractar a un cap d'ètica de la IA? World economic forum. Disponible a: <https://www.weforum.org/agenda/2021/09/artificial-intelligence-ethics-new-jobs/> (consultada el 12 de març de 2024).

Minkkinen, M., Laine, J. & Mäntymäki M. (2022). Auditoria continua de la IA: conceptualització i avaluació d'eines i marcs. DISO 1, 21 (2022). Disponible a: <https://doi.org/10.1007/s44206-022-00022-2> (consultada el 2 d'agost de 2023).

Mohammed R., Rawashdeh J. & Abdullah M. (2020) Aprenentatge automàtic amb tècniques de sobremostreig i submostreig: estudi general i resultats experimentals. Disponible a: <https://ieeexplore.ieee.org/document/9078901> (consultada el 20 de juny de 2024).

Molins Renter, A. (2016) *Tay* aprèn el que no toca. La Vanguardia. Disponible a: <https://www.lavanguardia.com/edicion-impres/20160403/40840835827/tay-apren-el-que-no-toca.html> (consultada el 11 de gener de 2024).

Mörch, C. M. et al (2020) Protocol de Canadà: una llista de comprovació ètica per a l'ús de la IA en la prevenció del suïcidi i la salut mental. Artificial Intelligence In Medicine 108 (2020) 1019342. Disponible a: <https://doi.org/10.1016/j.artmed.2020.101934> (consultada el 16 d'octubre de 2023).

Muoio, D. (2021) El model de predicció de sepsis d'Epic, àmpliament utilitzat, es queda curt entre els pacients de Michigan Medicine. Fierce healthcare. Disponible a: <https://tinyurl.com/s8yak4bz> (consultada el 10 d'octubre 2023).

Nellis, S. (2018) Appel detecta problemes més greus en els seus proveïdors a mesura que amplia les seves auditories. Reuters. Disponible a: <https://www.reuters.com/article/us-apple-suppliers-idUSKCN1GK04G> (consultada el 11 d'octubre 2023).

Nguyen, B. Microsoft s'associa amb els sindicats per la formació en la IA abans de la creixent preocupació per la pèrdua de feina. Forbes. Disponible a: <https://tinyurl.com/5eufhfd4> (consultada el 15 de febrer de 2024).

Notopoulos, K. (2016) L'aplicació de cites que saben en secret que no t'agraden els nois d'altres races. Buzz Feed. News. Disponible a: <https://tinyurl.com/229nvhff> (consultada el 11 de gener de 2024).

Nova, S. & Shapiro I. (2014). Avaluació de les reformes presentades en l'informe sobre la responsabilitat dels proveïdors d'Appel. Economic policy institute. Disponible a: <https://www.epi.org/publication/assessing-reforms-portrayed-apples-supplier/> (consultada el 11 d'octubre 2023).

OCDE (2021) OECD Business and Finance Outlook 2021 : AI en els negocis financers. Disponible a: <https://tinyurl.com/36brbj93> (consultada el 23 de desembre de 2023).

OCDE (2022) Mesurant l'impacte ambiental de la computació i les aplicacions de IA. empremta de la IA. Disponible a <https://www.oecd.org/publications/measuring-the-environmental-impacts-of-artificial-intelligence-compute-and-applications-7babf571-en.htm> (consultada el 13 de desembre de 2023).

Olavsrud, T. (2023) 5 famosos analítics i catàstrofes d'IA. CIO. Disponible a: [9 famous analytics and AI disasters | CIO](#) (consultada el 20 de març de 2024).

One.com (s.d) Què és un filtre antispam i antivirus?. Disponible a: <https://www.one.com/es/correelectronico/que-es-un-filtro-antispam-y-antivirus> (consultada el 12 de març de 2024).

ONU (2023) La intel·ligència artificial requereix una governança basada en els drets humans. Disponible a: <https://news.un.org/es/story/2023/11/1526062> (consultada el 7 de desembre de 2023).

Parlament Europeu i Consell de la UE (2000) Carta de drets fonamentals de la UE, de 7 de desembre del 2000 (2000/C 364/01). Disponible a: <https://tinyurl.com/ynhfhmek> (consultada el 20 de setembre de 2023).

Parlament Europeu i Consell de la UE (2001) Directiva 2001/18/CE del Parlament Europeu i del Consell, de 12 de març de 2001, sobre l'alliberament intencional al medi ambient d'organismes modificats genèticament, per la qual es deroga la Directiva 90/220/CEE del Consell. Disponible a: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:125:0075:0097:EN:PDF> (consultada el 10 de novembre de 2023).

Parlament Europeu i Consell de la UE (2003) Reglament (CE) 1829/2003 del Parlament Europeu i del Consell, de 22 de setembre de 2003, sobre aliments i pinsos modificats genèticament. Disponible a: <https://eur-lex.europa.eu/eli/reg/2003/1829/oj> (consultada el 20 de maig de 2024).

Parlament Europeu i Consell de la UE (2003) Reglament (CE) 1830/2003 del Parlament Europeu i del Consell, de 22 de setembre de 2003, relatiu a la traçabilitat i l'etiquetatge dels organismes modificats genèticament i la traçabilitat dels aliments i pinsos produïts a partir d'organismes modificats genèticament i pel qual es modifica la Directiva 2001/18/CE. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003R1830> (consultada el 20 de maig de 2024).

Parlament Europeu i Consell de la UE (2003) Reglament (CE) núm. 1946/2003 del Parlament Europeu i del Consell, de 15 de juliol de 2003, sobre els moviments transfronterers d'organismes modificats genèticament. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32003R1946> (consultada el 20 de maig de 2024).

Parlament Europeu i Consell de la UE (2003) 641/2004/CE de la Comissió, de 6 d'abril de 2004, sobre les normes de desenvolupament del Reglament (CE) núm. 1829/2003 del Parlament Europeu i del Consell, pel que fa a la sol·licitud d'autorització de nous aliments i pinsos modificats genèticament, la notificació de productes existents i la presència accidental o tècnicament inevitable de material modificat genèticament l'avaluació de risc del qual hagi estat favorable. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003R1830> (consultada el 20 de maig de 2024).

Parlament Europeu i Consell de la UE (2009) Directiva 2009/41/CE del Parlament Europeu i del Consell, de 6 de maig de 2009, relatiu a la utilització confinada de microorganismes modificats genèticament. Disponible a: <https://tinyurl.com/y84usr3c> (consultada el 10 de novembre de 2023).

Parlament Europeu i Consell de la UE (2011) Reglament (CE) 1169/2011 del Parlament Europeu i del Consell, del 25 d'octubre, elaborat per la Comissió per a establir i harmonitzar els mètodes de mostreig i anàlisi per al control oficial de pinsos. Disponible a: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0018:0063:en:PDF> (consultada el 21 de maig de 2024).

Parlament Europeu i Consell de la UE (2011) Reglament d'execució (CE) 1137/2013 de la Comissió, de 13 de desembre, s'estableixen disposicions d'aplicació del Reglament (UE) n^o 1169/2011 del Parlament Europeu i del Consell relatiu a les indicacions del país d'origen o el lloc de procedència per a la carn fresca, refrigerada o congelada de porc, ovella, cabra i aus de corral. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013R1337> (consultada el 21 de maig de 2024).

Parlament Europeu i Consell de la UE (2016) Directiva 2016/2102/CE del Parlament Europeu i del Consell de 26 d'octubre de 2016 sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils dels organismes del sector públic. Disponible a: [DIRECTIVE \(EU\) 2016/ 2102 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 26 October 2016 - on the accessibility of the websites and mobile applications of public sector bodies \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L2102) (consultada l'11 de març de 2024).

Parlament Europeu i Consell de la UE (2016) Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, sobre la protecció de les persones físiques pel que fa al tractament de dades personals i sobre la lliure circulació d'aquestes dades, i per la qual es deroga la Directiva 95/46/EC (Reglament General de Protecció de Dades). Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504&qid=1713264943329> (consultada el 20 de març de 2023).

Parlament Europeu i Consell de la UE (2019) Directiva 2019/882, de 17 d'abril del 2019, sobre els requisits d'accessibilitat dels productes i serveis. Disponible a: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:-32019L0882> (consultada l'11 de març de 2024).

Parlament Europeu (2021) Un dret universal a un medi ambient saludable. Disponible a: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698846/EPRS_ATA\(2021\)698846_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698846/EPRS_ATA(2021)698846_EN.pdf) (consultada el 4 de desembre de 2023).

Parlament Europeu i Consell de la UE (2023) Llei d'Intel·ligència Artificial: acord sobre normes integrals per a una IA fiable. Disponible a: <https://tinyurl.com/mtun6ne6> (consultada el 9 de desembre de 2023).

Parlament Europeu (2023) Esmenes adoptades pel Parlament Europeu el 14 de juny de 2023 sobre la proposta de reglament del Parlament Europeu i del Consell per establir normes harmonitzades sobre la intel·ligència artificial (Llei d'Intel·ligència Artificial) i per modificar determinats actes legislatius de la Unió (COM (2021) 0206 – C9-0146/2021 – 2021/0106 (COD) (1). Disponible a: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html (consultada el 16 de juny de 2023).

Parlament Europeu (2024) Resolució legislativa del Parlament Europeu de 13 de març de 2024 sobre la proposta de Reglament del Parlament Europeu i del Consell pel qual s'estableixen normes harmonitzades sobre intel·ligència artificial (Llei d'Intel·ligència Artificial) i es modifiquen determinats actes legislatius de la Unió (COM (2021) 0206 – C9-0146/2021 – 2021/0106 (COD)). Disponible a: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html (consultada el 14 de març de 2024)

Pautaran, A. (2023). FQ: Tot el que cal saber sobre el RankBrain de Google el 2021. Disponible a: [Google's RankBrain Algorithm Complete Fact Sheet \(link-assistant.com\)](https://link-assistant.com/google-rankbrain-algorithm-complete-fact-sheet) (consultada el 15 de febrer de 2024).

Petropoulos, G. (2022) El costat fosc de la intel·ligència artificial: la manipulació del comportament humà. Bruegel. Disponible a: <https://www.bruegel.org/blog-post/dark-side-artificial-intelligence-manipulation-human-behaviour> (consultada el 12 de març de 2024).

Price, R.& Bastone, N. (2019). Google cancel·la el comitè que havia de regular l'ètica de la intel·ligència artificial. Business insider. Disponible a: <https://www.businessinsider.es/google-cancela-comite-regular-etica-intel·ligencia-artificial-400609> (consultada el 12 de març de 2024).

Puig, A. (2023) Les errades en la protecció de la privacitat de Ring va causar espionatge i assetjament a través de les càmeres de Seguretat de la llar. La comisió federal de comerç. Disponible a: <https://consumidor.ftc.gov/alertas-para-consumidores/2023/05/los-fallos-en-la-proteccion-de-la-privacidad-de-ring-causaron-espionaje-y-acoso-traves-de-camaras-de> (consultada el 11 de gener de 2024).

Quach, K. (2020). Estudiant nord-americà acusat després d'accedir i filtrar presumptament el codi d'IA dels superordinadors de Nvidia. The Register. Disponible a: https://www.theregister.com/AMP/2020/12/08/texas_compsci_phd_ai/ (consultada el 4 de març de 2024).

Universia (2022) Quina informació poden extreure les empreses gràcies al Big Data? Disponible a: <https://tinyurl.com/5axwavnu> (consultada el 20 de març de 2024).

Ramírez, L. (2023) Algoritme k-means: Què és i com funciona?. IEBS. Disponible a: <https://www.iebschool.com/blog/algoritmo-k-means-que-es-y-como-funciona-big-data/> (consultada el 15 de febrer de 2024).

Ren, Y. (2021) Reconeixement facial: Sistemes de seguretat. Ericsson. Disponible a: <https://www.ericsson.com/en/blog/2021/5/facial-recognition-security-system> (consultada el 15 de febrer de 2024).

Resilinc. (s.d). Quadre de puntuació de risc de proveïdors. Disponible a: <https://www.resilinc.com/supplier-risk-scorecard/> (consultada el 20 de març de 2024).

Responsible AI. Disponible a: <https://www.responsible.ai/> (consultada el 4 de març de 2024).

Roekens, N. (2014) La Convenció en IA i Drets Humans dels quals ningú parla. Disponible a: <https://www.linkedin.com/pulse/convention-ai-human-rights-one-talks-nele-roekens-6zzif> (consultada el 16 de gener de 2024).

Rossi, F. & Treviño, N. & Ahmed, A. (2022) Ètica quotidiana per a la IA. IBM. Disponible a: <https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf> (consultada el 4 de març de 2024).

Satariano, A. (2023) Meta s'enfronta a una possible multa record de la UE per la privadesa de dades de Facebook. The New York Times. Disponible a: <https://tinyurl.com/3e638pj7> (consultada el 12 de març de 2024).

Scope. Disponible a: <https://www.scope.org.uk/> (consultada el 11 de gener de 2024).

Servei d'Acció Exterior de la UE (2023) Important advancements from Strasbourg and Brussels on first binding rules for Artificial Intelligence. Disponible a: <https://tinyurl.com/yhe294fw> (consultada el 19 de desembre de 2023).

Shung, D.L. & Byrne, M.F. (2020) Com la intel·ligència artificial impactarà a les colonoscopies i criatge colorectal. PubMed Central. Disponible a: <https://pubmed.ncbi.nlm.nih.gov/32439090/> (consultada el 12 de març de 2024).

Siddiqui, F. & Merrill, G.B. (2023) 17 accidents mortals i 736 accidents: El peatge impactant del pilot automàtic de Tesla. The Washington post. Disponible a: <https://tinyurl.com/2rvn5jaa> (consultada el 11 d'octubre 2023).

Silicon Canals (2023) AI amb seu a Londres: startup deep render assegura finançament. Siliconcanals. Disponible a: <https://siliconcanals.com/es/noticias/AI-con-sede-en-Londres-startup-deep-render-secures-funding/> (consultada el 20 de març de 2024).

Society for Computers & Law (SCL) AI Group – AI Clauses Projecte (octubre 2023). Artificial Intelligence Contractual Clauses. (Informe guia per a detallar la responsabilitat de proveïdors i clients en les relacions contractuals en el marc de sistemes d'IA) Disponible a: <https://www.scl.org/news/13004-society-for-computers-and-law-ai-group-launches-artificial-intelligence-contractual-clauses> (consultada el: 17 d'octubre 2023).

Taylor, J. (2023) *ChatGPT*: El fabricant d'Open AI publica una eina “no del tot fiable” per a detectar continguts generats per la IA. The Guardian. Disponible a: <https://tinyurl.com/mvkzmabs> (consultada l'11 d'octubre 2023).

TitanHQ (s.d.) Filtre antispam per als e-mails entrants. Disponible a: <https://www.titanhq.fr/filtre-emails-entrants/> (consultada el 4 de març de 2024).

Theodorou, A. & Dignum, V. (2020). Cap a una governança ètica i sociojurídica de la IA. Nature Machine Intelligence, 2 (1), 10–12. <https://doi.org/10.1038/s42256-019-0136-y> (consultada el 16 de gener de 2024).

Toolify.ai. La importància del monitoreig i l'explicabilitat dels sistemes d'IA. (toolify.ai) Disponible a: <https://www.toolify.ai/es/ai-news-es/la-importancia-del-monitoreo-y-la-explicabilidad-en-los-sistemas-de-ia-2586738> (consultada el 11 de gener de 2024).

Tribunal Europeu de Drets Humans. (1950). Convenció per a la protecció dels drets humans i de les llibertats fonamentals. Disponible a: <https://tinyurl.com/ytwhsdma> (consultada l'11 d'octubre 2023).

Turner, N. (2024) Emmagatzematge al núvol vs. Disc dur: Què és millor per a la seguretat de les dades? Internxt. Disponible a: <https://blog.internxt.com/cloud-storage-vs-hard-disk/> (consultada el 11 de gener de 2024).

Tyson, M. (2023). Deep render dice que su tecnología de compresión de vídeo con IA «salvará Internet». Tom'sHardware. Disponible a: <https://www.tomshardware.com/news/deep-render-says-its-ai-video-compression-tech-will-save-the-internet> (consultada el 12 de març de 2024).

UNESCO (2021) Esborrany sobre la recomanació de la ètica d'IA. SHS/IGM-AIETHICS/2021/JUN/3Rev.2. Disponible a: <https://tinyurl.com/2rp79ba3> (consultada el 29 de gener de 2024).

International Telecommunication Union (2022) United Nations Activities on Artificial Intelligence (AI). Disponible a: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2022-PDF-E.pdf (consultada el 4 de març de 2024).

Universidad de Oviedo. (s.d.) L'algoritme k-means aplicat per a la classificació i processament d'imatges. Disponible a: <https://tinyurl.com/m2mhy72> (consultada el 11 de gener de 2024).

Veil.AI (s/d) Permetre l'ús segur de dades sensibles amb anonimització d'última generació. Disponible a: <https://veil.ai/> (consultada el 15 de febrer de 2024).

Verma, P. (2023). Estafa de veu per la IA. The Washington Post. Disponible a: <https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/> (consultada el 4 de març de 2024).

Vincent, J. Getty Images ha demandat als creadors de les eines d'IA «stable diffusion» per a copiar els seus continguts. The verge. Disponible a: <https://tinyurl.com/49tuty78> (consultada el 20 de març de 2024).

Villavicencio, K. (2012) Google controla el 90% de les cerques. La Nación. Disponible a: <https://www.lanacion.com.ar/economia/google-controla-el-90-de-las-busquedas-nid1504500/> (consultada el 4 de març de 2024).

Wakefield, J. (2018) La IA suposa menys riscos per als llocs de feina dels que temíem. BBC. Disponible a: <https://www.bbc.com/news/technology-44561838> (consultada el 20 de març de 2024).

Weise, K. (2024) Amazon presenta llur resultats, superant les expectatives dels analítics. The New York Times. Disponible a: <https://www.nytimes.com/2024/02/01/technology/amazon-earnings.html> (consultada el 12 de gener de 2024).

Wes, D. (2023) Tesla sota investigació a Califòrnia sobre qüestions de seguretat del pilot automàtic i la publicitat enganyosa. They verge. Disponible a: <https://tinyurl.com/yc6z9wvm> (consultada l'11 d'octubre 2023).

Wiggers, K. (2020). Els investigadors troben indicis de biaix racial, de gènere i socioeconòmic en els classificadors de radiografies de tòrax. VentureBeat. Disponible a: <https://tinyurl.com/5n6atcuH> (consultada el 12 de març de 2024).

Wilkins, A. (2023) Detectar amb fiabilitat el text generat amb la IA es matemàticament impossible. New scientist. Disponible a: <https://www.newscientist.com/article/2366824-reliably-detecting-ai-generated-text-is-mathematically-impossible/> (consultada l'11 d'octubre 2023).

Yong, E. The Atlantic. (2018) Com els ordinadors preveuen el crim i que pots afectar al seu futur. Disponible a: [A Popular Algorithm Is No Better at Predicting Crimes Than Random People - The Atlantic](https://www.theatlantic.com/technology/archive/2018/07/a-popular-algorithm-is-no-better-at-predicting-crimes-than-random-people/) (consultada el 12 de març de 2024).

Zenner, K. (2024) La llei d'IA: tots els documents disponibles públicament en maig de 2024. Digitizing Europe. Disponible a: <https://www.kaizenner.eu/post/aiact-part3> (consultada el 3 de juny de 2024).

Ziady, H. (2023) La UE imposa a Meta una multa rècord de 1.300 mil·lions de dòlars per la privacitat de llurs dades. Disponible a: <https://tinyurl.com/2fan7k4p> (consultada el 4 de març de 2024).

ANNEX I: RESUM DE LES PREGUNTES DEL QÜESTIONARI

Principi 1: Transparència i explicabilitat

1.1. Anàlisi preliminar de l'ús del sistema

Nº	Pregunta
1.1.1	El procés de generació de resultats del vostre sistema d'IA està ben documentat i és reproducible per si cal descobrir problemes en el futur?
1.1.2	Coneixeu amb precisió per a què s'utilitza el vostre sistema d'IA?
1.1.3	Sabeu si el vostre sistema d'IA utilitza el model més simple i intel·ligible en favor de la transparència?
1.1.4	El vostre sistema d'IA realitza registres automàtics del seu funcionament de manera continua?
1.1.5	Heu facilitat o posat a disposició informació sobre la identitat i les dades de contacte de la persona proveïdora (o les seves representants) ?
1.1.6	Heu tingut en compte les capacitats, competències i l'alfabetització en matèria d'IA de totes les possibles persones usuàries, incloent-hi grups vulnerables, amb problemes d'accessibilitat i/o necessitats especials?

1.2. Explicabilitat

Nº	Pregunta
1.2.1	El procés de desenvolupament del vostre sistema i les persones que hi han estat implicades estan documentats i són públics?
1.2.2	La informació tècnica necessària per a l'ús del vostre sistema (suport físic, versions de software, actualitzacions, etc) està documentada i és pública?
1.2.3	Proporcioneu informació i instruccions concises, clares i accessibles, sobre el funcionament i manteniment del vostre sistema?
1.2.4	Es possible identificar si el contingut que genera el vostre sistema ha estat creat per una IA (per exemple amb una etiqueta o segell) ?
1.2.5	Sou capaçs d'entendre i explicar com el vostre sistema d'IA arriba a un resultat determinat ?
1.2.6	Sou coneixedors de les possibles limitacions del vostre sistema d'IA i les heu comunicat a tots els actors implicats, incloent-hi les persones usuàries?
1.2.7	Heu donat informació a les persones que utilitzen el vostre sistema d'IA sobre l'intercanvi de dades, els resultats previstos i com exercir els seus drets?
1.2.8	Consideredu que heu establert un nivell de transparència i explicabilitat que no posa en risc la privacitat de les persones?

- 1.2.9 **Considereu que heu establert un nivell de transparència i explicabilitat que no posa en risc la seguretat del vostre sistema d'IA?**

1.3. Traçabilitat i representativitat

Nº	Pregunta
1.3.1	Heu assegurat que les dades utilitzades pel vostre sistema d'IA son suficientment representatives i adequades?
1.3.2	Heu documentat els tipus de dades, la seva procedència i els canvis efectuats en cada fase del cicle de vida del vostre sistema d'IA?
1.3.3	Per tal de protegir les dades de persones menors, heu tingut en compte salvaguardes com la traçabilitat de les dades per verificar l'edat de les persones?
1.3.4	En el cas d'utilitzar dades demogràfiques, heu validat la seva representativitat tenint en compte el context més proper a través de la informació mostral o poblacional d'una organització d'estadística?
1.3.5	Conserveu els registres dels arxius que genera el vostre sistema IA com a mínim sis mesos?

1.4. Protocols de comunicació

Nº	Pregunta
1.4.1	Heu establert eines de comunicació que permetin a les persones usuàries del vostre sistema d'IA realitzar comentaris sobre el seu funcionament?
1.4.2	Heu consultat a altres organitzacions que hagin dissenyat i/o implementat un sistema d'IA similar per a conèixer antecedents i experiències?
1.4.3	Heu establert una política de participació de diferents grups d'interès (stakeholders), incloent-hi les persones usuàries finals i/o receptors del vostre sistema d'IA?
1.4.4	En cas d'incident greu o error en el funcionament del vostre sistema d'IA heu previst un sistema de notificació?

Principi 2: Justícia i equitat

2.1. Inclusió i diversitat

Nº	Pregunta
2.1.1	Heu establert mesures d'inclusió i equitat com provar els resultats del vostre sistema d'IA per a diferents grups afectats?
2.1.2	Us heu assegurat que el vostre sistema d'IA no utilitza variables o "proxies" que poden ser injustament discriminatòries?

- 2.1.3 Heu avaluat si el vostre sistema d'IA s'adapta a un ampli espectre de preferències i habilitats individuals, incloent-hi les persones usuàries que requereixen tecnologies d'assistència?
- 2.1.4 Dins del vostre equip de treball, s'inclouen dones que garanteixin la diversitat d'opinions dins del procés de disseny i implementació del sistema d'IA?
- 2.1.5 Dins del vostre equip de treball s'inclouen persones de diversos orígens o cultures que garanteixin la diversitat d'opinions dins del procés de disseny i implementació del sistema d'IA?
- 2.1.6 Dins del vostre equip de treball s'inclouen persones de diferents disciplines de coneixement més enllà de la informàtica i l'enginyeria?
- 2.1.7 La vostra organització promou i fomenta una cultura organitzativa on la diversitat, l'equitat i la inclusió són elements prioritaris?
- 2.1.8 La vostra organització té coneixement o forma part d'associacions o entitats que fomenten la DEI per avançar en polítiques d'IA responsable?
- 2.1.9 El vostre sistema d'IA compta amb mesures per a augmentar l'accessibilitat o recolzar-ne l'ús per a persones vulnerables?
- 2.1.10 Heu verificat si el vostre sistema d'IA pot influenciar negativament en processos democràtics i de presa de decisions a les institucions públiques?

2.2. Identificació i mitigació de biaixos

Nº	Pregunta
2.2.1	Heu implementat mesures que permetin mitigar els possibles biaixos estadístics en el vostre sistema d'IA, siguin originats en les dades d'entrenament o a posteriori?
2.2.2	Heu establert mecanismes que permetin mitigar els possibles biaixos de classificació en el vostre sistema d'IA, siguin per categories canviant o inadequades segons el context sociocultural?
2.2.3	Heu adoptat mesures que permetin mitigar possibles biaixos cognitius en la fase de disseny o implementació del vostre sistema d'IA (e.x. el biaix de confirmació) ?
2.2.4	Heu realitzat una avaluació d'impacte dels possibles biaixos del vostre sistema d'IA per saber si podria reforçar discriminacions, estereotips o prejudicis envers persones vulnerables (e.x. persones amb discapacitat, minories ètniques o individus d'edat avançada) ?
2.2.5	El vostre sistema d'IA per a la identificació biomètrica remota compleix els estàndards de classificació d'alt risc que tracten els biaixos relacionats amb l'edat, l'ètnia, la raça, el sexe o les discapacitats?

- 2.2.6 **El vostre sistema d'IA incorpora mesures per mitigar els biaixos del conjunt de dades, especialment aquells que podrien perpetuar la discriminació o afectar la salut i la seguretat, alhora que s'adhereixen a les pràctiques de preservació de la privadesa d'acord amb els requisits de la legislació de la Unió?**
- 2.2.7 **Les mesures de detecció i correcció de biaix al vostre sistema d'IA, inclòs el tractament de categories especials de dades personals, compleixen la normativa que garanteix la protecció de dades? (Reglament (UE) 2016/679, Directiva (UE) 2016/ 680, i el Reglament (UE) 2018/1725)**
- 2.2.8 **El vostre sistema d'IA incorpora mecanismes de seguretat en cas d'anomalies o accions fora dels límits predeterminats, mitigant així els riscos per a la seguretat i els drets fonamentals?"**
- 2.2.9 **S'adverteix a les persones usuàries del vostre sistema d'IA d'alt risc contra el biaix d'automatització, especialment quan el sistema proporciona informació o recomanacions per a les decisions preses per persones?**
- 2.2.10 **Heu implementat mesures per abordar i mitigar el risc de sortides esbiaixades i bucles de retroalimentació, especialment per als sistemes que continuen aprenent després del desplegament?**
- 2.2.11 **Podeu proporcionar informació detallada sobre les dades i els recursos computacionals utilitzats per a la formació, les proves i la validació del vostre sistema d'IA, inclosa la procedència de les dades, les metodologies de curació i les mesures adoptades per detectar la inadequació i els biaixos de les dades**

Principi 3: Seguretat i no maleficència

3.1. Funcionament del sistema

Nº	Pregunta
3.1.1	Les persones que han dissenyat el vostre sistema d'IA han proporcionat orientació sobre com interpretar i respondre a les mètriques generades pel propi sistema?
3.1.2	Heu informat sobre el nivell de precisió i seguretat del vostre sistema d'IA?
3.1.3	Heu informat sobre com les accions de les persones usuàries poden influir en el rendiment del sistema?
3.1.4	Heu establert mecanismes de supervisió i control (intern o extern) per assegurar-vos que el vostre sistema d'IA funciona tal i com es pretén?
3.1.5	Coneixeu els possibles comportaments i escenaris que el vostre sistema d'IA mai hauria de transgredir per garantir la seguretat i preservar la no maleficència?

3.2. Traçabilitat per a la gestió del risc

Nº	Pregunta
3.2.1	El vostre sistema ha passat per una avaluació sobre els seus possibles impactes sobre la salut, la seguretat i els drets de les persones?
3.2.2	Heu establert o adoptat un protocol general de traçabilitat de les dades per a la gestió del risc del vostre sistema d'IA?
3.2.3	El vostre sistema d'IA compta amb mitjans per identificar i avaluar els riscos sorgits del seu ús?
3.2.4	El vostre sistema d'IA compta amb mitjans per identificar i avaluar els riscos sorgits amb les dades recollides després d'entrar en funcionament?
3.2.5	El vostre sistema d'IA compta amb mitjans que permeten l'adopció de mesures apropiades i específiques per eliminar o mitigar els riscos detectats?
3.2.6	Heu informat sobre els riscos residuals (aquells que no han pogut ser eliminats o corregits després d'haver pres totes les mesures possibles) ?
3.2.7	Heu avaluat els possibles riscos o danys que provocaria que el vostre sistema d'IA fes prediccions inexactes en els escenaris previstos?
3.2.8	Heu considerat els possibles riscos o danys que provocaria si el vostre sistema d'IA s'utilitzés per a altres usos més enllà dels previstos?
3.2.9	Heu avaluat que, en cap cas, les dades que recolliu, genereu o utilitzeu per al funcionament del vostre sistema d'IA no poden utilitzar-se per discriminar persones de forma negativa?

3.3. Mecanismes de seguretat

Nº	Preguntes
3.3.1	El vostre sistema està dotat de mesures per garantir la resistència davant d'errors sorgits de la seva interacció amb altres sistemes?
3.3.2	El vostre sistema compta amb mesures de mitigació de possibles biaixos o intents de manipulació derivats de les dades d'entrada durant el seu funcionament?
3.3.3	Poden les persones usuàries controlar fins a quin punt estan exposats i revocar el consentiment en qualsevol moment sense que això comprometi el rendiment del sistema d'IA?
3.3.4	Heu establert mesures per examinar la precisió del vostre sistema d'IA de forma contínua per conèixer si aquest està fent una quantitat inacceptable de prediccions inexactes?

3.4. Protecció enfront d'atacs

Nº	Preguntes
3.4.1	Heu avaluat els riscos i la vulnerabilitat del vostre sistema d'IA per garantir la seva seguretat, integritat i resiliència davant de diferents formes d'atac?
3.4.2	Heu portat a terme una avaluació de protecció que garanteixi que els conjunts de dades que utilitza el vostre sistema d'IA no han estat prèviament compromesos o piratejats?

Principi 4: Responsabilitat i retiment de comptes

4.1. Control

Nº	Preguntes
4.1.1	Us heu assegurat que les persones involucrades en el control tenen una comprensió adequada de la presa de decisions que efectua el vostre sistema d'IA?
4.1.2	Heu definit clarament els límits del nivell de control o participació humana dins del vostre sistema d'IA?
4.1.3	El vostre sistema d'IA compta amb una eina que permeti a les persones encarregades del seu control intervenir en les decisions d'aquest?
4.1.4	És possible modificar, eliminar o revertir les decisions preses pel vostre sistema d'IA quan aquestes no hagin resultat suficientment adequades o exactes per tal d'eliminar o mitigar un efecte perjudicial?
4.1.5	La persona encarregada de controlar les decisions preses pel vostre sistema d'IA compta amb la capacitat necessària per a exercir aquestes funcions?
4.1.6	La documentació del vostre sistema d'IA proporciona detalls complets sobre la seva supervisió i mesures de supervisió humana per garantir un desplegament informat i segur?

4.2. Retiment de comptes

Nº	Preguntes
4.2.1	Heu determinat qui és legalment responsable de les accions i/o decisions que pren el vostre sistema d'IA durant tot el seu cicle de vida?
4.2.2	Heu avaluat de quina manera el vostre sistema d'IA influeix en els processos de presa de decisions de la vostra organització?

4.2.3 **Heu establert mecanismes de revisió periòdica sobre responsabilitat i retiment de comptes amb els diferents agents involucrats en el desenvolupament i ús del vostre sistema d'IA?**

4.2.4 **Proporcioneu informació sobre si el sistema compta amb mesures de vigilància humana i qui és la persona responsable de les mateixes?**

4.3. Figures de protecció

Nº	Preguntes
----	-----------

4.3.1	Heu pres mesures per facilitar la demostració del compliment de la legislació vigent incloent-hi, per exemple, la Llei de Protecció de Dades (GDPR) ?
-------	--

4.3.2	Heu determinat una o més figures de protecció envers la persona usuària del vostre sistema d'IA com per exemple, la figura del Síndic de Greuges?
-------	--

4.3.3	Heu establert formes de reparació o compensació en cas que ocorri algun mal o impacte advers de responsabilitat a través de pòlisses d'assegurances, mitjans monetaris adequats i/o altres formes de compensació?
-------	--

4.4. Capacitats de la IA

Nº	Preguntes
----	-----------

4.4.1	Considerem que esteu exagerant el que pot fer el vostre sistema d'IA o fins i tot afirmeu que pot fer alguna cosa més enllà de la capacitat actual de qualsevol IA?
-------	--

4.4.2	La vostra organització promet que un sistema d'IA fa alguna cosa millor que un producte que no sigui IA i ho pot demostrar compartint dades i codi? Recordeu que en el cas que siguin impossibles d'obtenir no es pot fer aquesta afirmació.
-------	---

4.5. Promoció d'una cultura de l'ètica i responsabilitat relacionada amb la IA

Nº	Preguntes
----	-----------

4.5.1	La vostra organització té un codi ètic per l'ús responsable de la IA?
-------	--

4.5.2	La vostra organització incentiva al seu personal a promoure una IA responsable a través d'un/a responsable d'ètica de la IA en la mateixa organització?
-------	--

4.5.3 **Considereu que la IA responsable és una prioritat de la vostra organització i això es reflecteix en els objectius del sistema d'IA així com en les revisions del seu rendiment?**

4.5.4 **Us heu assegurat que el vostre sistema d'IA, quan s'utilitza per decidir sobre l'elegibilitat de serveis públics o privats, aborda de manera responsable les implicacions per als drets i el benestar de les persones?**

Principi 5: Privacitat

5.1. Protecció de la privacitat

Nº	Preguntes
5.1.1	Heu establert mecanismes de protecció de dades per tal que les dades de caràcter personal siguin tractades amb el grau de protecció legalment requerit i així evitar-ne el mal ús, alteració, pèrdua o sostracció per part de tercers?
5.1.2	Heu establert mecanismes de protecció de dades per tal que les dades de caràcter personal subministrades per la persona interessada no siguin venudes, llogades ni cedides, sense el seu consentiment?
5.1.3	Heu establert processos per mantenir o millorar la privacitat i la protecció de dades al llarg del cicle de vida del vostre sistema d'IA (com el xifratge, l'anonimització o l'agregació) ?
5.1.4	Heu establert un mecanisme a través del qual una persona pot sol·licitar que la seva informació personal sigui eliminada?
5.1.5	Heu establert un protocol per obtenir el consentiment abans d'iniciar qualsevol processament o anàlisi a través del vostre sistema d'IA?
5.1.6	La informació sobre el consentiment i la seva revocació és comprensible i accessible per totes les persones usuàries, incloent aquells que pertanyen a grups vulnerables, persones amb problemes d'accessibilitat o necessitats especials?
5.1.7	L'acceptació de les condicions en el vostre sistema d'IA implica la pèrdua de la privacitat de la persona usuària?
5.1.8	El vostre sistema d'IA incorpora mesures per protegir la privadesa i prevenir la discriminació contra grups vulnerables?
5.1.9	Us heu assegurat que el vostre sistema d'IA utilitza tècniques de preservació de la privadesa durant el seu desenvolupament?
5.1.10	Feu servir tècniques d'anonimat i xifratge per garantir la privadesa i la protecció de les dades personals en les operacions del vostre sistema d'IA (com el xifratge, l'anonimització o l'agregació) ?
5.1.11	El disseny i el desplegament del vostre sistema d'IA garanteix l'accés igualitari i la no discriminació per a les persones amb discapacitat alhora que respecta la seva privadesa i dignitat?

5.2. Governança de dades

Nº	Preguntes
5.2.1	Heu establert un registre de la informació d'accés a les dades (personals o no) per identificar clarament quan, qui i amb quin propòsit s'ha accedit a les dades?
5.2.2	Us heu assegurat que les persones que realitzen el processament i gestió de dades compten amb les competències necessàries i es mantenen al dia amb els nous desenvolupament per a comprendre i dur a terme la política de protecció de dades?
5.2.3	Heu establert els procediments per assegurar que els conjunts de dades siguin els adients i rellevants pel correcte rendiment i resultat previst del model?
5.2.4	Heu documentat el procés de recopilació i preparació de les dades pel vostre sistema d'IA?
5.2.5	El conjunt de dades recopilades per entrenar el vostre sistema són adequades pel context en el qual serà utilitzat (per exemple, les dades són representatives del territori on s'utilitza el sistema) ?
5.2.6	El vostre sistema d'IA està dissenyat per adherir-se als principis de minimització de dades i protecció de dades des del disseny i per defecte, tal com exigeixen les Lleis de Protecció de Dades?
5.2.7	Heu implementat tecnologies que permeten entrenar el vostre sistema d'IA sense necessitat de transmetre o copiar dades en brut o estructurades, millorant així la privadesa de les dades?
5.2.8	El vostre sistema d'IA limita la reutilització de dades personals sensibles i utilitza mesures avançades de seguretat i privadesa com la pseudònimització?

Principi 6: Autonomia

6.1. Impacte en les capacitats de les persones usuàries

Nº	Preguntes
6.1.1	Heu establert un procés d'avaluació del vostre sistema d'IA per garantir que en cap cas disminueix el nombre d'eleccions possibles, ni tampoc l'obliga o força a prendre unes determinades decisions?
6.1.2	Podeu assegurar que el vostre sistema d'IA, durant cap fase del seu cicle de vida, restringeix l'abast de les opcions d'estil de vida, creences, opinions, expressions o experiències personals?
6.1.3	Heu establert un protocol de comprovació sobre el vostre sistema d'IA que permeti certificar que ajuda les persones a prendre decisions millors i més informades d'acord amb els seus objectius?

- 6.1.4 **Heu pres mesures per garantir que les persones que interactuen amb el vostre sistema siguin conscients que es tracta d'una IA?**
- 6.1.5 **Heu establert els mecanismes per assegurar que totes les persones usuàries finals del sistema d'IA tenen prou capacitat i informació per a ser-ho, incloent-hi les persones amb problemes d'accessibilitat o que es troben en risc d'exclusió?**
- 6.1.6 **El vostre sistema d'IA evita l'ús de tècniques manipulatives o subliminals que podrien perjudicar l'autonomia, la presa de decisions o les eleccions lliures d'un individu?**
- 6.1.7 **El vostre sistema d'IA pot adaptar el seu nivell d'autonomia en funció de les preferències i requisits específics de la persona usuària?**

6.2. Percepció del sistema

Nº	Preguntes
----	-----------

- | | |
|-------|--|
| 6.2.1 | Heu avaluat si el vostre sistema d'IA encoratja als seus usuaris a desenvolupar una inclinació, simpatia o empatia que pugui portar als usuaris a sobreestimar les capacitats del mateix sistema? |
| 6.2.2 | Heu establert mesures per tal que, en cap cas, les operacions del vostre sistema d'IA puguin veure's com a opaques, enganyoses o manipuladores per a les persones usuàries? |
| 6.2.3 | El vostre sistema d'IA manté un nivell de supervisió humana per gestionar la seva autonomia i adaptabilitat, garantint un funcionament segur i controlat després del desplegament? |
| 6.2.4 | El vostre sistema d'IA té mecanismes per garantir que el seu grau d'autonomia està limitat per evitar comportaments no desitjats o d'alt risc? |
| 6.2.5 | Disposeu de mecanismes per garantir que l'autonomia del vostre sistema d'IA es mantingui en línia amb els objectius previstos i els requisits de seguretat? |
| 6.2.6 | Heu avaluat i mitigat els riscos relacionats amb les capacitats i el grau d'autonomia del vostre sistema d'IA? |
| 6.2.7 | El vostre model d'IA se sotmet a avaluacions de referència, especialment avaluant factors com la seva adaptabilitat a noves tasques i autonomia? |
| 6.2.8 | El vostre sistema d'IA, ja sigui autònom o com a part d'un producte, pot adaptar-se i aprendre del seu entorn sense comprometre la seguretat i els estàndards ètics? |

Principi 7: Sostenibilitat

7.1. Desenvolupament sostenible

Nº	Preguntes
7.1.1	Considereu que el vostre sistema d'IA té un impacte positiu en els drets laborals i/o en la qualitat del treball de les persones?
7.1.2	Considereu que el vostre sistema d'IA millora la qualitat de vida dels seus usuaris a nivell individual i vetlla pel desenvolupament sostenible a nivell col·lectiu?
7.1.3	Heu tingut en compte l'accés social, incloent-hi la bretxa digital, en l'ús i implantació del vostre sistema d'IA?
7.1.4	Heu abordat els punts cecs de l'anàlisi mitjançant la participació amb les parts interessades rellevants, per exemple comprovant les hipòtesis i discutint les implicacions del vostre sistema d'IA amb les comunitats afectades?
7.1.5	Us assegureu que existeixi una compensació justa i un tracte ètic a les persones implicades en l'etiquetatge de dades dels vostres sistemes d'IA?
7.1.6	Implementeu mesures per abordar problemes de drets d'autor i drets de propietat intel·lectual quan feu servir conjunts de dades externs en el vostre procés de desenvolupament d'IA?
7.1.7	Col·laboreu activament amb organitzacions laborals o sindicats per mitigar el possible desplaçament laboral causat per l'adopció de tecnologies d'IA a través de la requalificació de les persones treballadores afectades?

7.2. Impacte mediambiental

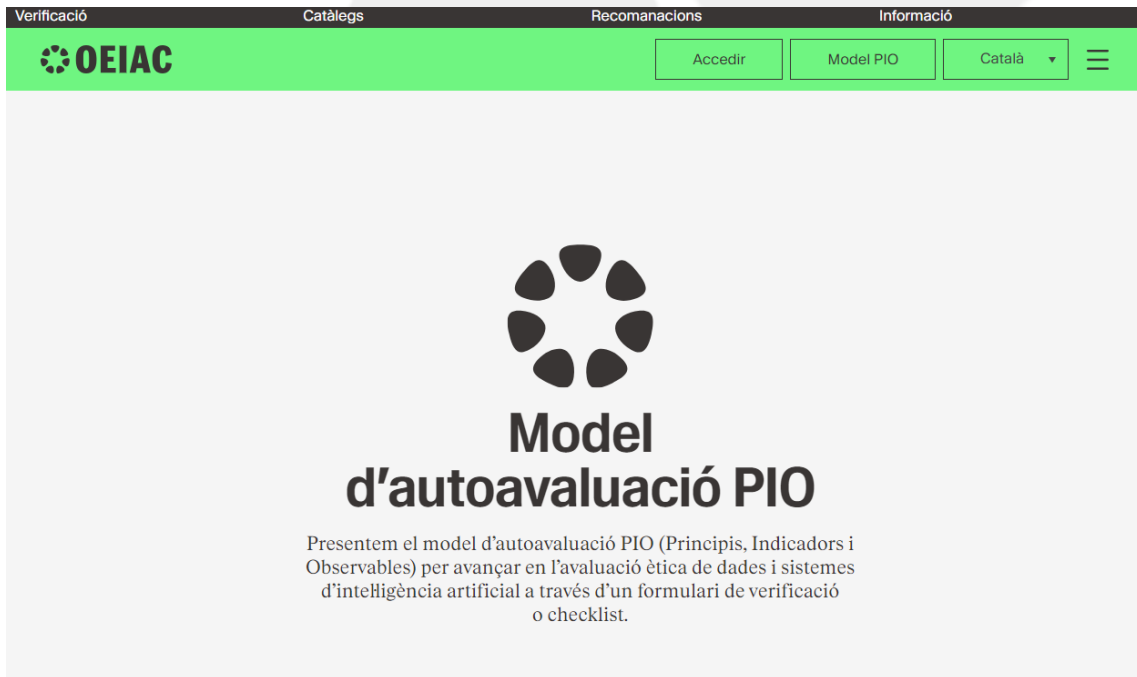
Nº	Preguntes
7.2.1	El vostre sistema d'IA és capaç d'enregistrar el seu consum d'energia i impacte ambiental durant tot el seu cicle de vida?
7.2.2	Heu avaluat l'eficiència energètica del vostre sistema d'IA tenint en compte el seu cicle de vida?
7.2.3	Heu establert mesures per incrementar l'eficiència energètica del vostre sistema d'IA a través de la supervisió que, per naturalesa, és més eficient amb les dades?
7.2.4	Heu establert mesures per incrementar l'eficiència energètica del vostre sistema d'IA a través de la minimització de dades o de l'ús de dades sintètiques?
7.2.5	Heu establert mesures per incrementar l'eficiència energètica del vostre sistema d'IA transferint coneixement de dades riques a dominis de dades pobres?

- 7.2.6 **Incorporeu una programació eficient energèticament i pràctiques de disseny sostenible als vostres sistemes d'IA, especialment quan tracteu amb el processament de dades a gran escala?**
- 7.2.7 **Heu implementat estratègies per reduir la petjada ambiental dels vostres sistemes d'IA, especialment quan manegeu conjunts de dades extensos?**
- 7.2.8 **Heu explorat l'ús de fonts d'energia renovables i pràctiques d'informàtica verda en el desplegament i l'operació dels teus sistemes d'IA per millorar la sostenibilitat?**
- 7.2.9 **Col·laboreu amb organitzacions i iniciatives enfocades a promoure pràctiques d'IA sostenibles per reduir l'impacte ambiental de les tecnologies d'IA?**

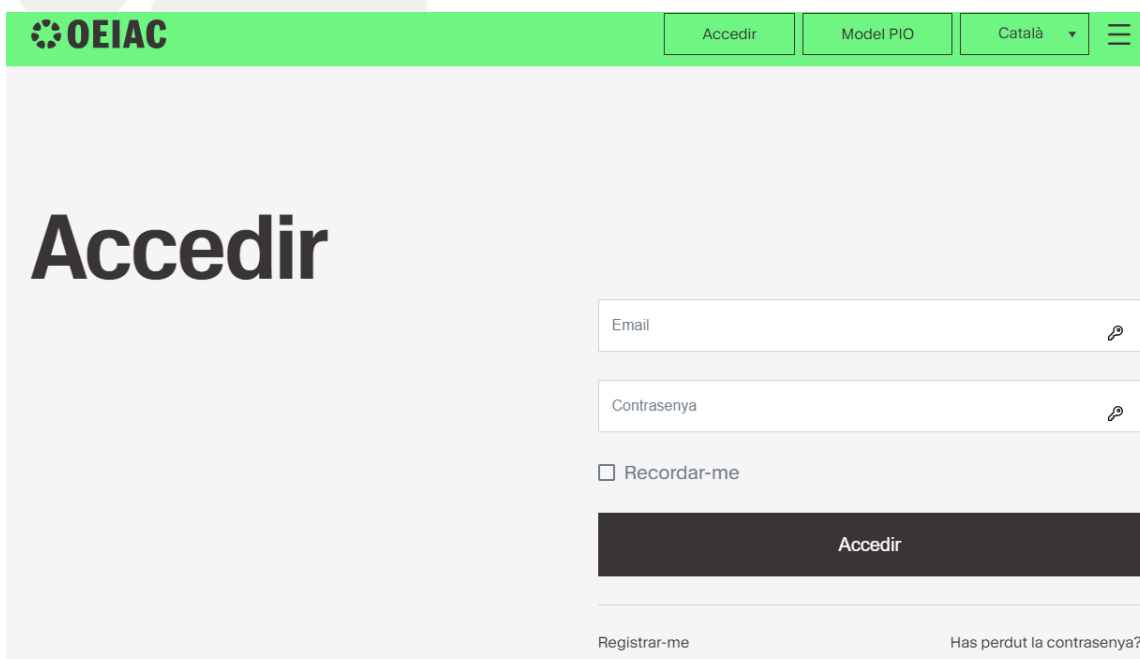
ANNEX II: NAVEGACIÓ DE LA WEB DEL MODEL PIO OBLIGACIONS I DRETS.

En aquest apartat us indicarem com navegar per la nostra nova [pàgina web](#) mitjançant imatges:

1- Pàgina d'inici:



2- Pàgina d'accés amb el vostre usuari:



3- Menú d'opcions:



4- Pestanya d'autoavaluació:

Hi trobareu tres opcions: La preavaluació, l'avaluació i els models sectorials.

Preavaluació

En aquest apartat podeu realitzar una preavaluació del vostre sistema d'IA en funció d'una aproximació de risc inicial que està basada en la legislació europea sobre intel·ligència artificial (AI Act). En aquesta es determinen diferents obligacions tenint en compte una aproximació de risc (que significa la major o menor probabilitat de que ocorri un dany i la gravetat d'aquest dany) segons quatre categories:


- Risc inacceptable**
Aquest fa referència a un conjunt molt limitat d'usos que són especialment nocius de la IA i que contravenen els valors de la UE ja que violen els drets fonamentals i, per tant, estan prohibits.
- Risc alt**
Aquest fa referència a un nombre limitat de sistemes d'IA que poden generar un impacte advers en la seguretat de les persones o els seus drets fonamentals segons la Carta dels Drets Fonamentals de la UE i, per tant, es consideren d'alt risc.
- Risc limitat**
Aquest fa referència als riscos associats a la falta de transparència en l'ús de la IA i, per tant, a la necessitat d'obligacions específiques de transparència per garantir que els humans estiguin informats quan sigui necessari, fomentant la confiança.
- Risc mínim**
Aquest fa referència a tots els altres sistemes d'IA que es poden desenvolupar i utilitzar d'acord amb la legislació vigent sense obligacions legals addicionals. Voluntàriament, els promotores d'aquests sistemes poden optar per aplicar principis ètics com els del Model PIO.

Establiment de risc inacceptable o usos prohibits

La legislació europea sobre intel·ligència artificial contempla en el seu article 5 un conjunt de pràctiques considerades de risc inacceptable perquè incideixen en els drets fonamentals i la seguretat humana de manera tan greu que el seu ús no pot ser permès. Per aquest motiu, qualsevol sistema d'IA que coincideixi amb alguna d'aquestes pràctiques no podrà ser comercialitzat, desenvolupat ni utilitzat dins del territori de la UE.

A continuació trobareu un llistat dels usos inacceptables. Si algun d'ells s'aplica al vostre sistema, no és necessari que completeu les preguntes del Model, ja que aquest ha estat pensat per avaluar sistemes que podran ser efectivament utilitzats d'acord amb la legislació.

Usos prohibits



Aquesta taula conté les pràctiques considerades d'usos prohibits per l'article 5 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act).

<p>Sistemes que despleguen tècniques subliminars, enganyoses o manipuladores que alterin el comportament d'una persona o grup de persones perquè prenguin una decisió que causi perjudicis significatius a ella mateixa o altres persones.</p> <p>Aquesta pregunta es basa en l'article 5 quart 1.a)</p>	<p>Sistemes d'IA que exploten les vulnerabilitats d'una persona o grup de persones (per exemple l'edat, la situació social o econòmica o la capacitat mental) alterant el seu comportament de manera que causi perjudicis significatius a ella mateixa o altres persones.</p> <p>Aquesta pregunta es basa en l'article 5 quart 1.b)</p>	<p>Sistemes d'IA que avaluin o classifiquen persones físiques o grups de persones durant un període de temps determinat en funció del seu comportament social o les seves característiques personals o altres conegudes, deduïdes o previstes amb els següents efectes:</p> <ol style="list-style-type: none"> Tracte perjudicial o desfavorable de determinades persones físiques o grups de persones en contextos socials que no guarden relació amb els contextos en què les dades van ser recollides o generades originalment. Tracte perjudicial o desfavorable a determinades persones físiques o grups de persones que sigui injustificat o desproporcionat respecte al seu comportament social o a la seva gravetat <p>Aquesta pregunta es basa en l'article 5 quart 1.c)</p>	<p>Sistemes d'IA que duen a terme avaluació de riscos de persones físiques amb el fi d'avaluar o predir el risc que una persona cometi un delictes basat únicament en l'elaboració de perfils, avaluació dels seus trets i característiques de personalitat.</p> <p>Aquesta pregunta es basa en l'article 5 quart 1.d)</p>	<p>Sist de risc alt</p>
--	---	---	--	-------------------------

Establiment de risc alt, risc limitat o risc baix

En aquest apartat trobareu les qüestions que us permetran saber el nivell de risc associats al vostre sistema més enllà del risc inacceptable o usos prohibits. Per a completar la reavaluació si us plau seguïu el següent circuit:

Risc alt



Aquesta taula conté les pràctiques considerades d'alt risc per l'article 6 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act).

Si contesteu de forma afirmativa a una o més de les següents preguntes, llavors podeu considerar que el vostre sistema està considerat d'aquest grup de risc.

Excepcions

<p>El vostre sistema és utilitzat per autoritats judicials o en el seu nom per investigar, interpretar fets i normes jurídiques o aplicar la llei; usar-se de manera similar en la resolució alternativa de conflictes (per exemple en un procés de mediació); o per influenciar els resultats de processos democràtics o en el comportament dels votants?</p> <p>Aquesta pregunta es basa en l'article 6.2 de la AI Act</p>	<p>El vostre sistema d'IA és un producte, o es tracta d'un component de seguretat d'un producte, subjecte a la normativa europea continguda a l'Annex I de la AI Act?</p> <p>Aquesta pregunta es basa en l'article 6.1.a) de la AI Act</p>	<p>El vostre sistema d'IA és un producte, o es tracta d'un component de seguretat d'un producte, que ha de ser sotmès a una avaluació de conformitat per tercers abans de poder ser comercialitzada o posada en servei d'acord amb la normativa europea continguda a l'Annex I de la AI Act?</p> <p>Aquesta pregunta es basa en l'article 6.1.b) de la AI Act</p>	<p>El vostre sistema s'utilitza per a la identificació biomètrica i categorització de persones físiques en base a dades sensibles o reconeixement d'emocions (perquè incloure sistemes que únicament confirmen la identitat de la persona física)?</p> <p>Aquesta pregunta es basa en l'article 6.2 de l'AI Act</p>	<p>Sist de risc alt</p>
--	--	---	---	-------------------------

Risc limitat

Seleccionar risc



Aquesta taula conté els sistemes considerats de risc limitat, que inclouen els sistemes d'IA generativa i els sistemes de reconeixement d'emocions i identificació biomètrica que no coincideixen amb els supòsits de sistemes prohibits o d'alt risc, segons l'article 50 i els sistemes de propòsit general, segons d'acord amb l'article 51 del Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act).

Si contesteu de forma afirmativa a una o més de les següents preguntes, llavors podeu considerar que el vostre sistema està considerat d'aquest grup de risc

El vostre sistema té la capacitat de servir per a una varietat de propòsits, tant per a l'ús directe com per a la integració en altres sistemes d'IA?

Aquesta pregunta es basa en l'article 3 i l'article 51 de la AI Act.

El vostre sistema es utilitza per a crear contingut de text, so, imatge o vídeo?



Aquesta pregunta es basa en l'article 50.2 i 4 de la AI Act.

El vostre sistema és tracta d'una eina de reconeixement d'emocions o categorització biomètrica?



Aquesta pregunta es basa en l'article 50.3 de la AI Act.

El vostre sistema d'IA està pensat per a persones físiques?

Aquesta pregunta es basa en l'article 5

Risc mínim

Seleccionar risc



En el cas que el vostre sistema no recaigui en cap de les categories anteriors, podrà ser considerat de risc mínim. Si bé el Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial (AI Act) pot requerir alguns requisits de transparència per a determinats sistemes d'IA d'aquest tipus, no imposa obligacions addicionals als sistemes considerats de risc mínim, però convida a comprometre's amb codis de conducta o una avaluació ètica de forma voluntària.

Exemples pràctics d'aplicació de la AI Act

En el cas que no tingueu clar si la legislació europea d'intel·ligència artificial (AI Act) és aplicable en el vostre cas així com la possible categoria de risc aplicable, us proporcionem 50 exemples pràctics d'aplicació de la AI Act segons el nivell de risc. Evidentment, es tracta d'exemples orientatius i, en tots els casos, aquests només serveixen com una guia referència i, per tant, no és exhaustiva i sempre cal contextualitzar-los.

- Una empresa del sector de la salut utilitza una aplicació impulsada per IA per al triatge de pacients.
- Una empresa implementa un sistema de vigilància amb càmeres dotades de reconeixement facial per a la seguretat de les seves instal·lacions.
- Una institució pública utilitza tecnologia de reconeixement de veu per analitzar la prioritat en l'atenció de trucades telefòniques.
- Una institució educativa utilitza un sistema d'IA per fer seguiment del rendiment acadèmic dels estudiants i predir possibles abandonaments.
- Un hospital utilitza un sistema d'IA per analitzar imatges mèdiques i ajudar en el diagnòstic de malalties.
- Un centre de salut utilitza un sistema de IA per a la gestió de les cites i l'organització de les llistes d'espera.
- Una oficina de serveis socials utilitza IA per identificar famílies amb risc de patir situacions de vulnerabilitat i oferir suport proactiu.

Avaluació

En aquest apartat trobareu les preguntes que us permetran, a través d'una autoavaluació, verificar fins a quin grau el vostre sistema d'IA respon a unes consideracions ètiques, legals i d'impacte social a través de 7 principis guia que vertebreren el Model PIO.

Com veureu, cada principi és divideix en taules segons la temàtica que aborden, de manera que cada pregunta es troba inclosa en una casella. El quadre de la qüestió a respondre ve acompanyat de dues altres caselles. La primera conté les referències legals i acadèmiques en què es basa la pregunta, mentre que la segona exposa un exemple amb finalitats il·lustratives, així com la bibliografia de la qual s'ha extret el mateix.

En el procés de verificació trobareu que us mostrem totes les preguntes contingudes en el Model PIO, incloent-hi les de risc alt, risc limitat i risc mínim. Malgrat que el procés de preavaluació us permet identificar quines són les preguntes a contestar més adequades a través d'una etiquetació de les mateixes, us encoratgem a tenir una mirada que sigui específica i alhora global per tal d'aprendre sobre els requeriments que poden afectar-vos més enllà de la normativa.

El teu nivell de risc predefinit és: **Mínim**.
Si ho desitjes, pots canviar-lo a continuació:

Nivell de risc alternatiu

Seleccioneu un nivell de risc alternatiu ▼

Projecte

Nom del projecte per a poder identificar-lo a posteriori

Títol

Títol de l'avaluació

Declaració de responsabilitat

Afirmo haver llegit i accepto la [Declaració de Responsabilitat](#)

Següent

Guardar

Models sectorials

Els Models Sectorials són adaptacions del Model PIO que es desenvolupen amb diferents professionals i persones usuàries per donar resposta a les necessitats específiques d'àmbits o sectors concrets com la salut, l'educació, els serveis socials, etc. Aquest espai estarà dedicat a aquests Models Sectorials que estaran disponibles en els propers mesos en la seva versió beta.



5- Pestanya dels catàlegs:

Legal

Els catàlegs serveixen com a eina per localitzar i conèixer contingut específic que inclou el Model PIO. El present catàleg conté les normes jurídiques en les que s'han inspirat les preguntes del Model PIO. Així mateix, s'enumeren textos d'altres tipologies que contenen recomanacions relatives a l'ús ètic de la IA.

1	Transparència i explicabilitat		+
2	Justícia i equitat		+
3	Seguretat i no maleficència		×
	↳ 1. Funcionament del sistema		
		ARTICLE	PREGUNTA MODEL PIO
	Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 12 14 16	3.1.1 3.1.2 3.1.3 3.1.4 3.1.5
	Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Act]	4	3.1.5
	Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	9 13 14 17 27 33 35 72	3.1.1 3.1.2 3.1.3 3.1.4 3.1.5
	Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		3.1.1 3.1.4 3.1.5

Exemples

Els catàlegs serveixen com a eina per localitzar i conèixer contingut específic que inclou el Model PIO. El present catàleg conté exemples reals justificats i hipotètics a les preguntes del Model PIO que permet a les persones usuàries especificar millor allò que es demana a cada pregunta.

1	Transparència i explicabilitat		+
2	Justícia i equitat		×
	↳ Inclusió i diversitat		
			PREGUNTA MODEL PIO
	Allenghey, cribratge familiar		2.1.2
	Disseny del sistema (H)		2.1.3
	Projecte Gmeface		2.1.9

6- Pestanya de recomanacions:

Hi trobareu dos tipus de recomanacions: de contractes i d'avaluacions.

Contractes

En aquest apartat trobareu contingut recomanat per a la redacció de clàusules de contractes relacionats amb sistemes d'IA. Aquest contingut organitzat a través dels principis del Model PIO, és rellevant per a molts casos d'ús i per determinar l'aplicació de la legislació europea sobre intel·ligència artificial (AI Act) així com el compliment dels més alts estàndards de responsabilitat, seguretat i respecte pels drets humans.

1	Transparència i explicabilitat	+
2	Justícia i equitat	+
3	Seguretat i no maleficència	+
4	Responsabilitat i retiment de comptes	+
5	Privacitat	×

→ 5.1. Protecció de la privacitat

Nº	RECOMANACIÓ DE CLÀUSULA
5.1.1	<p>Comptarà amb mecanismes de protecció de dades presents durant tot el seu cicle de vida encaminats a garantir els següents aspectes:</p> <ul style="list-style-type: none"> • Que les dades de caràcter personal siguin tractades d'acord amb el grau de protecció legalment requerit per tal d'evitar-ne el mal ús, l'alternació, la pèrdua, o la sostracció per part de tercers. • Que les dades subministrades per la persona interessada no siguin venudes, llogades, ni cedides sense el seu consentiment. • Que el sistema compti amb processos per a mantenir o millorar la privacitat i protecció de les dades durant tot el seu cicle de vida. • Que es fan servir tècniques d'anonimat, xifratge i agregació. • Que existeix un protocol per a obtenir el consentiment de les persones afectades abans d'iniciar qualsevol processament de dades a través del sistema, i la informació relativa a aquestes accions és comprensible i accessible per a totes les possibles persones usuàries, inclosos aquelles amb necessitats especials. • Que existeix un mecanisme a través del qual la persona interessada pot sol·licitar que la seva informació sigui eliminada.

Avaluacions

Avaluació de conformitat

Avaluació d'impacte sobre drets fonamentals
Obligacions de transparència

Avaluació de conformitat:

La AI Act exigeix que les persones proveïdores dels sistemes d'alt risc sotmetin la seva IA a una avaluació de conformitat (art.16 i desenvolupada a l'art. 43) i remet als annexos de la Llei per a la seva especificitat. Aquesta consisteix a demostrar que el sistema en qüestió compleix amb els requisits que li són imposats per la AI Act.

La regulació preveu diferents modalitats d'avaluació en funció del tipus de sistema d'alt risc.

A continuació, us proporcionem informació sobre les característiques principals de les avaluacions de conformitat previstes a la AI Act.

1. Procediment d'avaluació intern contemplat a l'annex VI de la AI Act.

Quins sistemes han de ser sotmesos a aquesta avaluació?

- Sistemes de categorització o d'identificació biomètrica i de reconeixement d'emocions.
- Sistemes utilitzats en infraestructures crítiques.
- Sistemes utilitzats en l'àmbit de l'educació i formació professional.
- Sistemes utilitzats en l'àmbit de l'ocupació, gestió dels treballadors i accés a l'autoocupació.
- Sistemes utilitzats en l'àmbit de l'accés i gaudi de serveis i prestacions essencials (públiques o privades).
- Sistemes utilitzats en l'àmbit del compliment de la llei.
- Sistemes utilitzats en l'àmbit de la migració, l'asil i el control de fronteres.
- Sistemes utilitzats en l'àmbit de l'administració de justícia i processos democràtics.

7- Pestanya d'informació:

Hi trobareu les següents informacions: Qui som, el **Model PIO**, justificacions, recursos i la **AI Act**.

Qui som

Qui som
Principis ètics

Qui som

L'Observatori d'Ètica en Intel·ligència Artificial de Catalunya (OEIAC), que pren forma de Càtedra a la Universitat de Girona, i s'insereix en l'Estratègia d'Intel·ligència Artificial (IA) impulsada per la Generalitat de Catalunya amb el nom de CATALONIA.AI.

CATALONIA.AI inclou un eix sobre "Ètica i Societat", que és on es situa l'OEIAC, per tal de promoure el desenvolupament d'una IA ètica, que respecti la legalitat vigent, que sigui compatible amb les nostres normes socials i culturals, i que estigui centrada en les persones.

Podeu consultar més informació sobre l'OEIAC a la seva web de la Universitat de Girona i sobre l'Estratègia CATALONIA.AI a la seva web.

Principis ètics

L'avaluació a través d'aquesta llista de verificació, que integra la legislació actual sobre dades i IA, juntament amb les recomanacions de diversos organismes, està dissenyada per oferir un marc d'avaluació ètica a través de set principis bàsics:

- **Transparència i explicabilitat**, per garantir la claredat de les operacions d'IA i la presa de decisions, fent-les comprensibles per als usuaris i les parts interessades.
- **Justícia i equitat**, per prevenir els biaixos i garantir un tracte just i resultats equitatius per a tots els usuaris de sistemes d'IA.

El Model PIO

Com funciona
A qui va dirigit
Senzillesa

Com funciona

El Model PIO és una nova eina d'avaluació sobre els usos ètics i legals que està harmonitzada amb els requisits legislatius i els estàndards i recomanacions ètiques actuals. Aquesta eina d'avaluació consisteix en una llista de verificació o checklist sobre usos ètics estructurada al voltant de set principis, i dissenyada per al desenvolupament, desplegament i avaluació de dades i sistemes d'IA.

El Model PIO s'inicia amb unes anomenades preguntes zero o preguntes bàsiques que reflecteixen el contingut ètic essencial que conforma la llista de verificació del model i, en aquest sentit, permet fer una ràpida aproximació sobre les consideracions ètiques fonamentals a tenir en compte (Fase 0).

Després d'aquest posicionament inicial, el Model PIO permet realitzar una preavaluació segons les categories de risc contemplades en la normativa sobre intel·ligència artificial de la UE (AI Act). En aquest sentit, es classificaran els sistemes d'IA segons si són considerats de risc inacceptable a partir de la normativa de la AI Act. El risc inacceptable fa referència a un conjunt molt limitat d'usos que són especialment nocius de la IA i que contravenen els valors de la UE, ja que violen els drets fonamentals i, per tant, estan prohibits (Fase 1).

Una cop realitzada aquesta distinció sobre risc inacceptable o no, en la mateixa preavaluació es classificaran els sistemes d'IA segons la AI Act de la següent manera (Fase 2):

- **Risc alt:** aquest fa referència a un nombre limitat de sistemes d'IA que poden generar un impacte advers en la seguretat de les persones o els seus drets fonamentals segons la Carta dels Drets Fonamentals de la UE i, per tant, es consideren d'alt risc.
- **Risc limitat:** aquest fa referència als riscos associats a la falta de transparència en l'ús

Justificacions

Per què verificació?

Per què catàlegs?

Per què recomanacions sobre contractes?

Per què verificació?

La verificació és una eina per avaluar el nostre sistema d'IA a l'abast de tothom per a contribuir a l'ús d'una IA Ètica i d'acord amb la normativa vigent.

Amb aquest procés de verificació descobrim o tenim la certesa sobre la categoria de risc associada al nostre sistema amb la fase de preavaluació i posteriorment, coneixem el detall de l'adequació als set principis ètics troncats del Model PIO. Finalment, s'obté un resultat a través del qual us guiem i indiquem les fortaleses i les millores del vostre sistema d'acord amb el procés realitzat.

Per què catàlegs?

Els catàlegs serveixen com a eina per localitzar i conèixer contingut específic que inclou el Model PIO. Ambdós segueixen l'ordre del Model PIO, és a dir, la categorització a partir dels set principis i la classificació dels apartats corresponents. Així com, la informació classificada també està ordenada de manera alfabètica per facilitar la navegació.

Text per a l'apartat concret:

Text: El present catàleg conté la normativa legal i les recomanacions d'altres sistemes.

Recursos

Avaluem

Acompanyem

Aconsellem

Formem

Avaluem

Proporcionem una eina per la pròpia autoavaluació organitzativa en l'ús ètic de dades i sistemes d'IA que va molt més enllà de l'aplicació de llistes de verificació o checklists sobre usos ètics, especialment a la llum de la nova legislació sobre IA a la Unió Europea (AI Act).

Per què? Doncs perquè a través del nou Model PIO sobre Obligacions i Drets avaluem l'adequació o no dels sistemes i dades als requisits normatius i a estàndards internacionals donant resposta a diverses consideracions crítiques:

-Sobre complexitat i conseqüències no desitjades: Les llistes de verificació aborden qüestions sobre els sistemes d'IA que poden ser complexes, amb el potencial de conseqüències no desitjades i que poden no ser immediatament evidents. En aquest sentit, ajuden als desenvolupadors i a les parts interessades que tinguin en compte una àmplia gamma d'impactes potencials com els relacionats amb la transparència, l'equitat, la responsabilitat o la privadesa.

-Sobre confiança tècnica i confiança social: L'establiment de directrius ètiques clares a través de llistes de verificació pot ajudar a generar aquesta doble confiança a través de la seva adopció generalitzada. Sense elles és molt més difícil que es generi confiança sobre els sistemes que s'estan desenvolupant i desplegant, ja que no hi haurà alineació amb els valors de la societat i els principis ètics.

La AI Act

Antecedents legislatius
Cronologia
Terminis d'aplicació
Altres dates rellevants

En aquest apartat trobareu la informació relativa als antecedents que ha donat lloc a la AI Act tenint en compte la proposta inicial de la Comissió Europea, que forma part de l'executiu de la Unió Europea, el Consell de la Unió Europea, informalment conegut com a Consell de Ministres, i el Parlament Europeu, que juntament amb el Consell de la UE adopta la legislació europea, a proposta de la Comissió Europea.

Així doncs, aquest apartat l'hem dividit en cinc apartats els quals són el recull dels textos per ordre cronològic que s'han aprovat. Comencem per la Comissió Europea, seguim pel Consell de la Unió Europea organitzat segons els informes aprovats en cada presidència, ens centrem en les publicacions de cada comissió del Parlament Europeu, així com en altres institucions o òrgans consultius que integren la Unió Europea i acabem amb el recull del procés de negociació a tres bandes entre la Comissió Europea, el Consell de la Unió Europea i el Parlament Europeu.

També s'ha inclòs una cronologia per facilitar la lectura i interpretació dels antecedents legals que acompanya l'actual Reglament, així com els terminis d'aplicació des de la publicació i entrada en vigor, així com les especificitats d'articles concrets.

Finalment, hi ha un apartat on s'ha resumit altres dates rellevants per al procés d'elaboració i discussió de la AI Act, com les futures a tenir en compte.

Antecedents legislatius

Textos aprovats per:

La Comissió Europea

21.04.2021 – Regulació del Parlament Europeu i del Consell per harmonitzar normes sobre intel·ligència artificial i el perquè es modifiquen determinats actes legislatius de la UE

AI Liability Directive

Objectiu

Relació amb la AI Act
Contingut
Antecedents legislatius

El 28 de setembre de 2022 la Comissió va publicar la Proposta de directiva del Parlament Europeu i del Consell relativa a l'adaptació de les normes de responsabilitat civil extracontractual a la intel·ligència artificial (AI Liability Directive).

En tractar-se encara d'una proposta legislativa, en aquests moments no és possible saber quan es publicarà o entrarà en vigor.

Objectiu

La AI Liability Directive tindrà com a objectiu establir normes que permetran determinar qui serà responsable dels danys i perjudicis derivats d'un sistema d'IA en aquells casos en els quals aquesta qüestió no s'hagués previst prèviament en un contracte. D'aquesta manera, es crearà un règim de responsabilitat uniforme amb el que es pretén millorar el funcionament del mercat interior europeu.

Aquesta regulació podria ser útil, per exemple, en cas que el sistema d'IA que utilitza l'empresa de gestió de residus d'una ciutat per planificar la recollida d'escombraries no fos suficient precisa amb la regularitat en què cal buidar els contenidors d'un carrer, causant molèsties les persones que hi viuen.

8- Navegar per la pàgina d'inici:

Model d'autoavaluació PIO

Autoavaluació per al compliment de la normativa de dades i sistemes d'IA

Iniciar preavaluació

Promou el compliment de la normativa sobre riscos de la intel·ligència artificial mitjançant una verificació exhaustiva. Identifica accions adequades o inadequades i sensibilitza la quàdruple hèlix sobre l'ús ètic i responsable de dades i sistemes d'intel·ligència artificial. Tot això, alineat amb els principis ètics i estàndards internacionals en el disseny, implementació i ús d'aquests sistemes.

Objectius



Garantim el compliment dels més alts estàndards de responsabilitat, seguretat i respecte pels drets humans.

- Una eina d'avaluació que afavoreix el compliment de la normativa i regulació actual sobre riscos associats a la intel·ligència artificial a través d'un procés de verificació exhaustiu.
- Una eina que permet identificar accions adequades o inadequades i sensibilitzar a la quàdruple hèlix a través dels usos ètics i responsables de les dades i sistemes d'intel·ligència artificial.

Preguntes inicials

Sabeu quin és el problema que esteu intentant resoldre amb l'ús d'un sistema d'IA?	Sou conscients del vostre grau de responsabilitat respecte els possibles perjudicis d'utilitzar un sistema d'IA?
Us heu plantejat si és necessari utilitzar un sistema d'IA per resoldre aquest problema?	Utilitzeu dades d'una forma que es garanteixen drets fonamentals com el dret a la privadesa i els drets d'autor?
Heu considerat els beneficis que aportarà l'ús d'un sistema d'IA i si aquests superen els riscos que planteja?	Sabeu que un sistema d'IA ha d'augmentar capacitats però, en cap cas, limitar l'autonomia de les persones i la seva presa de decisions?
Sabeu explicar de quina manera el sistema d'IA resoldrà el problema o objectiu concret d'una manera comprensible?	Teniu en compte que la sobreestimació de les capacitats d'un sistema d'IA contribueix a la desinformació tècnica i comercial?
Heu establert mecanismes per evitar que el sistema d'IA no s'exploti de manera maliciosa?	Coneixeu l'impacte ambiental com la petjada de carboni associada a l'ús del sistema d'IA?

Catàlegs

A-B

Exemples

Exemples reals i hipotètics a les preguntes del Model PIO.

100+

Legal i recomanacions

Normes jurídiques en les que s'han inspirat les preguntes del Model PIO.

Recomanacions

Oferim contingut recomanat per a la redacció de clàusules de contractes relatius a sistemes d'IA.

Transparència	Justícia	Seguretat	Responsabilitat
Privacitat	Autonomia	Sostenibilitat	
Totes les recomanacions			



T'oferim

Model PIO

El Model PIO és una nova eina d'avaluació sobre els usos ètics i legals que està harmonitzada amb els requisits legislatius i els estàndards i recomanacions ètiques actuals.

Avaluem

Proposem una sèrie de preguntes

Acompanyem

T'oferim la possibilitat d'un acompanyament del procés d'adaptació per assolir una uniformitat

Aconsellem

T'oferim la possibilitat de rebre

Formem

T'oferim diverses modalitats formatives de caràcter general i específic sobre les temes

Preguntes

FAQs

Quina és la relació de la AI Act amb els drets humans?

+

Quan entra en vigor la AI Act?

+

És aconsellable complir amb la AI Act encara que el meu sistema no estigui contemplat?

+

ANNEX III: CATÀLEG LEGAL I DE RECOMANACIONS.

El present catàleg conté les normes jurídiques en les que s'han inspirat les preguntes del **Model PIO** Obligacions i Drets. Així mateix, s'enumeren textos d'altres tipologies que contenen recomanacions relatives a l'ús ètic de la IA.

	ARTICLE	PREGUNTA MODEL PIO
1. TRANSPARÈNCIA I EXPLICABILITAT		
1.1. ANÀLISI PRELIMINAR DE L'ÚS DEL SISTEMA		
Carta de drets fonamentals de la UE	11	1.1.5
Conveni europeu de drets humans	10 i 14	1.1.3, 1.1.5 i 1.1.6
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 10 , 14 , 16 i 18	1.1.2, 1.1.3, 1.1.4, 1.1.5 i 1.1.6
Declaració universal dels DDHH	19	1.1.3 i 1.1.5
Directiva 2019/882, de 17 d'abril del 2019 [Directiva sobre els requisits d'accessibilitat dels productes i serveis]	4	1.1.6
Directiva 2016/2102, de 26 d'octubre de 2016 [Directiva sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic]	4	1.1.6
Pacte internacional de drets civils i polítics	19	1.1.3 i 1.1.5
Proposta Directiva del Parlament Europeu i del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	1.1.2 i 1.1.3
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	11 , 12 , 13 , 14 , 16 , 22 , 50 , 53 , 54 , 55 i 95	1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5 i 1.1.6
AI and data protection risk toolkit d'ICO		1.1.1 i 1.1.2

AI ethics assessment de GSMA		1.1.6
An interdisciplinary framework to operationalise AI ethics d'AIEIG		1.1.3
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		1.1.1, 1.1.3 i 1.1.6
Open letter The PROPOSTA Must Protect the Rule of Law de la Civil Liberties Union for Europe I l'European Civic Forum.		1.1.6
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		1.1.6

1.2. EXPLICABILITAT

Carta de drets fonamentals de la UE	11	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.6 i 1.2.7
Conveni europeu de drets humans	10	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.6 i 1.2.7
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8, 11, 14, 15 i 16	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.7, 1.2.8 i 1.2.9.
Declaració universal dels DDHH	19	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.6 i 1.2.7
Regulació 2022/868, de 30 de Maig del 2022 [Llei Europea sobre la Governança de dades]	21	1.2.7
Pacte internacional de drets civils i polítics	19	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.6 i 1.2.7
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	1.2.5, 1.2.6 i 1.2.8
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	10, 11, 13, 14, 15, 50 i 53	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.7, 1.2.8 i 1.2.9

Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	5 i 13	1.2.7 i 1.2.8
AI and data protection risk toolkit d'ICO		1.2.6 i 1.2.7
AI ethics assessment de GSMA		1.2.5 i 1.2.6
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		1.2.5 i 1.2.6
Inteligència artificial: Transparencia, de l'Agència Espanyola de Protecció de Dades		1.2.4
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		1.2.8 i 1.2.9

1.3. TRAÇABILITAT I REPRESENTATIVITAT

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 11 , 12 , 14 i 18	1.3.1, 1.3.2, 1.3.3, 1.3.4 i 1.3.5
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	1.3.1 i 1.3.4
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	10 , 13 , 17 , 26 , 53 , 61 i 72	1.3.1, 1.3.2, 1.3.3, 1.3.4 i 1.3.5
Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	8	1.3.3
A Human Rights-Based Approach To Data d'ACNUDH.		1.3.1, 1.3.2 i 1.3.4
AI and data protection risk toolkit d'ICO		1.3.4
AI ethics assessment de GSMA		1.3.4

[Assessment list for Trustworthy artificial Intelligence \(ALTAI\) for self assessment](#) 1.3.2 i 1.3.3

1.4. PROTOCOLS DE COMUNICACIÓ

[Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret](#) [8](#), [14](#) i [16](#) 1.4.1, 1.4.2, 1.4.3 i 1.4.4

[Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial \[AI Act\]](#) [9](#) i [95](#) 1.4.1, 1.4.2, 1.4.3 i 1.4.4

[A Human Rights-Based Approach To Data d'ACNUDH](#) 1.4.3

[Algorithmic Equity Toolkit d'ACLU](#) 1.4.3

[An interdisciplinary framework to operationalise AI ethics d'AIEIG](#) 1.4.1

[Assessment list for Trustworthy artificial Intelligence \(ALTAI\) for self assessment](#) 1.4.1, 1.4.2 i 1.4.3

[Recommendation on the Ethics of Artificial Intelligence de la UNESCO](#) 1.4.1

ARTICLE

PREGUNTA
MODEL PIO

2. JUSTÍCIA I EQUITAT

2.1. INCLUSIÓ I DIVERSITAT

[Carta de drets fonamentals de la UE](#) [21](#) i [26](#) 2.1.1, 2.1.2, 2.1.3 i 2.1.9

[Carta social europea](#) [15](#) 2.1.9

Conveni europeu de drets humans	14	2.1.1, 2.1.2, 2.1.3 i 2.1.9
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	5, 10, 16 i 18	2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.7, 2.1.8, 2.1.9, 2.1.10,
Declaració universal dels DDHH	21	2.1.10
Directiva 2019/882, de 17 d'abril del 2019 [Directiva sobre els requisits d'accessibilitat dels productes i serveis]	4	2.1.9
Directiva 2016/2102, de 26 d'octubre de 2016 [Directiva sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic]	4	2.1.9
Pacte internacional de drets civils i polítics	26	2.1.1, 2.1.2, 2.1.3 i 2.1.9
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	9, 10, 15, 16, 27, 55 i 95	2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.1.9 i 2.1.10
AI and data protection risk toolkit d'ICO		2.1.5, 2.1.6, 2.1.7 i 2.1.8
AI ethics assessment de GSMA		2.1.1, 2.1.2 i 2.1.3
A Human Rights-Based Approach To Data d'ACNUDH		2.1.5
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		2.1.3, 2.1.5, 2.1.6, 2.1.7 i 2.1.8
Getting The Future Right, Artificial Intelligence And Fundamental Rights de la FRA		2.1.1 i 2.1.2
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		2.1.1 i 2.1.2

2.2. IDENTIFICACIÓ I MITIGACIÓ DE BIAIXOS

Carta de drets fonamentals de la UE	7 , 8 , 11 , 21 , 26 i 47	2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8 i 2.2.9
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 10 , 11 , 12 , 14 , 16 i 18	2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.10 i 2.2.11
Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals	7	2.2.6
Conveni europeu de drets humans	8 , 10 , 13 i 14	2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8 i 2.2.9
Declaració universal dels DDHH	8 , 12 i 19	2.2.6, 2.2.8 i 2.2.9,
Directiva 2016/680, de 27 d'abril de 2016, [Directiva de protecció de dades amb fins de prevenció, investigació, detecció, enjudiciament o execució d'infraccions penals]	10	2.2.7
Pacte internacional de drets civils i polítics	2 , 17 , 19 i 26	2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8 i 2.2.9
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	2.2.1, 2.2.2, 2.2.5, 2.2.7, 2.2.8, 2.2.9, 2.2.10 i 2.2.11
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	9 , 10 , 13 , 14 , 15 , 27 , 53 , 55 , 72 i 95	2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.9, 2.2.10 i 2.2.11
Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	9 , 24-31 i 32	2.2.6, 2.2.7 i 2.2.11

Reglament 2018/1725, de 23 d'octubre de 2018, [Reglament de protecció de dades tractades per institucions, òrgans i organismes de la Unió]	10	2.2.7
A Human Rights-Based Approach To Data d'ACNUDH		2.2.2
An interdisciplinary framework to operationalise AI ethics d'AIEIG		2.2.4
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		2.2.1, 2.2.2, 2.2.3, 2.2.6 i 2.2.11
Getting The Future Right, Artificial Intelligence And Fundamental Rights de la FRA		2.2.1, 2.2.5 i 2.2.7
Towards meaningful fundamental rights impact assessments under the DSA d'Accessnow i el European Center for Not-for-Profit Law.		2.2.4

	ARTICLE	PREGUNTA MODEL PIO
--	---------	--------------------

3. SEGURETAT I NO MALEFICÈNCIA

3.1. FUNCIONAMENT DEL SISTEMA

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8, 12, 14, i 16	3.1.1, 3.1.2, 3.1.3, 3.1.4 i 3.1.5
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	3.1.5
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	9, 13, 14, 17, 27, 53, 55 i 72	3.1.1, 3.1.2, 3.1.3, 3.1.4 i 3.1.5
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		3.1.1, 3.1.4 i 3.1.15

3.2. TRAÇABILITAT PER A LA GESTIÓ DEL RISC

Carta de drets fonamentals de la UE	1 , 3 , 7 i 8	3.2.1
Conveni europeu de drets humans	14	3.2.9
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 10 , 12 , 14 i 16	3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.2.8 i 3.2.9
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	9 , 10 , 12 , 15 , 27 , 50 , 55 , 72 i 95	3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.2.8 i 3.2.9
Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	9	3.2.9
Algorithmic Equity Toolkit d'ACLU		3.2.8 i 3.2.9
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		3.2.2, 3.2.7, 3.2.8 i 3.2.9
Open letter The AI Act Must Protect the Rule of Law de la Civil Liberties Union for Europe i l'European Civic Forum		3.2.1
Towards meaningful fundamental rights impact assessments under the DSA d'AN i ECNL		3.2.1

3.3. MECANISMES DE SEGURETAT

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	7 , 8 , 11 , 12 i 16	3.3.1, 3.3.2, 3.3.3 i 3.3.4
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	3.3.1 i 3.3.2
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	12 , 15 , 17 , 55 i 72	3.3.1, 3.3.2, 3.3.3 i 3.3.4

A Human Rights-Based Approach To Data d'ACNUDH		3.3.3
Algorithmic Equity Toolkit d'ACLU		3.3.4
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		3.3.3 i 3.3.4
Declaració de Barcelona		3.3.3

3.4. PROTECCIÓ ENFRONT D'ATACS

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	12	3.4.1 i 3.4.2
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	3.4.1 i 3.4.2
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	15 i 55	3.4.1 i 3.4.2
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		3.4.1 i 3.4.2

ARTICLE PREGUNTA
MODEL PIO

4. RESPONSABILITAT I RETIMENT DE COMPTES

4.1. CONTROL

Carta de drets fonamentals de la UE	47	4.1.3 i 4.1.4
---	--------------------	---------------

Conveni europeu de drets humans	13	4.1.3 i 4.1.4
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 14 i 16	4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5 i 4.1.6
Declaració universal dels DDHH	8	4.1.3 i 4.1.4
Pacte internacional de drets civils i polítics	2	4.1.3 i 4.1.4
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	4.1.2, 4.1.3 i 4.1.4
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	11 , 14 i 55	4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5 i 4.1.6
AI and data protection risk toolkit d'ICO		4.1.1
AI ethics assessment de GSMA		4.1.2
Algothritic Equity Toolkit d'ACLU		4.1.2
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		4.1.2

4.2. RETIMENT DE COMPTES

Carta de drets fonamentals de la UE	47	4.2.1, 4.2.3 i 4.2.4
Conveni europeu de drets humans	13	4.2.1, 4.2.3 i 4.2.4
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 9 i 14	4.2.1, 4.2.2, 4.2.3 i 4.2.4
Declaració universal dels DDHH	8	4.2.1, 4.2.3 i 4.2.4

Pacte internacional de drets civils i polítics	2	4.2.1, 4.2.3 i 4.2.4
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	4.2.1
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	13, 14, 17 i 72	4.2.1, 4.2.2, 4.2.3 i 4.2.4
Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	24 - 31	4.2.1
Artificial Intelligence Contractual Clauses de 'Society for Computers & Law (SCL) AI Group.		4.2.1
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		4.2.2 i 4.2.3
Canada protocol		4.2.1
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		4.2.1
Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain,		4.2.1

4.3. FIGURES DE PROTECCIÓ

Carta de drets fonamentals de la UE	47	4.3.1, 4.3.2 i 4.3.3
Conveni europeu de drets humans	13	4.3.1, 4.3.2 i 4.3.3
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8, 9 i 14	4.3.1, 4.3.2 i 4.3.3
Declaració universal dels DDHH	8	4.3.1, 4.3.2 i 4.3.3
Pacte internacional de drets civils i polítics	2	4.3.1, 4.3.2 i 4.3.3

Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	1-9	4.3.3
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	11, 13, 17, 27 i 72	4.3.1, 4.3.2 i 4.3.3
Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	24-31	4.3.1
AI and data protection risk toolkit d'ICO		4.3.1
AI ethics assessment de GSMA		4.3.3
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		4.3.1, 4.3.2 i 4.3.3

4.4. CAPACITAT DE LA IA

Carta de drets fonamentals de la UE	6	4.4.1 i 4.4.2
Conveni europeu de drets humans	5	4.4.1 i 4.4.2
Declaració universal dels DDHH	3	4.4.1 i 4.4.2
Pacte internacional de drets civils i polítics	9	4.4.1 i 4.4.2
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	13, 14 i 53	4.4.1 i 4.4.2
Keep your AI claims in check de la Federal Trade Comission		4.4.1 i 4.4.2

4.5. PROMOCIÓ D'UNA CULTURA DE L'ÈTICA I RESPONSABILITAT RELACIONADA AMB LA IA

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	9	4.5.1, 4.5.2 i 4.5.3
--	-------------------	----------------------

Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	27 i 95	4.5.1, 4.5.2, 4.5.3 i 4.5.4
--	---	-----------------------------

	ARTICLE	PREGUNTA MODEL PIO
5. PRIVACITAT		
5.1. PROTECCIÓ DE LA PRIVACITAT		
Carta de drets fonamentals de la UE	7 , 8 , 21 i 26	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.8, 5.1.9, 5.1.10 i 5.1.11
Carta social europea	15	5.1.11
Conveni europeu de drets humans	8	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.8, 5.1.9, 5.1.10 i 5.1.11
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 10 , 11 i 18	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8, 5.1.9, 5.1.10 i 5.1.11
Conveni 108 per a la protecció de les persones físiques pel que fa al tractament de dades personals	7 i 8	5.1.1, 5.1.2, 5.1.4 i 5.1.11
Declaració universal dels DDHH	12	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.8, 5.1.9, 5.1.10 i 5.1.11
Pacte internacional de drets civils i polítics	17 i 26	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.8, 5.1.9, 5.1.10 i 5.1.11
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	5.1.11

Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	10 , 13 , 17 , 27 , 50 , 55 , 72 i 95	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.8, 5.1.9, 5.1.10 i 5.1.11
Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	5 , 6 , 7 , 17 , 25 i 32	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8, 5.1.9, 5.1.10 i 5.1.11
Regulació 2022/868, de 30 de Maig del 2022 [Llei Europea sobre la Governança de dades]	21	5.1.1, 5.1.2, 5.1.4, 5.1.5 i 5.1.7
A Human Rights-Based Approach To Data d'ACNUDH.		5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.8, 5.1.9 i 5.1.10
AI and data protection risk toolkit d'ICO		5.1.1, 5.1.2 i 5.1.5
AI ethics assessment de GSMA		5.1.1
An interdisciplinary framework to operationalise AI ethics d'AIEIG		5.1.3, 5.1.4, 5.1.6, 5.1.8, 5.1.9 i 5.1.10
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		5.1.3, 5.1.4, 5.1.6, 5.1.9 i 5.1.10
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		5.1.8 i 5.1.11

5.2. GOVERNANÇA DE DADES

Carta de drets fonamentals de la UE	7 i 8	5.2.1, 5.2.2, 5.2.6, 5.2.7 i 5.2.8
Conveni europeu de drets humans	8	5.2.1, 5.2.2, 5.2.6, 5.2.7 i 5.2.8

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	8 , 11 i 12	5.2.1, 5.2.2, 5.2.6, 5.2.7 i 5.2.8
Declaració universal dels DDHH	12	5.2.1, 5.2.2, 5.2.6, 5.2.7 i 5.2.8
Directiva 2016/680, de 27 d'abril de 2016, [Directiva de protecció de dades amb fins de prevenció, investigació, detecció, enjudiciament o execució d'infraccions penals]	10 i 20	5.2.6 i 5.2.8
Pacte internacional de drets civils i polítics	17	5.2.1, 5.2.2, 5.2.6, 5.2.7 i 5.2.8
Proposta Directiva del Parlament Europeu del Consell relativa a normes de responsabilitat civil extracontractual a la intel·ligència artificial [AI Liability Directive]	4	5.2.3, 5.2.4, 5.2.5, 5.2.6 i 5.2.8
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	10 , 13 , 14 , 17 , 50 i 53	5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7 i 5.2.8
Reglament 2016/679, de 27 d'abril 2016 [Reglament general de protecció de dades]	5 , 9 , 24 , 25 , 26 - 31 , 30	5.2.1, 5.2.4, 5.2.6 i 5.2.8
Regulació 2022/868, de 30 de Maig del 2022 [Llei Europea sobre la Governança de dades]	20	5.2.1
Reglament 2018/1725, de 23 d'octubre de 2018, [Reglament de protecció de dades tractades per institucions, òrgans i organismes de la Unió]	4 , 10 i 27	5.2.6 i 5.2.8
AI Data Annotation • CertifAI • Accredible • Certificates, Badges and Blockchain		5.2.2
A Human Rights-Based Approach To Data d'ACNUDH.		5.2.5
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		5.2.1, 5.2.2, 5.2.3 i 5.2.4
Llibre blanc de la Comissió Europea sobre IA, un enfocament europeu d'excel·lència i confiança		5.2.7

	ARTICLE	PREGUNTA MODEL PIO
6. AUTONOMIA		
6.1. IMPACTE EN LES CAPACITAT DE LES PERSONES USUÀRIES		
Carta de drets fonamentals de la UE	6 i 38	6.1.1, 6.1.2, 6.1.4 i 6.1.7
Conveni europeu de drets humans	5	6.1.1, 6.1.2 i 6.1.7
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	7 , 8 , 15 i 18	6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6 i 6.1.7
Declaració Universal dels DDHH	3	6.1.1, 6.1.2 i 6.1.7
Pacte internacional de drets civils i polítics	9	6.1.1, 6.1.2 i 6.1.7
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	13 , 27 , 50 , 55 , 72 i 95	6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6 i 6.1.7
AI ethics assessment de GSMA		6.1.1 i 6.1.2
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		6.1.1 i 6.1.3, 6.1.2, 6.1.5 i 6.1.6
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		
6.2. PERCEPCIÓ DEL SISTEMA		
Carta de drets fonamentals de la UE	6	6.2.1 i 6.2.2
Conveni europeu de drets humans	5	6.2.1 i 6.2.2

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	7 , 8 , 12 i 16	6.2.1, 6.2.2, 6.2.3, 6.2.4 i 6.2.5, 6.2.6 i 6.2.8
Declaració Universal dels DDHH	3	6.2.1 i 6.2.2
Pacte internacional de drets civils i polítics	9	6.2.1 i 6.2.2
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	9 , 13 , 14 , 15 , 27 , 50 , 55 , 72 i 95	6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7 i 6.2.8
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		6.2.1 i 6.2.2
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		6.2.8

	ARTICE	PREGUNTA MODEL PIO
7. SOSTENIBILITAT		
7.1. DESENVOLUPAMENT SOSTENIBLE		
Carta de drets fonamentals de la UE	17 , 21 i 31 - 34	7.1.1, 7.1.3, 7.1.4, 7.1.5, 7.1.6 i 7.1.7
Carta social europea	1-4 , 5 , 6 , 7 - 29 i 30	7.1.1, 7.1.2 i 7.1.7
Conveni europeu de drets humans	14	7.1.3 i 7.1.4
Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	10 i 16	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.6 i 7.1.7
Declaració universal dels drets humans	7 , 17 , 22 - 24 i 25	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6co i 7.1.7
Directiva 2001/29/CE, de 22 de maig del 2001 [Directiva dels drets d'autor i drets afins en la societat de la informació]	1 _____ i següents	7.1.6
Directiva 2019/790, de 17 d'abril del 2019 [Directiva sobre els drets d'autor i drets afins en el mercat únic digital]	1 _____ i següents	7.1.6
Pacte internacional de drets civils i polítics	26	7.1.3, 7.1.4, i 7.1.7
Pacte internacional de drets econòmics, socials i culturals	6 , 7 , 8 i 11	7.1.1, 7.1.2, 7.1.5 i 7.1.7
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	27 , 53 , 55 i 95	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6 i 7.1.7
Protocol del Conveni europeu de drets humans per a la Protecció dels Drets Humans i les Llibertats Fonamentals	1	7.1.6
A Human Rights-Based Approach To Data d'ACNUDH		7.1.4

Algorithmic Equity Toolkit d'ACLU		7.1.4
Open letter The AI Act Must Protect the Rule of Law de la Civil Liberties Union for Europe i l'European Civic Forum		7.1.1
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		7.1.1, 7.1.2, 7.1.4, 7.1.5, 7.1.6 i 7.1.7
Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU		7.1.2
The Ethics of AI Business Practices: A Review of 47 AI Ethics Guidelines, d'Attard-Frost et al.		7.1.3

7.2. IMPACTE MEDIAMBIENTAL

Conveni marc del Consell d'Europa sobre intel·ligència artificial i drets humans, democràcia i estat de dret	16	7.2.1, 7.2.2, 7.2.7 i 7.2.9
Reglament 2024/1689 del Parlament i del Consell sobre intel·ligència artificial [AI Act]	53 i 95	7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6, 7.2.7, 7.2.8 i 7.2.9
AI ethics assessment de GSMA		7.2.2 i 7.2.3
Assessment list for Trustworthy artificial Intelligence (ALTAI) for self assessment		7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6, 7.2.7, 7.2.8 i 7.2.9
Ethical Impact Assessment: A Tool of the Recommendation on the Ethics of Artificial Intelligence d'UNESCO		7.2.6 i 7.2.9
Recommendation on the Ethics of Artificial Intelligence de la UNESCO		7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6, 7.2.7, 7.2.8 i 7.2.9
Resolució 48/13 de 8 d'Octubre de 2021 del Consell de Drets Humans de l'ONU		7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6, 7.2.7, 7.2.8 i 7.2.9

ANNEX IV: CATÀLEG D'EXEMPLES.

Llegenda:

Exemples reals – poden tenir una o dues entrades enllaçades

Exemples hipotètics (H) – enllaç a la pregunta del **Model PIO**

	PREGUNTA	MODEL PIO
1. TRANSPARÈNCIA I EXPLICABILITAT		
1.1. ANÀLISIS PRELIMINAR DE L'ÚS DEL SISTEMA		
Algoritme Rank Brain		1.1.2
Apple no identifica als proveïdors		1.1.5
Assistent de veu Alexa		1.1.4
Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)		1.1.3
Google Assistant		1.1.6
Google Flu Trends, calculador de prediccions		1.1.1
1.2. EXPLICABILITAT		
Allen NLP , llenguatge IA		1.2.1
Autopilot dels cotxes Tesla		1.2.3
ChatGPT no utilitza etiquetes		1.2.4
Explicació del funcionament (H)		1.2.9
IBM Watson , anàlisi de dades		1.2.2
ITutorGroup's , procés de selecció		1.2.5
Meta amb Facebook i Instagram		1.2.7
Siri, processament de llenguatge natural		1.2.6
Mesures (H)		1.2.8
1.3. TRAÇABILITAT I REPRESENTATIVITAT		
Departament de Treball i Pensions del Regne Unit		1.3.2

Edat (H)	1.3.3
Oficina Municipal de Dades (H)	1.3.4
Sepsis model, sistema sanitari	1.3.1

1.4. PROTOCOLS DE COMUNICACIÓ

Bústia digital (H)	1.4.1
Comitè d'ètica (H)	1.4.3
Incident (H)	1.4.4

PREGUNTA

MODEL PIO

2. JUSTÍCIA I EQUITAT

2.1. INCLUSIÓ I DIVERSITAT

Allenghey , cribratge familiar	2.1.2
Disseny del sistema (H)	2.1.3
Projecte Gmeface	2.1.9
Passaport expedit pel Regne Unit	2.1.1
Vots electrònics (H)	2.1.10

2.2. IDENTIFICACIÓ I MITIGACIÓ DE BIAIXOS

Algoritme GRADE	2.2.1
Auditoria ForHumanity	2.2.4
Avís de sortides esbiaixades (H)	2.2.10
Google Fitbit	2.2.6
Grup demogràfics diversos (H)	2.2.5
Expert d'ètica i diversitat	2.2.3
Regles i límits predefinitos (H)	2.2.8
Revisió de les dades (H)	2.2.11
Submostreig aleatori o Random Undersampling	2.2.2
Rufus chatbot d'Amazon	2.2.9
Sistemes de reconeixements facial	2.2.7

	<i>PREGUNTA</i>
	<i>MODEL PIO</i>
3. SEGURETAT I NO MALEFICIÈNCIA	
3.1. FUNCIONAMENT DEL SISTEMA	
Auditoria (H)	3.1.4
Cercador de Google	3.1.3
Tay, chatbot de Microsoft	3.1.1
Dades protegides (H)	3.1.5
3.2. TRAÇABILITAT PER LA GESTIÓ DEL RISC	
Assistència social (H)	3.2.4
Selecció de CV	3.2.1
Estafa telefònica	3.2.8
Lesions de tòrax	3.2.9
Protocol (H)	3.2.2
Risilinc	3.2.3
Vehicle autònom (H)	3.2.7
Xarxes socials (H)	3.2.5
3.3. MECANISMES DE SEGURETAT	
Tay, chatbot de Microsoft	3.3.2
Dades de la ciutadania (H)	3.3.1
Google Translate	3.3.4
Xarxa de trànsit (H)	3.3.3
3.4. PROTECCIÓ ENFRONT D'ATACS	
Obres visuals (H)	3.4.2
Firewall, sistema de seguretat	3.4.1

4. RESPONSABILITAT I RETIMENT DE COMPTES

4.1. CONTROL

Acomiadament Sr.Diallo	4.1.4
Formacions especialitzades	4.1.1
MasterCard	4.1.2
Persona responsable (H)	4.1.5
Protocol de monitoratge continu (H)	4.1.6
Revisió manual (H)	4.1.3

4.2. RETIMENT DE COMPTES

Comitè d'ètica	4.2.3
Portal de transparència (H)	4.2.4
Responsabilitat Civil	4.2.1

4.3. FIGURES DE PROTECCIÓ

Assegurança de responsabilitat civil (H)	4.3.3
Cambridge Analytica	4.3.1

4.4. CAPACITAT DE LA IA

Mapfre	4.4.1
Robot de cuina (H)	4.4.2

4.5. PROMOCIÓ D'UNA CULTURA DE L'ÈTICA I RESPONSABILITAT

Control de l'ús dels DDHH i benestar (H)	4.5.4
Institut de responsabilitat de la IA	4.5.1
Responsable d'ètica	4.5.2

	<i>PREGUNTA</i>
	<i>MODELPIO</i>
5. PRIVACITAT	
5.1. PROTECCIÓ DE LA PRIVACITAT	
Accés a la informació sensible (H)	5.1.9
Ring i Alexia	5.1.7
Consentiment en l'ús de dades (H)	5.1.6
Eliminació de dades personals (H)	5.1.4
Identificadors aleatoris (H)	5.1.10
Identificació biomèdica	5.1.8
Imatges facials	5.1.5
Meta, incompliment Llei de Protecció de Dades	5.1.2
Persones amb diversitat funcional (H)	5.1.11
Ring , filial d'Amazon en càmeres de videovigilància	5.1.1
Sistema VEIL.AI, dades sanitàries	5.1.3
5.2. GOVERNANÇA DE DADES	
ADP, anonimitzador de nòmines	5.2.8
K-means clustering, algoritme d'aprenentatge no supervisat	5.2.7
Menor quantitat de dades sensibles (H)	5.2.6

PREGUNTA
MODEL PIO

6. AUTONOMIA

6.1. IMPACTE EN LES CAPACITATS DELS USARIS

Assistent personal (H)	6.1.1
BlenderBot3 , robot conversacional	6.1.6
Càncer de colon	6.1.3
<i>ChatGPT</i> (H)	6.1.4
Coffe Meets Bagel	6.1.2
IA adaptativa	6.1.7
Organització Benèfica Scope	6.1.5

6.2. PERCEPCIÓ DEL SISTEMA

Adaptabilitat (H)	6.2.7
Algoritmes transparents (H)	6.2.2
Autonomia (H)	6.2.4
Avaluació de riscos (H)	6.2.6
Filtre one.com	6.2.8
Emmi , assistent virtual de Mediamarkt.	6.2.1
Monitoreig dels sistemes d'IA	6.2.5
Control i modificació de les decisions de la IA	6.2.3

	<i>PREGUNTA</i>
	<i>MODEL PIO</i>
7. SOSTENIBILITAT	
7.1. DESENVOLUPAMENT SOSTENIBLE	
Accés social	7.1.3
Cimera laboral	7.1.7
Entrega de productes	7.1.1
Organització Internacional del Treball	7.1.4
Projecte IKI	7.1.2
Tracte a les persones implicades en l'etiquetatge de dades (H)	7.1.5
Stable Diffusion	7.1.6
7.2. IMPACTE MEDIAMBIENTAL	
Autogrid	7.2.8
Cost energètic de les IA generatives	7.2.1
Depp Render	7.2.4
Emmagatzematge	7.2.7
Practiques de disseny sostenible de Switch	7.2.6
Reduir el consum d'energia	7.2.3
Trobades (H)	7.2.9
Zero-shot (H)	7.2.5

ANNEX V: LA AI ACT.

En aquest apartat trobareu la informació relativa als antecedents que ha donat lloc a la **AI Act** tenint en compte la proposta inicial de la Comissió Europea, que forma part de l'executiu de la Unió Europea, el Consell de la Unió Europea, informalment conegut com a Consell de Ministres, i el Parlament Europeu, que juntament amb el Consell de la Unió Europea adopta la legislació europea, a proposta de la Comissió Europea.

Així doncs, aquest apartat l'hem dividit en cinc apartats els quals són el recull dels textos per ordre cronològic que s'han aprovat. Comencem per la Comissió Europea, seguim pel Consell de la Unió Europea organitzat segons els informes aprovats en cada presidència, ens centrem en les publicacions de cada comissió del Parlament Europeu, així com en altres institucions o òrgans consultius que integren la Unió Europea i acabem amb el recull del procés de negociació a tres bandes entre la Comissió Europea, el Consell de la Unió Europea i el Parlament Europeu.

Finalment, s'ha inclòs una cronologia per facilitar la lectura i interpretació dels antecedents legals que acompanya l'actual Llei.

Antecedents legislatius

Textos aprovats per:

La Comissió Europea

21.04.2021 – Regulació del Parlament Europeu i del Consell per harmonitzar normes sobre intel·ligència artificial i el perquè es modifiquen determinats actes legislatius de la UE

[Llibre blanc sobre intel·ligència artificial. Una mirada europea de l'excel·lència i la confiança](#) (19.02.2020)

[El Reglament](#) (21.04.2021)

[Annexos al Reglament](#) (21.04.2021)

[Document de treball dels serveis de la Comissió per avaluar l'impacte de la normativa](#) (21.04.2021)

[Annexos del document de treball](#) (21.04.2021)

[Estudi per a fer costat a l'avaluació de l'impacte de la normativa](#) (21.04.2021)

[Comunicació per a la Comissió del Parlament Europeu, el Consell, el Comitè econòmic i social i el comitè de les regions](#) (21.04.2021)

[Annexos a la comunicació](#) (21.04.2021)

[Avaluació de l'impacte inicial: proposta de l'acte jurídic del Parlament Europeu i el Consell](#) (20.07.2021)

El Consell de la Unió Europea

Informe del procés d'elaboració del text de la AI Act amb les diferents presidències del Consell

[L'Informe resum](#) (06.12.2022)

Actuacions realitzades durant cada una de les presidències

Presidència d'Eslovènia (2a meitat 2021)	Informe de progrés (22.11.2021) Text adoptat (29.11.2021)
Presidència de França (1a meitat 2022)	Informe de progrés (16.05.2022) Text adoptat (15.06.22) Text adoptat (15.07.2022)
Presidència de Txèquia (2a meitat 2022)	Text adoptat dels articles 1 – 29 (16.09.2022) Text adoptat dels articles 30 – 85 (23.09.2022) Quart text adoptat (19.10.2022) Esborrany de cooperació (03.11.2022)

El Parlament Europeu

Comissions competents: Mercat Intern i Protecció del consumidor (IMCO) i Llibertats Civils, Justícia i Afers Socials (LIBE)

[Esmenes](#) (13.06.2022)

[Informe previ](#) (22.05.2023)

[Text adoptat](#) (14.06.2023)

Comissions associades: Qüestions Jurídiques (JURI), Indústria, Recerca i Energia (ITER) i Cultura i Educació (CULT)

Text consolidat [Esmenes](#) (24.03.2022)

Articles 13, 14, 52 i 69 [Esmenes](#) (31.03.2022)

Articles 15 i 55 [Esmenes](#) (01.04.2022)

Comissions per a dictamen simple

Transport i Turisme (TRAN) [Esmenes](#) (04.05.2022)

Medi Ambient, Salut Pública i Seguretat Alimentària (ENVI) [Esmenes](#) (25.01.2022)

Altres institucions de la UE o òrgans consultius

Comitè Europeu de Protecció de Dades (EDPB) i Supervisor Europeu de Protecció de Dades (EDPS)	Dictamen conjunt CEPD-CEPD 5/2021 sobre la proposta de la AI Act (18.06.2021)
Comitè Econòmic i Social Europeu (CESE)	Dictamen del CESE sobre la proposta de la AI Act (22.09.2021)
Comitè Europeu de les Regions (CDR)	Dictamen del CDR sobre la proposta de la AI Act (02.12.2021)
Banc Central Europeu	Propostes de redacció en relació amb la proposta de la AI Act (29.12.2021)

Negociació trileg entre la Comissió Europea, el Consell de la UE i el Parlament Europeu

- [Text proposat](#) (20.06.2023)
- [Anàlisi del text amb perspectiva d'acord](#) (26.01.2024)
- [Acord provisional fruit de les negociacions institucionals](#) (02.02.2024)
- [Esmenes del Parlament Europeu a la proposta de la Comissió](#) (06.03.2024)
- [Correccions al text](#) (19.04.2024)

Cronologia

2021

21 d'abril	La Comissió Europea publica la proposta de regulació sobre la intel·ligència artificial a la Unió Europea.
20 de juliol	El president d'Eslovènia al Consell de la Unió Europea organitza una conferència virtual per a discutir la regulació sobre la IA, ètica i drets fonamentals.
6 d'agost	Finalitza el període de consulta pública sobre la AI Act donat per la Comissió Europea. La Comissió va rebre 304 propostes. Les podeu llegir en aquest enllaç.
29 de novembre	Es publica l'estudi que analitza l'ús de tècniques biomèdiques amb una perspectiva ètica i jurídica encarregada pel Departament de Polítiques de Drets de la ciutadania i Afers constitucionals del Parlament Europeu.
1 de desembre	A causa de la Presidència rotatòria del Consell de la UE es comparteix el primer compromís de l'esborrany del text de la AI Act amb importants canvis als àmbits de puntuació social, sistemes de reconeixement biomètric i les aplicacions d'alt risc.
	Les comissions del Mercat Interior i Protecció del Consumidor (IMCO) i la de Llibertats Civils, Justícia i Afers Socials (LIBE) del Parlament Europeu dirigiran conjuntament les negociacions sobre la AI Act .

2022	
25 de gener	Les principals comissions del Parlament Europeu, la de Mercat Interior i Protecció del Consumidor (IMCO) i la de Llibertats Civils, Justícia i Afers Socials (LIBE) van celebrar el primer intercanvi de punts de vista sobre la Proposta de la AI Act .
2 de febrer	La Comissió Europea va presentar una nova Estratègia de Normalització on proposava el seu plantejament per a promoure els valors del mercat únic resistent, ecològic i digital d'escala mundial.
3 de febrer	La Presidència francesa al Consell Europeu difon el text sobre els articles 16 a 29 de la Proposta de la AI Act sobre les obligacions de les persones usuàries i proveïdores als sistemes d'alt risc. Així com, el compromís sobre els articles 40 a 52 sobre les normes harmonitzadores, les avaluacions de conformitat i les obligacions de transparència per a determinats sistemes de la IA.
2 de març	Les comissions associades sobre Qüestions Jurídiques (JURI) i la d'Indústria, Recerca i Energia (ITER) publiquen l'esborrany de les seves opinions respectives a la AI Act .
20 d'abril	Els membres del Parlament Europeu que dirigeixen la AI Act a la comissió del Mercat Intern i Protecció del Consumidor (IMCO) i a la de Llibertats Civils, Justícia i Afers Socials (LIBE) publiquen l'esborrany de les seves opinions respectives a la AI Act .
13 de maig	La Presidència francesa al Consell Europeu publica el text de l'article 4 bis sobre la regulació dels sistemes d'IA de propòsit general els quals són capaços de dur a terme un ampli ventall de tasques (comprendre imatges i veu, generar àudio i vídeos, detectar patrons, respondre preguntes i traduir textos).
1 de juny	Data límit per als grups polítics del Parlament Europeu per a presentar esmenes a la AI Act . En total s'hi van presentar milers d'esmenes les quals es resumeixen breument en el següent enllaç .
15 de juny	La Presidència francesa al Consell Europeu publica el seu últim text abans del canvi de presidència.
17 de juny	La Presidència Txeca al Consell Europeu comparteix una discussió amb els Caps d'Estat dels estats membres de la UE indicant llurs prioritats a la AI Act .
5 de setembre	La comissió sobre Qüestions Jurídiques (JURI) al Parlament Europeu publica l'esborrany de les seves opinions respectives a la AI Act .
28 de setembre	La Comissió Europea va proposar l'harmonització específica de les normes internes en matèria de responsabilitat per la IA amb l'objectiu de complementar la IA Act facilitant les reclamacions de Responsabilitat civil per danys i perjudicis.
6 de desembre	El Consell de la UE adopta la seva posició a la AI Act .
2023	
14 de juny	El Parlament Europeu adopta la seva posició negociadora sobre la AI Act amb 499 vots a favor, 28 vots en contra i 93 abstencions.

9 de desembre	El Parlament Europeu i el Consell de la UE adopten l'acord provisional sobre la AI Act .
2024	
13 de febrer	A les comissions del Mercat Interior i Protecció del Consumidor (IMCO) i la de Llibertats Civils, Justícia i Afers Socials (LIBE) el resultat de la votació va ser 71 a favor, 8 vots en contra i 7 abstencions per tal d'aprovar el resultat de les negociacions amb els estats membres sobre la AI Act .
21 de febrer	L'Oficina Europea de Intel·ligència artificial es va crear en el si de la Comissió Europea depenent de la Direcció General de Xarxes de Comunicació, continguts, tecnologia per a donar suport a la implementació de la AI Act , especialment per als sistemes de propòsit general.
21 de maig	El Consell Europeu adopta formalment la Llei d'IA de la UE.

Terminis d'aplicació

2024	
12 de juliol	Publicació al Diari Oficial de la UE de la IA Act.
1 d'agost	La Llei entra en vigor 20 dies després de la seva publicació. A partir d'aquesta data, el desplegament es fa segons l'article 113.
2025	
2 de febrer	S'aplicaran els capítols I i II (prohibicions sobre la IA de risc inacceptable).
2 de maig	cal que els codis de pràctiques estiguin preparats d'acord amb l'article 56.
2 d'agost	s'aplicaran el capítol III Secció 4 (autoritats notificadores), el capítol V (models d'IA d'ús general), el capítol VII (governança), el capítol XII (confidencialitat i sancions) i l'article 78 (confidencialitat), amb l'excepció de l'article 101 (que fa referència a les multes per a les persones proveïdores dels models d'IA d'ús general).
2026	
2 d'agost	s'aplicarà la resta de la Llei d'IA, exceptuant l'article 6.1, relatiu als sistemes d'IA d'alt risc enumerats a l'Annex I de la AI Act .
2027	
2 d'agost	s'aplicarà l'article 6.1 i les obligacions corresponents als sistemes d'alt risc inclosos en l'Annex I de la AI Act .

Altres dates rellevants

2024	
24 de gener	La decisió de la Comissió de crear una Oficina d'Intel·ligència Artificial de la UE. Comunicació sobre l'impuls a les empreses emergents i la innovació en IA fiable. La proposta de modificació del EuroHPC (Reglament (UE) 2021/1173) per tal de crear fàbriques d'IA.
16 d'abril	Informe especial del Tribunal de Comptes Europeu que fiscalitza el «Pla coordinat sobre IA» de la Comissió Europea de 2018 i 2021.
19 de juny	Se celebra la primera reunió d'alt nivell de la pròxima Junta d'IA per adoptar el reglament intern i crear grups de treball per a preguntes específiques relacionades amb l'aplicació de la AI Act .
16 de juliol	Declaració de l'EDPB sobre el paper de les Autoritats de Protecció de Dades en el marc de la AI Act
22 de juliol	Convocatòria de manifestacions d'interès per participar en l'elaboració del primer Codi de Bones Pràctiques dels models d'IA d'ús general. Llançament d'una consulta multilateral sobre tals models fiables en el marc de la AI Act .
12 de setembre	Primera reunió del Comitè de la IA.
2 de novembre	Final del termini on els estats membres han hagut de notificar a les autoritats responsables la protecció dels drets fonamentals (previst a l'article 77.2 de la AI Act).
2025	
2 de maig	Finalització de la redacció del codi de bones pràctiques per als models d'IA d'ús general.

ANNEX VI: AI LIABILITY DIRECTIVE

Proposta de Directiva del Parlament Europeu i del Consell relativa a l'adaptació de les normes de responsabilitat civil extracontractual a la intel·ligència artificial.

La AI Liability Directive:

El 28 de setembre de 2022 la Comissió va publicar la [Proposta de directiva del Parlament Europeu i del Consell relativa a l'adaptació de les normes de responsabilitat civil extracontractual a la intel·ligència artificial](#) (AI Liability Directive).

En tractar-se encara d'una proposta legislativa, en aquests moments no és possible saber quan es publicarà o entrarà en vigor.

Objectiu:

La AI Liability Directive tindrà com a objectiu establir normes que permetran determinar qui serà responsable dels danys i perjudicis derivats d'un sistema d'IA en aquells casos en els quals aquesta qüestió no s'hagués previst prèviament en un contracte. D'aquesta manera, es crearà un règim de responsabilitat uniforme amb el que es pretén millorar el funcionament del mercat interior europeu.

Aquesta regulació podria ser útil, per exemple, en cas que el sistema d'IA que utilitza l'empresa de gestió de residus d'una ciutat per planificar la recollida d'escombraries no fos suficient precisa amb la regularitat en què cal buidar els contenidors d'un carrer, causant molèsties les persones que hi viuen.

Relació amb la AI Act:

La directiva funcionarà de manera complementària a la **AI Act**, ja que la AI Liability Directive es remet a les obligacions contingudes a la **AI Act** per tal d'identificar com a presumptes culpables dels danys i perjudicis denunciats els subjectes sobre els quals s'imposen aquestes normes.

Cal esmentar que, si bé la **AI Act** es tracta d'un reglament europeu i, per tant, és aplicable des del moment en què es va publicar al Diari Oficial de la UE, la AI Liability Directive és una directiva europea. En conseqüència, fins i tot quan s'hagi aprovat i publicat el DOUE, el seu contingut no serà exigible en un territori fins que l'estat hagi creat una norma pròpia transposant el seu contingut.

Contingut:

ATENCIÓ! La proposta de directiva va ser publicada amb anterioritat a l'adopció definitiva de la AI Act. En conseqüència, diversos dels articles de la AI Act als que la AI Liability Directive fa referència han patit canvis en la seva numeració. Per tal de facilitar la consulta d'ambdós documents, el contingut d'aquest annex ha estat adaptat de manera que fem menció de la numeració definitiva de la AI Act, per la qual cosa és possible trobar diferències respecte al text original de la proposta de directiva.

Normes respecte a l'exhibició de proves:

Un problema freqüent en relació amb els perjudicis causats pels sistemes d'IA, és demostrar la relació amb l'ús del sistema i el dany produït, ja que aquestes proves sovint només estan en possessió dels responsables finals de la IA. A més, els òrgans judicials no sempre tenen el coneixement i les facultats necessàries per saber com tractar i valorar-les.

Per això l'article 3 de la directiva conté les següents normes en relació amb l'exhibició d'aquestes proves:

- Els estats han de vetllar perquè els seus òrgans judicials estiguin facultats per ordenar a la persona proveïdora, usuària o altres subjectes a les obligacions de la **AI Act** que aportin proves sobre el sistema d'IA (art. 3.1).
- Aquesta ordre ha de ser sol·licitada per la persona que formula la demanda, qui haurà de recolzar la petició en fets i proves suficients sobre el perjudici causat pel sistema (art.3.1).
- L'òrgan jurisdiccional només podrà ordenar l'exhibició de proves als subjectes esmentats si la persona que interposa la demanda ja ha intentat obtenir-les de la part demandada prèviament (art. 3.2)
- Els òrgans jurisdiccional hauran d'estar facultats per conserva les proves en qüestió (art. 3.3).
- L'exhibició de les proves i les mesures per a la seva conservació s'hauran de limitar a aquelles que siguin necessàries per al desenvolupament del procediment judicial i proporcionades respecte als interessos legítims de cada part (art. 3.4).
- En cas que la part demandada incompleixi l'ordre de l'òrgan judicial en relació amb l'exhibició o conservació de les proves, es presumirà que, d'haver-se exhibit, aquestes haguessin corroborat els fets demandats i, per tant, que la demandada és culpable dels danys i perjudicis causats. No obstant, la demandada podrà intentar demostrar la seva innocència amb altres mitjans.

Normes respecte a la presumpció de culpa:

A causa de l'autonomia de la qual gaudeixen tots els sistemes d'IA, sigui en major o menor grau, pot ser complicat identificar als possibles responsables dels danys i perjudicis derivats del seu ús.

Per aquest motiu, l'AI Liability Act indica a l'article 4 que la responsabilitat per incidents relacionats amb l'ús de sistemes d'IA recau sobre aquells subjectes que han actuat de manera negligent en el seu desenvolupament, implementació o ús. A tals efectes, la proposta de directiva es remet a la **AI Act** i determina que es considerarà negligent l'incompliment dels requisits legals contemplats a aquesta norma per part dels subjectes que hi estan obligats al seu compliment, com per exemple les persones proveïdores.

En aquest sentit, l'article 4.1 de la AI Liability Act disposa que es presumirà que la part demandada és culpable dels danys i perjudicis demandats quan es compleixin una sèrie de requisits. Al mateix temps, els punts 2 i 3 del mateix precepte preveuen criteris específics perquè es consideri complert el primer dels requisits en relació amb els proveïdors i usuaris de sistemes d'alt risc.

Els requisits esmentats són els següents:

- 1) La persona que ha interposat la demanda ha de demostrar que el demandat, o algú sota la seva responsabilitat, ha incomplert un deure de diligència establert per l'**AI Act** o altres lleis. O bé els tribunals han de poder inferir aquesta circumstància (art. 4.1.a).
 - Quan la demanda s'interposa contra la persona proveïdora d'un sistema d'IA d'alt risc, o contra una altra que estigui subjecta a les mateixes obligacions, qui interposi la demanda haurà de demostrar que s'han incomplert els requisits continguts als articles 10 (dades i governança de dades), 13 (transparència), 14 (vigilància humana) i 15 (precisió, robustesa i cibeseuretat) de la **AI Act** (art. 4.2).
 - Quan la demanda s'interposa contra la persona usuària d'un sistema d'IA d'alt risc, qui interposi la demanda haurà de demostrar que la demandada no va complir amb les obligacions de l'article 26.1, 2 i 4 de la **AI Act** (utilitzar o supervisar el sistema de conformitat amb les instruccions d'ús adjuntes i evitar exposar el sistema a dades d'entrada sota el seu control que no siguin adequades per a la seva finalitat prevista) (art. 4.3).
- 2) Ha de ser raonablement probable que la negligència hagi influït en els resultats del sistema d'IA, o en la seva manca de resultats (art. 4.1.b).
- 3) La persona que ha interposat la demanda ha de demostrar que els danys i perjudicis van ser causats pels resultats produïts o no produïts pel sistema d'IA (art. 4.1.c).

Aquesta presumpció de culpa només ha d'aplicar-se en aquells supòsits en els quals la persona que presenta la demanda li sigui impossible o massa difícil demostrar la culpabilitat de les persones sobre les quals s'imposen les obligacions de la **AI Act**.

En conseqüència, l'article 4 de la AI preveu les següents excepcions a la presumpció de culpa:

- En relació amb els sistemes d'alt risc, la presumpció no s'aplicarà quan la persona demandada demostri que qui ha interposat la demanda pot accedir raonablement a

proves i coneixements especialitzats suficients per demostrar que els danys i perjudicis han estat causats per la demandada.

- En relació amb sistema d'IA que no siguin d'alt risc, la presumpció només s'aplicarà si l'òrgan judicial considera excessivament complicat per a la part demandant demostrar que els danys i perjudicis han estat causats a conseqüència del comportament de la persona demandada.
- Quan la demanda s'interposi contra algú que no ha utilitzat el sistema per a portar a terme una activitat professional, la presumpció únicament s'aplicarà quan el demandat hagi interferit substancialment en les condicions de funcionament del sistema d'IA o quan el demandat tingués l'obligació i estigués en condicions de determinar les condicions de funcionament del sistema d'IA i no ho hagi fet.

Antecedents legislatius

Textos aprovats per:

La Comissió Europea

[Llibre blanc sobre intel·ligència artificial. Una mirada europea de l'excel·lència i la confiança](#) (19.02.2020)

[Informe de la Comissió al Parlament Europeu, al Consell i al Comitè Econòmic i Social Europeu. Informe sobre les implicacions de seguretat i responsabilitat de la IA, la internet de les coses i la robòtica](#) (19.02.2020)

[Avaluació d'impacte que acompanya la proposta d'una AI Liability Directive](#) (28.09.2022)

El Parlament Europeu

[Projecte d'informe de la Comissió d'Affers Jurídics del Parlament amb recomanacions a la Comissió Europea sobre un règim de responsabilitat civil per a la IA](#) (28.09.2020)

[Resolució del Parlament Europeu amb recomanacions a la Comissió sobre un règim de responsabilitat civil per a la intel·ligència artificial](#) (20.10.2020)

Altres institucions de la UE o òrgans consultius

Comitè Econòmic i Social Europeu

[Dictamen del CESE: Directiva sobre responsabilitat per intel·ligència artificial](#) (25.01.2023)

ANNEX VII: AVALUACIÓ DE CONFORMITAT.

La **AI Act** exigeix que les persones proveïdores dels sistemes d'alt risc sotmetin la seva IA a una avaluació de conformitat (art.16). Aquesta consisteix a demostrar que el sistema en qüestió compleix amb els requisits que li són imposats per la **AI Act**.

La regulació preveu diferents modalitats d'avaluació en funció de la finalitat prevista del sistema d'alt risc.

1. Procediment d'avaluació intern contemplat a l'annex VI de la AI Act.

Quins sistemes han de ser sotmesos a aquesta avaluació?

- Sistemes de categorització o d'identificació biomètrica i de reconeixement d'emocions.
- Sistemes utilitzats en infraestructures crítiques.
- Sistemes utilitzats en l'àmbit de l'educació i formació professional.
- Sistemes utilitzats en l'àmbit de l'ocupació, gestió dels treballadors i accés a l'autoocupació.
- Sistemes utilitzats en l'àmbit de l'accés i gaudi de serveis i prestacions essencials (públiques o privades).
- Sistemes utilitzats en l'àmbit del compliment de la llei.
- Sistemes utilitzats en l'àmbit de la migració, l'asil i el control de fronteres.
- Sistemes utilitzats en l'àmbit de l'administració de justícia i processos democràtics.

Com funciona aquest procediment?

Es tracta d'una avaluació interna, és a dir, que la porta a terme la persona proveïdora del sistema, en la qual s'hauran de verificar els següents aspectes:

- Que s'ha establert un sistema de gestió de qualitat que compleix amb els requisits de l'art. 17 de la **AI Act**.
- Que s'ha examinat que la informació continguda en la documentació tècnica compleix amb els requisits aplicables als sistemes d'alt risc.
- Que el disseny i el procés de desenvolupament del sistema, així com el seu monitoratge de postcomercialització, és coherent amb la informació continguda en la documentació tècnica.

2. Procediment d'avaluació extern, basat en l'avaluació del sistema de gestió de la qualitat i de la documentació tècnica, amb la participació d'un organisme notificat, contemplat a l'annex VII de la AI Act.

Quins sistemes han de ser sotmesos a aquesta avaluació?

Aquesta modalitat d'avaluació és obligatòria respecte als sistemes de categorització o d'identificació biomètrica i de reconeixement d'emocions quan es doni alguna de les següents circumstàncies:

- Quan la Unió Europea no hagi creat normes harmonitzades o especificacions comunes aplicables.
- Quan aquestes normes harmonitzades o especificacions comunes si existeixen, però la persona proveïdora no les ha aplicat.
- Quan alguna les normes harmonitzades a què es refereix la lletra a) s'hagi publicat amb una restricció (és a dir, que no cobreixen tots els elements que han de ser objecte d'avaluació), les qüestions a les quals es refereix la restricció han de ser sotmeses a aquesta opció d'avaluació.

Tot i que no concorrin les circumstàncies anteriors, les persones proveïdores dels sistemes de categorització o d'identificació biomètrica i reconeixement d'emocions poden sotmetre's voluntàriament a aquest procediment d'avaluació de manera alternativa al procediment intern previst a l'annex VI si així ho desitgen.

Com funciona aquest procediment?

L'avaluació la portarà a terme un organisme extern anomenat organisme notificat. Aquests es tracten d'organitzacions independents de les persones proveïdores, designades per l'autoritat competent de cada estat membre, per tal de portar a terme tasques d'avaluació.

L'avaluació de conformitat constarà de les següents parts:

- Avaluació del sistema de gestió de qualitat:
 - La persona proveïdora ha d'enviar una sol·licitud d'avaluació del sistema de gestió de qualitat del seu sistema a l'organisme notificat de la seva elecció.
 - La sol·licitud ha d'incloure la informació detallada al punt 3 de l'annex VII de la **AI Act**.
 - L'organisme notificat enviarà a la persona proveïdora una notificació amb les conclusions de l'avaluació i la seva decisió justificada.
 - Qualsevol canvi previst per al sistema de gestió de qualitat ha de ser informat l'organisme notificat, qui haurà de decidir si el sistema continua complint amb els requisits legals o si ha de ser reavaluat.
- Control de la documentació tècnica:
 - La persona proveïdora ha d'enviar una sol·licitud d'avaluació de la documentació tècnica del sistema a l'organisme notificat de la seva elecció.
 - La sol·licitud ha d'incloure la informació detallada al punt 4 de l'annex VII de la **AI Act**.
 - L'organisme notificat pot exigir l'accés complet a les dades de formació, validació i proves utilitzades i/o demanar proves addicionals. Si aquests mitjans són insuficients, també pot sol·licitar accés als models de formació del sistema com a últim recurs.
 - L'organisme notificat enviarà les conclusions de l'avaluació i la seva decisió justificada.
 - Si l'avaluació se supera positivament, l'organisme notificat emetrà un certificat.
 - Qualsevol canvi que pugui afectar el compliment dels requisits legals o la finalitat prevista del sistema ha de ser informat a l'organisme notificat, el qual haurà de decidir si el sistema ha de ser reavaluat o si és possible abordar els canvis de manera aïllada. En aquest últim cas, l'organisme emetrà un suplement al certificat.
- Vigilància del sistema de gestió de qualitat aprovat:
 - Un cop aprovat el sistema de gestió de qualitat l'organisme notificat vigilarà que aquest és degudament aplicat.
 - La persona proveïdora ha de permetre que l'organisme notificat accedeixi a les instal·lacions on es dissenya, desenvolupa i prova el sistema i compartirà tota la informació necessària.
 - L'organisme notificat realitzarà auditories periòdiques i lliurarà a la persona proveïdora els informes que en siguin resultants. Com a part d'aquestes auditories l'organisme notificat pot portar a terme proves addicionals.

3. Procediment d'avaluació específic per a alguns sistemes:

Quins sistemes han de ser sotmesos a aquesta avaluació?

Sistemes subjectes per les regulacions enumerades a l'annex I, secció A, de la **AI Act**. Aquests comprenen:

- Joguines;
- Embarcacions d'esbarjo i motos d'aigua;
- Ascensors;
- Equips i sistemes de protecció utilitzats en atmosferes potencialment explosives.
- Equips radioelèctrics;
- Equips a pressió;
- Instal·lacions de telefèric;
- Equips de protecció individual, aparells de protecció de combustibles gasosos;
- Productes sanitaris i de diagnòstic *in vitro*;
- Màquines que coincideixen amb la definició de la directiva 2006/42/CE).

Com funciona aquest procediment?

- Els sistemes d'IA hauran de ser sotmesos a les avaluacions de conformitat que es preveuen a les regulacions enumerades a l'annex I, secció A, de la **AI Act** (les que han estat esmentades anteriorment) a les que estiguin subjectes.
- En portar a terme les avaluacions esmentades, serà necessari incorporar l'examen del compliment de les obligacions que la **AI Act** imposa als sistemes d'IA d'alt risc. En alguns casos, els organismes que tinguin la condició d'organismes notificats en virtut dels actes jurídics esmentats podran portar a terme aquesta part de l'avaluació, per a adquirir la condició d'organismes notificats s'hagin tingut en compte alguns requisits contemplats a l'art. 31 de la **AI Act**.
- Així mateix, com a part de l'avaluació de conformitat també s'haurà de portar a terme el control de la documentació tècnica que forma part del procediment d'avaluació extern descrit a l'annex VII de la **AI Act** (i que ha estat explicat en el punt anterior).
- En els casos en què aquestes altres regles permetin a la persona proveïdora no sotmetre's a l'avaluació externa, la persona proveïdora també pot optar per aquesta opció en relació amb les normes de la **AI Act**, sempre que la Unió Europea hagi creat normes harmonitzades relatives a aquestes qüestions i que la persona proveïdora les hagi aplicat.

Independentment del procediment aplicable, en cas que el sistema sigui modificat substancialment després d'haver aprovat l'avaluació caldrà que sigui sotmès a una nova avaluació de conformitat.

A aquests efectes no suposarà una modificació substancial els canvis dels sistemes que continuen aprenent després del seu desplegament, sempre que aquests hagin estat predeterminats abans de l'avaluació de conformitat inicial i es contemplin en la documentació tècnica.

ANNEX VIII: AVALUACIÓ D'IMPACTE SOBRE DRETS FONAMENTALS.

L'article 27 de la **AI Act** exigeix que, prèviament al seu desplegament, alguns sistemes siguin sotmesos a una avaluació sobre l'impacte que el seu ús pot suposar per als drets fonamentals.

Aquesta avaluació serà obligatòria en els següents casos:

- Quan un organisme públic o un organisme privat que presta serveis públics desplegui un sistema d'IA destinat a algun dels següents àmbits:
 - Identificació o categorització biomètrica i reconeixement d'emocions.
 - Educació i formació professional.
 - Ocupació, gestió dels treballadors i accés a l'autoocupació.
 - Accés i gaudi de serveis i prestacions essencials (públiques o privades).
 - Compliment de la llei.
 - Migració, asil i control de fronteres.
 - Administració de justícia i processos democràtics.
- En tot cas, quan es desplegui un sistema d'IA destinat a alguna de les següents finalitats:
 - Avaluar la solvència de les persones físiques o establir la seva puntuació creditícia, amb l'excepció dels sistemes d'IA utilitzats amb la finalitat de detectar frau financers.
 - Avaluar els riscos i la fixació de preus en relació amb persones físiques en el cas d'assegurances de vida i salut.

L'avaluació d'impacte sobre drets fonamentals ha d'incloure els següents aspectes:

- Una descripció dels processos en què el desplegador utilitzarà el sistema d'IA d'acord amb la finalitat prevista d'aquest.
- Una descripció del període de temps i freqüència en què es pretén utilitzar el sistema.
- Les categories de persones físiques i grups susceptibles de veure's afectats per la utilització del sistema en el context específic en el qual serà utilitzat.
- Els riscos específics de dany susceptibles d'afectar les categories de persones o grups de persones identificades.
- Una descripció de les mesures de supervisió humana que seran aplicades d'acord amb les instruccions d'ús del sistema.
- Les mesures que es preveu adoptar en cas de materialització d'aquests riscos, inclosos els mecanismes de govern intern i denúncia.
- Quan alguns dels elements mencionats també sigui objecte de l'avaluació d'impacte relativa a la protecció de dades establerta a l'article 35 del Reglament (UE) 2016/679 o l'article 27 de la Directiva (UE) 2016/680, ambdues avaluacions es realitzaran de manera conjunta.

Un cop realitzada l'avaluació, caldrà omplir el formulari que serà desenvolupat per l'Oficina d'IA de la UE (encara no disponible). Aquest haurà de ser remès a l'autoritat de vigilància de mercat competent.

L'avaluació només s'ha de portar a terme abans d'utilitzar el sistema per primer cop. Les posteriors vegades en què es vulgui fer servir el sistema en circumstàncies similars és possible basar-se en les avaluacions dutes a terme prèviament o, fins i tot, aquelles que poden haver estat realitzades per la persona proveïdora.

En cas de produir-se algun canvi que afecti les qüestions avaluades, serà necessari actualitzar la informació.

ANNEX IX: OBLIGACIONS DE TRANSPARÈNCIA.

Entre les moltes regles establertes per la **AI Act**, s'estableixen obligacions de transparència que estan disperses entre l'articulat de la regulació i els seus annexos.

Per facilitar la comprensió d'aquests requisits, us deixem un esquema que sintetitza les normes de transparència establertes per la llei.

Obligacions de transparència per als sistemes d'alt risc:

D'acord amb l'article 13, els sistemes d'alt risc han de ser dissenyats i desenvolupats de manera que el seu funcionament sigui prou transparent per permetre als desplejadors interpretar els seus resultats i utilitzar-ho correctament.

Amb aquest propòsit, i amb la finalitat de complir els requisits que la **AI Act** preveu per als sistemes d'alt risc, els sistemes han d'anar acompanyats de la documentació tècnica prevista a l'article 11 i l'annex IV de la llei. Dins d'aquesta documentació tècnica s'inclouen les instruccions d'ús del sistema. De manera sintètica, el contingut mínim exigint per aquests documents és el següent:

- Una descripció general del sistema. Aquesta inclou:
 - La identitat i les dades de contacte de la persona proveïdora i del seu representant autoritzat, si n'hi ha.
 - La descripció de la versió del sistema que reflecteixi la seva relació amb versions anteriors;
 - Informació que permeti als desplejadors interpretar les respostes del sistema i usar-la adequadament.
 - Els recursos computacionals i de maquinari necessaris, la vida útil prevista del sistema d'IA d'alt risc i qualsevol mesura de manteniment i cura necessària per garantir el bon funcionament del sistema.
 - Una descripció dels mecanismes inclosos en el sistema IA que permeti a les persones usuàries recollir, emmagatzemar i interpretar correctament els registres del seu funcionament.
 - Com el sistema pot interactuar amb maquinari o programari que no formen part del mateix sistema d'IA.
 - Les versions del programari o microprogramari rellevants i qualsevol requisit relacionat amb l'actualització de la versió.
 - La descripció de totes les formes en què el sistema d'IA es posa al mercat o es posa en servei.
 - Quan el sistema d'IA sigui un component de productes, fotografies o il·lustracions que mostrin característiques externes, marcatge i disposició interna d'aquests productes.
- Una descripció detallada dels elements del sistema d'IA i del procés per al seu desenvolupament. Aquesta inclou:
 - Els mètodes i passos realitzats per al desenvolupament del sistema d'IA, incloent-hi si s'han utilitzat altres sistemes prèviament entrenats.
 - La descripció del disseny del sistema, això inclou la lògica general del sistema d'IA i dels algorismes, i les eleccions clau de disseny.
 - La descripció de l'arquitectura del sistema.

- Fitxes que descriguin les metodologies i tècniques d'entrenament i els conjunts de dades d'entrenament utilitzats, inclosa una descripció general d'aquests conjunts de dades, informació sobre la seva procedència, abast, tractament i característiques principals.
 - Avaluació de les mesures de supervisió humana previstes.
 - Els canvis del sistema que hagin estat predeterminats per la persona proveïdora en el moment de l'avaluació de la conformitat inicial, si escau.
 - Els procediments de validació i assaig utilitzats, inclosa informació sobre les dades de validació i assaig utilitzades, les mètriques utilitzades per mesurar la precisió i la robustesa, així com els impactes potencialment discriminatoris.
 - Els registres de proves i tots els informes de proves datats i signats per les persones responsables.
 - Mesures de ciberseguretat implantades.
- Informació sobre el seguiment, funcionament i control del sistema. Aquesta inclou:
 - Les seves capacitats i limitacions i el grau de precisió previst, tan global com per a persones o grups de persones específics.
 - Els resultats no desitjats previsibles i les fonts de riscos per a la salut i la seguretat, els drets fonamentals i la discriminació d'acord amb la seva finalitat prevista.
 - Especificacions sobre les dades d'entrada.
 - Una descripció detallada del sistema de gestió de riscos.
 - Una descripció dels canvis rellevants fets per la persona proveïdora al sistema al llarg del seu cicle de vida.
 - Una llista de les normes harmonitzades publicades al Diari Oficial de la UE aplicades, les solucions adoptades per complir els requisits establerts a la **AI Act**, i una llista d'altres normes i especificacions tècniques pertinents aplicades.
 - Una còpia de la declaració de conformitat UE.
 - Una descripció detallada del sistema de vigilància postcomercialització adoptat.

Obligacions de transparència per als models de propòsit general:

A part de les obligacions contemplades per als sistemes d'alt risc, la **AI Act** preveu unes obligacions de transparència determinades per als sistemes de propòsit general en els articles 50 a 53 i els annexos XI i XII. És possible que un sistema de propòsit general també reuneixi les característiques per ser considerat d'alt risc. En aquest cas, resultarien aplicables tant les obligacions previstes per als sistemes d'alt risc com aquelles únicament plantejades per als sistemes de propòsit general.

Les obligacions de transparència dels models de propòsit general són les següents:

- Els sistemes que interactuïn amb persones físiques s’han de dissenyar i desenvolupar de manera que les persones siguin informades que estan interactuant amb una d’IA.
- Les sortides dels sistemes que generin contingut sintètic d’àudio, imatge, vídeo o text, han d’estar marcades en un format llegible per màquina i detectables com a generades o manipulades artificialment.
- Els desplegadors de sistemes que generin o manipulin contingut d’imatge, àudio o vídeo que constitueixi un *deepfake*, han de revelar que el contingut ha estat generat o manipulat artificialment.
- Si la IA es tracta d’un sistema de reconeixement d’emocions o categorització biomètrica, s’haurà d’informar a les persones físiques exposades al mateix del seu funcionament.
- Els desplegadors d’un sistema d’IA que generi o manipuli text que es publica amb la finalitat d’informar el públic sobre qüestions d’interès públic han de revelar que el text ha estat generat o manipulat per una IA. Aquesta obligació no s’aplicarà quan el contingut hagi estat sotmès a un procés de revisió humana o control editorial, sempre que s’hagi determinat qui és la persona responsable del contingut publicat.
- Elaborar i posar a disposició del públic un resum prou detallat sobre el contingut utilitzat per a la formació del model d’IA de propòsit general, d’acord amb una plantilla proporcionada per l’Oficina d’IA (encara no disponible).
- Elaborar i mantenir actualitzada la **documentació tècnica del model**, que contindrà com a mínim els següents elements:
 - Una descripció general del model. Aquesta inclou:
 - Les tasques que pretén realitzar el model i el tipus i naturalesa dels sistemes d’IA en què es pot integrar.
 - Les polítiques d’ús acceptable aplicables.
 - La data de llançament i els mètodes de distribució.
 - L’arquitectura i el nombre de paràmetres.
 - La modalitat i el format de les entrades i sortides (textos, imatges, etc).
 - La llicència.
 - Una descripció detallada dels elements del model i informació rellevant del procés per al seu desenvolupament. Aquesta inclou:
 - Els mitjans tècnics necessaris perquè el model s’integri a altres sistemes d’IA.
 - Les especificacions de disseny del model i del procés de formació.
 - Informació sobre les dades utilitzades per a la formació, les proves i la validació del model, a més de la seva procedència, el tractament al qual han estat sotmeses, les característiques principals i els mètodes aplicats per identificar biaixos.
 - Els recursos computacionals utilitzats per entrenar el model.
 - El consum energètic conegut o estimat del model.

- Quan el model hagi de ser classificat com a un model de propòsit general de risc sistèmic d'acord amb l'article 51 de la **AI Act**, s'haurà d'aportar la següent informació addicional:
 - Una descripció detallada de les estratègies d'avaluació utilitzades per identificar i mitigar els possibles riscos sistèmics originats per l'ús del model.
 - Una descripció de les mesures adoptades per portar a terme proves contradictòries (internes o externes) així com l'adaptació i ajustament de model.
- Elaborar i posar a disposició de les persones proveïdores **que pretenguin integrar el model de propòsit general en el seu sistema d'IA documentació i informació** la qual inclourà, com a mínim, el següent contingut:
 - Una descripció general del model d'IA de propòsit general. Aquesta inclou:
 - Les tasques que es pretén realitzar el model i el tipus i naturalesa dels sistemes d'IA en què es pot integrar.
 - Les polítiques d'ús acceptable aplicables.
 - La data de llançament i els mètodes de distribució.
 - Com el model interactua o es pot utilitzar per interactuar amb maquinari o programari que no forma part del propi model.
 - Les versions del programari rellevant relacionades amb l'ús del model d'IA de propòsit general.
 - L'arquitectura i nombre de paràmetres.
 - La modalitat i el format de les entrades i sortides (textos, imatges, etc).
 - La llicència del model.
 - Una descripció dels elements del model i del procés per al seu desenvolupament. Aquesta inclou:
 - Els mitjans tècnics necessaris perquè el model s'integri altres sistemes d'IA.
 - La modalitat i format de les entrades i sortides i la seva mida màxima (textos, imatges, etc).
 - Informació sobre les dades utilitzades per a la formació, proves i validació, incloent-hi el tipus i la procedència de les dades i com aquestes han estat tractades.

ANNEX X: SUBJECTES CONTEMPLATS PER LA AI ACT.

Subjectes en l'ús de la IA segons la **AI Act**.

A l'article 3 de la **AI Act** fa el recull de les definicions dels conceptes destacats com a prioritaris de conèixer que intervenen al llarg de tot el text normatiu, i és concretament l'apartat 3 a 8 que defineix els subjectes.

PERSONA	ARTICLE	DEFINICIÓ
Proveïdora	3.3	Persona física o jurídica, administració pública, organisme o un altre cos que desenvolupen sistemes d'IA el comercialitza o el posa en servei amb la seva pròpia marca o nom, sigui de pagament o gratuït.
Desplegadora	3.4	Persona física o jurídica, administració pública, organisme o un altre cos que utilitza un sistema d'IA, excepte si s'usa per a desenvolupar una activitat no professional.
Representat autoritzada	3.5	Persona física o jurídica nacional o resident a la UE que ha rebut o acceptat un mandat escrit d'una persona proveïdora d'un sistema d'IA per tal que efectui i dui a terme en llur nom les obligacions i procediments establerts per la llei.
Importadora	3.6	Persona física o jurídica nacional o resident a la UE que comercialitza al mercat un sistema d'IA amb el nom o la marca comercial d'una altre persona física o jurídica nacional o resident d'un tercer país.
Distribuïdora	3.7	Persona física o jurídica de la cadena de subministrament, diferent de la persona proveïdora o importadora, que comercialitza un sistema d'IA al mercat de la UE.
Operadora	3.8	La suma de les figures anteriors, es a dir, persona proveïdora, fabricant de productes, despelgadora, representant autoritzada, implementada o distribuïdora. Concepte en general per aglutinar tots els subjectes.

ANNEX XI: 50 EXEMPLES DE L'APLICACIÓ DE LA AI ACT.

1	Una empresa del sector de la salut utilitza una aplicació propulsada per IA per al triatge de pacients.
2	Una empresa implementa un sistema de vigilància amb càmeres dotades de reconeixement facial per a la seguretat de les seves instal·lacions.
3	Una institució pública utilitza tecnologia de reconeixement de veu per analitzar la prioritat en l'atenció de trucades telefòniques.
4	Una institució educativa utilitza un sistema d'IA per fer seguiment del rendiment acadèmic dels estudiants i predir possibles abandonaments.
5	Un hospital utilitza un sistema d'IA per analitzar imatges mèdiques i ajudar en el diagnòstic de malalties.
6	Un centre de salut utilitza un sistema de IA per a la gestió de les cites i l'organització de les llistes d'espera.
7	Una oficina de serveis socials utilitza IA per identificar famílies amb risc de patir situacions de vulnerabilitat i oferir suport proactiu.
8	Una empresa utilitza IA per a la selecció de personal, analitzant els currículums dels candidats i predir el seu rendiment potencial.
9	Un banc utilitza IA per analitzar les sol·licituds de crèdit i avaluar la solvència dels sol·licitants.
10	Una asseguradora utilitza IA per avaluar les quotes mensuals a pagar per la persona que contracta una assegurança de vida.
11	Una empresa d'energia utilitza IA per predir possibles incidències en el subministrament d'electricitat.
12	Una empresa de transport disposa de camions que compten amb un sistema de conducció automàtica.
13	Un sistema d'IA que s'utilitza per identificar l'autenticitat dels documents utilitzats com a prova en el marc de la investigació d'un delicte.
14	Una les autoritats ferroviàries de dos països fronterers utilitzen un sistema IA per optimitzar la programació dels trens i gestionar el trànsit transfronterer.
15	Una empresa de transport instal·la un sistema IA en els seus vehicles per optimitzar les rutes de lliurament i reduir els temps de transport.

16	Una universitat utilitza IA per analitzar les dades d'inscripció i determinar els criteris d'accés per al futur curs acadèmic.
17	Una empresa que es dedica als serveis jurídics utilitza <i>ChatGPT</i> o <i>Copilot</i> per redactar la documentació relativa a les sol·licituds de residència dels seus clients i analitzar les probabilitats de que aquestes prosperin.
18	Una empresa utilitza un sistema biomètric per al control d'accés a les seves oficines, basat en empremtes digitals.
19	Una organització d'ajuda humanitària contracta un model d'IA de propòsit general per analitzar les necessitats de les comunitats afectades per desastres naturals i planificar la distribució d'ajuda.
20	Una empresa utilitza un model d'IA de propòsit general per personalitzar la publicitat en línia basant-se en el comportament de navegació dels usuaris.
21	Una empresa proporciona als seus empleats un servei de <i>ChatGPT</i> per generar correus electrònics i altres textos.
22	Una empresa ha desenvolupat una eina d'imatges sintètiques basada en un LLM i l'utilitza per generar imatges pels seus documents de treball.
23	Una empresa compta amb un <i>chatbot</i> al seu lloc web per a respondre a consultes generals sobre l'empresa.
24	Una institució pública utilitza un model de propòsit general per predir aglomeracions com manifestacions o actes similars basant-se en dades de xarxes socials.
25	Una plataforma de comerç electrònic utilitza IA proveïda per una bigtech entrenada amb conjunts de dades massius per recomanar productes als clients basant-se en les seves preferències de compra.
26	Una empresa utilitza un sistema d'IA que genera propostes de contractes personalitzats.
27	Una empresa de logística utilitza una IA amb grans conjunts de dades per predir els colls d'ampolla en la cadena de subministrament i evitar retards.
28	Una empresa de telecomunicacions utilitza IA per optimitzar la xarxa, millorar la qualitat del servei i executar autònomament modificacions en el subministrament individual dels seus clients.
29	Un servei meteorològic utilitza IA per a fer prediccions del temps i alertar a autònomament a la població sobre fenòmens meteorològics extrems i elaborar informes.
30	Una empresa d'energia d'abast nacional utilitza IA per predir la demanda, optimitzar la distribució d'electricitat i analitzar els hàbits de consum de la seva clientela.

31	Una empresa d'arquitectura utilitza IA per generar dissenys innovadors basant-se en les preferències dels clients i les tendències del mercat.
32	En un sistema de rec de conreus s'instal·la una IA de propòsit general perquè determini la quantitat d'aigua necessària i la freqüència de rec en funció de les condicions meteorològiques i l'estació de l'any.
33	Una clínica veterinària encarrega una IA entrenada amb les seves pròpies dades per a diagnosticar malalties en animals de companyia basant-se en els símptomes descrits pels propietaris.
34	Una empresa implementa sensors intel·ligents a les seves fàbriques i magatzem per a controlar el seu estoc.
35	Una farmàcia utilitza IA per gestionar les existències de medicaments i advertir quan quedin poques unitats d'un.
36	Un supermercat utilitza IA per analitzar els patrons de compra dels clients i optimitzar l'inventari.
37	Un restaurant ha adquirit una d'IA entrenada amb les seves dades històriques per analitzar les preferències dels clients i ajustar el menú segons la demanda.
38	Una biblioteca utilitza IA per gestionar el catàleg de llibres i ordenar el catàleg de lectures situant les més sol·licitades en primer lloc.
39	Un servei meteorològic utilitza IA per crear un recull de precipitacions durant tot el segle passat en una zona geogràfica concreta.
40	Una empresa que fabrica llibretes utilitza IA per detectar defectes en la producció i millorar la qualitat dels productes.
41	Una empresa alimentària utilitza IA per controlar la qualitat dels productes durant el procés de producció.
42	Un restaurant ha adquirit una d'IA entrenada amb les seves dades històriques per analitzar les preferències dels clients i ajustar el menú segons la demanda.
43	Una empresa utilitza un sistema d'IA per filtrar els correus que rep i detectar els que contenen comentaris negatius sobre la seva marca per després fer millores.
44	Una empresa de recursos humans utilitza IA per analitzar les dades de satisfacció dels empleats i millorar l'ambient laboral.
45	Una empresa utilitza un sistema d'IA que organitza automàticament els seus fitxers electrònics

46	Un sistema d'IA que corregeixi activitats de càlcul mental de l'alumnat.
47	Una piscina municipal utilitza una IA per regular el nivell de clor i la temperatura de l'aigua.
48	En un hivernacle s'instal·la un sistema d'IA que activa el rec quan detecta una baixada de la humitat.
49	Una casa de turisme rural utilitza un sistema d'IA per a regular la temperatura interior en relació amb la temperatura exterior i si està llogada.
50	Una perruqueria utilitza un sistema d'IA per a preveure l'estoc de colors de tints segons la demanda de la seva clientela cada mes.

ANNEX XII: PREGUNTES FREQUENTS (FAQ).

Quina és la relació de la AI Act amb els drets humans?

L'arribada de la IA pot entrar en conflicte amb els drets humans i llur tutela en diversos textos normatius i és per això que fem èmfasi en que l'ús ha de ser ètic i d'acord als drets fonamentals de totes les persones.

Els sistemes d'IA no poden estar exempts de respectar els consensos socials assolits al voltant dels drets mínims garantits per a tothom, sinó al contrari, s'ha de promoure que l'aplicació de la IA sigui adequada i d'acord aquets. I no només en la seva creació, sinó també durant totes les seves fases i ús.

Per això diem que la relació entre la **AI Act** i els drets humans és estreta i de cooperació perquè són la base d'un bon funcionament dels sistemes d'IA.

Quan entra en vigor la AI Act?

La **AI Act** va entrar en vigor el passat dia 1 d'agost de 2024, vint dies després de la seva publicació al Diari Oficial de la UE el 12 de juliol.

Això no obstant, no totes les obligacions contingudes a la norma són ja exigibles, sinó que l'article 113 de la **AI Act** preveu diferents terminis per algunes seccions, amb l'objectiu de brindar als subjectes de temps per adaptar-se als requisits previstos.

És per aquest motiu que les normes relatives a les pràctiques prohibides no seran aplicables fins al 2 de febrer del 2025. Les disposicions relacionades amb els sistemes d'IA generativa, de categorització biomètrica, de reconeixement d'emocions, i models de propòsit general seran exigibles a partir del 2 d'agost del 2025.

Pel que fa a les normes aplicables als sistemes d'alt risc, seran exigibles a partir del 2 d'agost del 2026 per als sistemes inclosos en l'Annex III de la **AI Act** (sistemes relatius a àmbits d'especial incidència sobre els drets fonamentals, com per exemple la salut), i a partir del 2 d'agost del 2027 respecte als sistemes enumerats a l'Annex I (sistemes ja coberts per la regulació sobre productes de la UE).

És aconsellable complir amb la AI Act encara que el meu sistema no estigui contemplat?

Si, és aconsellable que, fins i tot si el vostre sistema no estigui contemplat de manera expressa a la **AI Act**, heu d'adoptar mesures per tal de complir amb els estàndards que en ella mateixa es contemplen. Cal tenir en compte que la normativa contigua a la **AI Act** també funciona com una adequació als paràmetres ètics i que, per tant, permeten avançar en l'anomenada IA ètica i responsable.

Així mateix, cal notar que la categorització de sistemes que contempla la versió actual de la **AI Act** no és hermètica, sinó que la mateixa llei atribueix a la Comissió la potestat per incloure més tipus

de sistemes a les categories establertes. En conseqüència, que el vostre sistema actualment no estigui afectat per la legislació no implica que no pugui estar-ho en un futur. Així doncs, començar a treballar en el compliment dels requisits de la **AI Act** us pot aportar seguretat de cara a qualsevol possible canvi en la legislació.

Quines són les categories de risc definides segons la AI Act?

La **AI Act** classifica els sistemes d'IA en 4 categories de risc: 1) sistemes de risc inacceptable, on se situen els sistemes destinats als usos prohibits per l'article 5 de la **AI Act**; 2) sistemes d'alt risc, enumerats a l'article 6 de la **AI Act**, que són considerats com a tal perquè es considera que el seu ús pot suposar un perill per als drets i llibertats fonamentals, la salut i seguretat de les persones, el medi ambient i/o la democràcia i l'estat de dret; 3) sistemes de risc limitat, categoria en la qual s'encabeixen diversos tipus de sistemes amb relació als quals es preveuen determinades obligacions de transparència; i 4) sistemes de risc mínim, els quals no són considerats potencialment perillosos, motiu pel qual la normativa pràcticament no els contempla.

Quines són les possibles sancions si no es compleix la AI Act?

Les possibles sancions davant l'incompliment de la **AI Act** es contemplen en el capítol XII de la regulació. La infracció de les normes relatives als usos prohibits establertes a l'article 5 de la legislació pot comportar una multa administrativa de fins a 35.000.000 euros, o el 7% de la facturació global si aquesta darrera xifra és més elevada. Pel que fa a l'incompliment dels requisits establerts per als sistemes d'alt risc o les obligacions de transparència en relació amb els sistemes d'IA generativa, categorització biomètrica, reconeixement d'emocions a aquests pot comportar una multa de fins a 15.000.000 euros, o el 3% de la facturació, de nou, depenent de si aquesta segona xifra és més elevada que la primera.

Així mateix, la **AI Act** contempla la possibilitat d'imposar multes de fins a un 3% de la facturació global, o 15.000.000 euros, segons quina sigui la xifra més alta, als proveïdors de models de propòsit general que, de manera intencional o negligent, infringeixin la regulació.

Quina normativa regula la IA?

La **AI Act** és la normativa europea que introdueix un marc regulador i legal comú sobre intel·ligència artificial per a tots els estats membres de la UE però, no n'és la única.

Així doncs, destaquem que en els següents textos legals també consta regulació en matèria de la IA: la AI Liability Directive; la Directiva sobre els requisits d'accessibilitat dels productes i serveis; la Directiva sobre l'accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic; la Directiva de protecció de dades amb fins de prevenció, investigació, detecció, enjudiciament o execució d'infraccions penals; la Directiva dels drets d'autor i drets afins en la societat de la informació; la Directiva sobre els drets d'autor i drets afins en el mercat únic digital; la Llei Europea sobre la Governança de dades; el Reglament general de protecció de dades; i el Reglament de protecció de dades tractades per institucions, òrgans i organismes de la Unió.

Tot això sense incloure les recomanacions ètiques i les legals, pel que us encoratgem a utilitzar el **Model PIO** per anar a l'avançada i actuar de manera coherent amb els requisits legals i estàndards ètics esperats.

