

2024/1689

12.7.2024

REGLAMENT (UE) 2024/1689 DEL PARLAMENT EUROPEU I DEL CONSELL de 13 de juny de 2024

pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial i pel qual es modifiquen els reglaments (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 i les directives 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Llei d'intel·ligència artificial)

(Text rellevant als efectes de l'EEE)

(Traducció no oficial al català del text oficial publicat en anglès al DOUE L 2024/1689 de 12.07.2024)

EL PARLAMENT EUROPEU I EL CONSELL DE LA UNIÓ EUROPEA,

Atès el Tractat de funcionament de la Unió Europea i, en particular, els articles 16 i 114,

Atesa la proposta de la Comissió Europea,

Havent-se tramès prèviament el projecte d'acte legislatiu als parlaments nacionals,

Atès el dictamen del Comitè Econòmic i Social Europeu [\(1\)](#),

Atès el dictamen del Banc Central Europeu [\(2\)](#),

Atès el dictamen del Comitè de les Regions [\(3\)](#),

actuant d'acord amb el procediment legislatiu ordinari [\(4\)](#),

Considerant el següent:

(1) El Reglament té per objectiu la millora del funcionament del mercat interior mitjançant l'establiment d'un marc jurídic uniforme; en particular, per desenvolupar, introduir en el mercat, posar en servei i fer servir sistemes d'intel·ligència artificial (d'ara endavant, "sistemes d'IA") a la Unió, de conformitat amb els valors de la Unió, per promoure l'adopció d'una intel·ligència artificial (IA), centrada en l'ésser humà i fiable, tot garantint un nivell de protecció alt de la salut, la seguretat i els drets fonamentals que es consagren en la Carta dels Drets Humans Fonamentals de la Unió Europea (d'ara endavant, "Carta"), en què s'inclouen la democràcia, l'estat de dret i la protecció del medi ambient, protegir davant els efectes perjudicials dels sistemes d'IA a la Unió i contribuir a la innovació. El present Reglament garanteix la lliure circulació, transfronterera, de mercaderies i serveis basats en la IA, i així impedeix que els estats membres imposin restriccions al desenvolupament, la comercialització i l'ús de sistemes d'IA, tret que el present Reglament ho autoritzi de manera explícita.

(2) El Reglament s'ha d'aplicar de conformitat amb els valors de la Unió que es consagren a la Carta, amb la qual cosa es facilita la protecció de les persones físiques i les empreses, la democràcia, l'estat de dret i el medi ambient; alhora, s'impulsen la innovació i l'ocupació i es converteix la Unió en líder en l'adopció d'una intel·ligència artificial fiable.

(3) Els sistemes d'IA es poden desplegar fàcilment en una gran varietat de sectors de l'economia i en moltes parts de la societat, incloent-hi l'altra banda de les fronteres, i poden circular fàcilment arreu de la Unió. Hi ha estats membres que ja han explorat l'adopció de normes nacionals destinades a assegurar que la IA sigui fiable i segura i es desenvolupi i faci servir d'acord amb les obligacions relatives als drets fonamentals. La divergència entre les normes nacionals pot conduir a la fragmentació del mercat interior i pot disminuir la seguretat jurídica dels operadors que desenvolupen, importen o utilitzen sistemes d'IA. Per tant, cal garantir un nivell elevat i coherent de protecció a tota la Unió per aconseguir una IA fiable, i també evitar les divergències que obstaculitzen la lliure circulació, la innovació, el desplegament i l'adopció en el mercat interior dels sistemes d'IA i els productes i serveis connexos mitjançant l'establiment d'obligacions uniformes per als operadors i la garantia d'una protecció uniforme dels fins imperiosos d'interès general i dels drets de les persones en tot el mercat interior, sobre la base de l'article 114 del Tractat de Funcionament de la Unió Europea (TFUE). En la mesura que el present Reglament conté normes específiques per a la protecció de les persones en relació amb el tractament de dades personals que restringeixen l'ús de sistemes d'IA per a la identificació biomètrica remota amb finalitats de garantia del compliment de la llei, l'ús de sistemes d'IA per a la pràctica d'avaluacions de riscos de persones físiques amb finalitats de garantia del compliment de la llei i l'ús de sistemes d'IA de categorització biomètrica amb finalitats de garantia del compliment de la llei, pel que fa a aquestes normes específiques, resulta adequat basar aquest Reglament en l'article 16 del TFUE. A la llum d'aquestes normes específiques i del recurs a l'article 16 del TFUE, convé consultar el Comitè Europeu de Protecció de Dades.

(4) La IA és un conjunt de tecnologies en ràpida evolució que contribueix a generar beneficis econòmics, mediambientals i socials molt diversos en tots els sectors econòmics i les activitats socials. En millorar la predicció, optimitzar les operacions i l'assignació dels recursos, i personalitzar les solucions digitals que hi ha a disposició de la població i les organitzacions, l'ús de la IA pot proporcionar avantatges competitius essencials a les empreses i facilitar l'obtenció de resultats positius des del punt de vista social i mediambiental en els àmbits de l'assistència sanitària, l'agricultura, la seguretat alimentària, l'educació i la formació, els mitjans de comunicació, l'esport, la cultura, la gestió d'infraestructures, l'energia, el transport i la logística, els serveis públics, la seguretat, la justícia, l'eficiència dels recursos i l'energia, el seguiment ambiental, la conservació i restauració de la biodiversitat i els ecosistemes, i la mitigació del canvi climàtic i l'adaptació a aquest, entre d'altres.

(5) Alhora, en funció de les circumstàncies relatives a l'aplicació, l'ús i el nivell de desenvolupament tecnològic, la IA pot generar riscos i perjudicar els interessos públics i els drets fonamentals que la legislació de la Unió protegeix. El perjudici pot ser tangible o intangible, i inclou danys físics, psicològics, socials o econòmics.

(6) Ateses la importància de les repercussions que la IA pot tenir en la societat i la necessitat de generar confiança, és fonamental que la IA i el mar que la reguli es desenvolupin d'acord amb els valors de la Unió que es consagren en l'article 2 del Tractat de la Unió Europea (TUE), els drets i les llibertats fonamentals consagrats en els Tractats i, de conformitat amb l'article 6 del TUE, la Carta. Com a requisit previ, la IA ha de ser una tecnologia centrada en l'ésser humà. A més, ha de servir com a eina per a les persones i tenir com a objectiu últim augmentar el benestar humà.

(7) Cal establir normes comunes per als sistemes d'IA d'alt risc i així garantir un nivell alt i coherent de protecció dels interessos públics pel que fa a la salut, la seguretat i els drets fonamentals. Les normes que s'estableixin han de ser coherents amb la Carta, no discriminatòries i conformes amb els compromisos comercials que la Unió ha assumit en matèria comercial. Les normes també han de tenir en compte la Declaració Europea sobre els Drets i Principis Digitals per a la Dècada Digital i les Directrius ètiques para a una IA fiable del Grup independent d'experts d'alt nivell sobre intel·ligència artificial (AI HLEG).

(8) Cal, per tant, un marc jurídic de la Unió per impulsar el desenvolupament, l'ús i l'adopció al mercat interior de la IA i que, alhora, ofereixi un nivell alt de protecció dels interessos públics, com ara la salut i la seguretat i la protecció dels drets fonamentals, inclosos la democràcia, l'estat de dret i la protecció del medi ambient, que el dret de la Unió reconeix i protegeix. L'assoliment de l'objectiu esmentat requereix que hi hagi normes que regulin la introducció en el mercat, la posada en servei i l'ús de determinats sistemes d'IA, i així assegurar el bon funcionament del mercat interior i permetre que aquests sistemes es beneficiïn del principi de la lliure circulació de béns i serveis. Les normes han de ser clares i robustes pel que fa a protegir els drets fonamentals, donar suport a solucions innovadores noves, fer possible un ecosistema europeu d'agents públics i privats que creïn sistemes d'IA en consonància amb els valors de la Unió i alliberar el potencial de la transformació digital en totes les regions de la Unió. En establir aquestes normes, i també mesures de suport a la innovació que se centren especialment en les empreses petites i mitjanes (pimes), incloses les empreses emergents, el Reglament avala l'objectiu de promoure l'enfocament europeu de la IA centrat en l'ésser humà i de ser un líder mundial en el desenvolupament d'IA segura, digna de confiança i ètica, tal com indica el Consell Europeu [\(5\)](#), i garanteix la protecció dels principis ètics, tal com sol·licita específicament el Parlament Europeu [\(6\)](#).

(9) Són necessàries normes harmonitzades aplicables a la introducció en el mercat, la posada en servei i l'ús de sistemes d'IA d'alt risc en consonància amb el Reglament (CE) 765/2008 del Parlament Europeu i del Consell [\(7\)](#), la Decisió 768/2008/CE del Parlament Europeu i del Consell [\(8\)](#) i el Reglament (UE) 2019/1020 del Parlament Europeu i del Consell [\(9\)](#) (d'ara endavant, "nou marc legislatiu"). Les normes harmonitzades que s'estableixen en el Reglament s'han d'aplicar a tots els sectors i, en coherència amb el nou marc legislatiu, s'han d'entendre sense perjudici del dret vigent de la Unió, en particular en matèria de protecció de dades, protecció dels consumidors, drets fonamentals, ocupació, protecció dels treballadors i seguretat dels productes, el qual el Reglament complementa. Per tant, la

totalitat dels drets i remeis previstos pel dret de la Unió a favor dels consumidors i altres persones que es poden veure afectades negativament per la IA, la qual cosa inclou la compensació per possibles danys d'acord amb la Directiva 85/374/CEE [\(10\)](#) del Consell romanen sense afectació i són plenament aplicables. A més, en el context de l'ocupació i la protecció dels treballadors, el present Reglament no ha d'afectar, per tant, el Dret de la Unió en matèria de política social ni el Dret laboral nacional —de conformitat amb el Dret de la Unió— relativa a les condicions d'ocupació i de treball, incloses la salut i seguretat en el treball i la relació entre ocupadors i treballadors. El present Reglament tampoc no ha d'afectar l'exercici dels drets fonamentals reconeguts dins els estats membres i a escala de la Unió, inclosos el dret o la llibertat de vaga o d'emprendre altres accions cobertes pels sistemes específics de relacions laborals dels estats membres, ni el dret a negociar, concloure i fer complir acords col·lectius o emprendre accions col·lectives d'acord amb la legislació nacional. El Reglament no ha d'afectar les disposicions adreçades a millorar les condicions laborals en la feina en plataformes digitals establertes en una directiva del Parlament Europeu i del Consell relativa a la millora de les condicions laborals en el treball en plataformes digitals. A més, el Reglament té per objectiu enfortir l'eficàcia dels drets i recursos existents esmentats mitjançant l'establiment de requisits i obligacions específics, fins i tot pel que fa a la transparència, la documentació tècnica i el manteniment de registres dels sistemes d'IA. A més, les obligacions que s'imposen als diversos operadors que participen en la cadena de valor de la IA en virtut del Reglament s'han d'aplicar sense perjudici del dret nacional que, de conformitat amb el dret de la Unió, tingui per objecte limitar l'ús de determinats sistemes d'IA quan aquest dret quedi fora de l'àmbit d'aplicació del Reglament o vulgui assolir objectius d'interès públic diferents dels que el Reglament mateix vol assolir. Així, per exemple, el present Reglament no pot afectar el dret laboral nacional ni el dret en matèria de protecció de menors, és a dir, de persones menors de divuit anys, que tenen en compte l'Observació general 25 (2021) de la Convenció sobre els drets dels infants de les Nacions Unides relatives als drets dels infants en relació amb l'entorn digital, en la mesura en què no són específiques dels sistemes d'IA i persegueixen altres objectius legítims d'interès públic.

(10) El dret fonamental a la protecció de dades personals està protegit, en particular, pels reglaments (UE) 2016/679 [\(11\)](#) i (UE) 2018/1725 [\(12\)](#) del Parlament Europeu i del Consell i la Directiva (UE) 2016/680 del Parlament Europeu del Consell [\(13\)](#). La Directiva 2002/58/CE del Parlament Europeu i del Consell [\(14\)](#) protegeix la vida privada i la confidencialitat de les comunicacions, també establint condicions per a l'emmagatzematge de dades personals i no personals en els equips terminals i l'accés des dels equips mateixos. Aquests actes legislatius de la Unió constitueixen la base per a un tractament de dades sostenible i responsable, també quan els conjunts de dades contenen una combinació de dades personals i no personals. El present Reglament no vol afectar l'aplicació del dret de la Unió vigent que regula el tractament de dades personals, incloses les funcions i les competències de les autoritats de supervisió independents competents per vigilar que els instruments esmentats s'acompleixin. Tampoc no afecta les obligacions de proveïdors i responsables del desplegament de sistemes d'IA en el paper de responsables o encarregats del tractament de dades que deriven del dret de la Unió o del dret nacional en matèria de protecció de dades personals en la mesura en què el disseny, el desenvolupament o l'ús de sistemes d'IA impliquen el tractament de dades personals. També cal aclarir que els interessats continuen gaudint de tots els drets i garanties que el dret de la Unió els confereix, inclosos els drets relacionats amb les decisions individuals totalment automatitzades, com ara l'elaboració de

perfils. Unes normes harmonitzades per a la introducció en el mercat, la posada en servei i l'ús de sistemes d'IA establertes en virtut del present Reglament han de facilitar l'aplicació efectiva i permetre l'exercici dels drets i altres vies de recurs dels interessats garantits pel Dret de la Unió en matèria de protecció de dades personals i, també, d'altres drets fonamentals.

(11) El present Reglament s'ha d'interpretar sense perjudici de les disposicions relatives a la responsabilitat dels proveïdors de serveis intermediaris previstes en el Reglament (UE) 2022/2065 del Parlament Europeu i del Consell [\(15\)](#).

(12) Cal definir de manera clara el concepte de “sistema d'IA” en el present Reglament, i harmonitzar-lo estretament amb la tasca de les organitzacions internacionals que treballen en la IA, per garantir la seguretat jurídica i facilitar la convergència a escala internacional i una àmplia acceptació, alhora que es preveu la flexibilitat necessària per encabir els ràpids avenços tecnològics en aquest àmbit. A més, la definició s'ha de basar en les característiques principals dels sistemes d'IA que els distingeixen dels sistemes de programari o els plantejaments de programació tradicionals i més senzills, i no ha d'incloure els sistemes basats en normes definides únicament per persones físiques per permetre l'execució automàtica d'operacions. Una característica principal dels sistemes d'IA és la capacitat d'inferència. Té a veure amb el procés d'obtenció de resultats de sortida, com prediccions, continguts, recomanacions o decisions, que pot influir en entorns físics i virtuals, i amb la capacitat dels sistemes d'IA per deduir models o algorismes, o ambdós, a partir d'informació d'entrada o dades. Les tècniques que permeten la inferència en construir un sistema d'IA inclouen estratègies d'aprenentatge automàtic que aprenen de les dades com es poden assolir determinats objectius i estratègies basats en la lògica i el coneixement que infereixen a partir de coneixements codificats o d'una representació simbòlica de la tasca per resoldre. En permetre l'aprenentatge, el raonament o la modelització, la capacitat d'inferència d'un sistema d'IA va més enllà del tractament de dades bàsic. El terme “basat en màquina” té a veure amb el fet que els sistemes d'IA s'executen en màquines. La referència a objectius explícits o implícits subratlla que els sistemes d'IA poden funcionar d'acord amb objectius explícits definits o implícits. Els objectius del sistema d'IA poden diferir de l'objectiu perseguit pel sistema d'IA en un context específic. Als efectes del present Reglament, s'ha d'entendre que els entorns són els contextos en què els sistemes d'IA funcionen, mentre que els resultats de sortida generats pel sistema d'IA reflecteixen diferents funcions fetes pels sistemes d'IA i inclouen prediccions, continguts, recomanacions o decisions. Els sistemes d'IA estan dissenyats per funcionar amb diferents nivells d'autonomia, i això vol dir que poden actuar amb cert grau d'independència en relació amb l'actuació humana i que tenen capacitats per funcionar sense intervenció humana. La capacitat d'adaptació que un sistema d'IA pot mostrar després que s'hagi desplegat té a veure amb les capacitats d'autoaprenentatge que permeten que el sistema canviï mentre se n'està fent ús. Els sistemes d'IA es poden fer servir de manera independent o com a components d'un producte, amb independència de si el sistema forma part físicament del producte (integrat) o contribueix a la funcionalitat del producte sense formar-ne part (no integrat).

- (13) El concepte de «responsable del desplegament» a què el present Reglament fa referència s'ha d'interpretar com qualsevol persona física o jurídica, inclosa qualsevol autoritat pública, òrgan o organisme, que utilitzi un sistema d'IA sota l'autoritat pròpia, excepte quan l'ús s'emmarqui en una activitat personal de caràcter no professional. En funció del tipus, l'ús del sistema d'IA pot afectar persones diferents del responsable del desplegament.
- (14) El concepte “dades biomètriques” que s'empra en el Reglament s'ha d'interpretar tenint en present la definició que del concepte mateix s'ofereix a l'article 4, punt 14, del Reglament (UE) 2016/679, a l'article 3, punt 18, del Reglament (UE) 2018/1725, i a l'article 3, punt 13, de la Directiva (UE) 2016/680. Les dades biomètriques poden permetre l'autenticació, identificació o classificació de les persones físiques i reconèixer-ne les emocions.
- (15) El concepte “identificació biomètrica” a què el present Reglament es refereix s'ha de definir com el reconeixement automatitzat de trets físics, fisiològics i conductuals humans; per exemple, el posat de la cara, el moviment dels ulls, la forma del cos, la veu, l'entonació, la forma de caminar, la postura, la freqüència cardíaca, la pressió arterial, l'olor o les característiques de les pulsacions de tecla, per determinar la identitat d'una persona comparant-ne les dades biomètriques amb les dades biomètriques de persones emmagatzemades en una base de dades de referència, amb independència de si la persona en qüestió hi ha consentit o no. Se n'exclouen els sistemes d'IA destinats a la verificació biomètrica, que inclou l'autenticació i que té com a única finalitat confirmar que una persona física en particular és qui diu que és, i també confirmar-ne la identitat amb la finalitat exclusiva que accedeixi a un servei, desbloquegi un dispositiu o tingui accés segur a un local.
- (16) El concepte “categorització biomètrica” a què el present Reglament es refereix s'ha de definir com a la inclusió de persones físiques en categories específiques segons les seves dades biomètriques. Es tracta de categories específiques que poden tenir a veure amb aspectes com ara sexe, edat, color d'ulls, color de cabells, tatuatges, trets conductuals o de personalitat, idioma, religió, pertinença a una minoria nacional, orientació sexual o tendència política. No inclou els sistemes de classificació biomètrica que siguin una funció merament accessòria vinculada intrínsecament amb un altre servei comercial, la qual cosa vol dir que, per raons tècniques objectives, la característica no es pot fer servir sense el servei principal i integrar-la no és un mitjà per eludir l'aplicabilitat de disposicions del present Reglament. Per exemple, els filtres que classifiquen les característiques facials o corporals emprades en els mercats en línia podrien constituir una característica accessòria d'aquesta mena, ja que només se'n pot fer ús en relació amb el servei principal, que consisteix a vendre un producte, permetre al consumidor previsualitzar com li quedaria i ajudar-lo a prendre una decisió de compra. Els filtres que es fan servir en els serveis de xarxes socials que classifiquen les característiques facials o corporals perquè els usuaris puguin afegir imatges o vídeos o modificar-ne també es podrien considerar una característica accessòria, ja que són filtres que no es poden fer servir sense el servei principal de les xarxes socials, que consisteix a compartir continguts en línia.

(17) El concepte “sistema d'identificació biomètrica remota” a què el Reglament es refereix s'ha de definir funcionalment, com un sistema d'IA destinat a identificar persones físiques sense que hi participin de manera activa, normalment a distància, comparant les dades biomètriques d'una persona amb les dades biomètriques contingudes en una base de dades de referència, independent de la tecnologia, els processos o els tipus de dades biomètriques utilitzats. Aquests sistemes d'identificació biomètrica remota se solen fer servir per percebre múltiples persones o el seu comportament alhora, per facilitar de manera significativa la identificació de persones físiques sense que hi participin activament. En queden exclosos els sistemes d'IA que tenen per finalitat la verificació biomètrica, incloent-hi l'autenticació, que té com a objectiu únic confirmar que una persona física en concret és la persona que diu que és i confirmar-ne la identitat per a l'objectiu únic de tenir accés a un servei, desbloquejar un dispositiu o tenir accés a instal·lacions de seguretat. L'exclusió es justifica per la probabilitat que aquests sistemes tinguin una repercussió menor en els drets fonamentals de les persones físiques que els sistemes d'identificació biomètrica de què es faci ús per al tractament de les dades biomètriques d'un gran nombre de persones sense que aquestes hi participin de manera activa. En el cas dels sistemes “en temps real”, la captura de les dades biomètriques, la comparació i la identificació es produeixen de forma instantània, gairebé instantània o, en qualsevol cas, sense un retard significatiu. Així, cal no deixar marge a la possibilitat d'eludir les normes previstes en el present Reglament en relació amb l'ús “en temps real” dels sistemes d'IA de què es tracti generant retards mínims. Els sistemes “en temps real” comporten l'ús de material “en viu” o “gairebé en viu”, com ara imatges de vídeo, generades per una càmera o un altre dispositiu amb funcionalitat similar. En canvi, pel que fa als sistemes “en diferit”, les dades biomètriques ja han estat capturades i la comparació i la identificació només tenen lloc després d'un retard significatiu. Per a aquesta finalitat, es fan servir materials, com ara imatges o enregistraments de vídeo captats per càmeres de televisió de circuit tancat o dispositius privats, generats abans de l'ús del sistema en relació amb les persones físiques afectades.

(18) El concepte “sistema de reconeixement d'emocions” a què el present Reglament es refereix s'ha de definir com un sistema d'IA destinat a identificar o deduir emocions o intencions de les persones físiques a partir de les seves dades biomètriques. Té a veure amb emocions o intencions com ara felicitat, tristor, indignació, sorpresa, fàstic, mal tràngol, entusiasme, vergonya, menyspreu, satisfacció i divertiment. No inclou el dolor o la fatiga o altres estats físics, incloent-hi, per exemple, sistemes emprats per detectar el cansament dels pilots o conductors professionals per evitar accidents. Tampoc no inclou la mera detecció d'expressions, gestos o moviments que es considerin obvis, tret que se'n faci ús per identificar emocions o inferir-ne. Es pot tractar d'expressions facials bàsiques; per exemple, un nas arrufat o un somriure; gestos, com ara el moviment de mans, braços o cap, o característiques de la veu d'una persona; com ara el to alt o un xiuxiueig.

(19) Als efectes del present Reglament, s'ha d'entendre que el concepte d'«espai d'accés públic» es refereix a qualsevol espai físic al qual pugui accedir un nombre indeterminat de persones físiques i amb independència de si és de propietat privada o pública i de l'activitat per a la qual es pugui utilitzar l'espai, ja siguin activitats comercials, per exemple, botigues, restaurants, cafeteries; de prestació de serveis, per exemple, bancs, activitats professionals, hostaleria; esportives, per exemple, piscines, gimnasos, estadis; de transport, per exemple,

estacions d'autobús, metro i ferrocarril, aeroports, mitjans de transport; d'entreteniment, per exemple, cinemes, teatres, museus, sales de concerts, sales de conferències; d'oci o d'un altre tipus, per exemple, vies i places públiques, parcs, boscos, parcs infantils. Un espai també s'ha de classificar com a accessible al públic si, independentment de la capacitat o les restriccions de seguretat, l'accés està subjecte a certes condicions predeterminades que un nombre indeterminat de persones pot complir, com ara la compra d'un bitllet o títol de transport, el registre previ o tenir una certa edat. Per contra, un espai no s'ha de considerar d'accés públic si únicament hi poden accedir determinades persones físiques definides, ja sigui en virtut del Dret de la Unió o del Dret nacional directament relacionat amb la seguretat pública o en virtut d'una clara manifestació de voluntat de la persona que exerceixi l'autoritat competent sobre l'espai. Per si sola, la possibilitat real d'accés, com una porta no tancada amb clau o una reixa oberta, no implica que l'espai sigui d'accés públic si hi ha indicis o circumstàncies que suggereixin el contrari, com ara senyals que prohibeixin o restringeixin l'accés. Els locals d'empreses i fàbriques, i també les oficines i els llocs de treball a què només han de poder accedir membres del personal i proveïdors autoritzats, no són espais d'accés públic. No s'han d'incloure en els espais d'accés públic les presons ni les zones en què es fan inspeccions frontereres. Hi ha espais que poden incloure tant zones que són d'accés públic com zones que no en són; per exemple, els aeroports o el vestíbul d'un edifici residencial privat pel qual s'accedeix a una consulta mèdica. Com que no són espais físics, els espais en línia no s'hi inclouen. Tanmateix, cal determinar, cas per cas, si un espai és d'accés públic o no ho és tenint en compte les particularitats de la situació concreta.

(20) Per obtenir els beneficis màxims dels sistemes d'IA, sense deixar de protegir els drets fonamentals, la salut i la seguretat, per possibilitar el control democràtic, l'alfabetització en matèria d'IA ha de dotar proveïdors, responsables del desplegament i persones afectades dels conceptes necessaris per prendre decisions amb coneixement de causa en relació amb els sistemes d'IA. Són conceptes que poden variar en funció del context de què es tracti i incloure la comprensió de l'aplicació correcta dels elements tècnics durant la fase de desenvolupament del sistema d'IA, les mesures que s'han d'aplicar mentre se'n fa ús, les formes adequades d'interpretar els resultats de sortida del sistema d'IA i, pel que fa a les persones afectades, els coneixements necessaris per entendre la forma en què les decisions que s'adopten amb l'ajuda de la IA les afectaran. En el context de l'aplicació del present Reglament, l'alfabetització en IA ha de proporcionar a tots els actors rellevants de la cadena de valor de la IA els coneixements necessaris per garantir el compliment adequat i l'execució correcta. A més, l'aplicació general de mesures d'alfabetització en IA i la introducció d'accions de seguiment adequades podrien contribuir a millorar les condicions de treball i, en darrer terme, a sostenir la consolidació i la via d'innovació d'una IA fiable a la Unió. El Consell Europeu d'Intel·ligència Artificial ("Consell") ha de contribuir a fer que la Comissió pugui promoure les eines d'alfabetització en matèria d'IA, la sensibilització pública i la comprensió dels avantatges, els riscos, les salvaguardes, els drets i les obligacions en relació amb l'ús de sistemes d'IA. En cooperació amb les parts interessades pertinents, la Comissió i els estats membres han de facilitar l'elaboració de codis voluntaris de conducta per avançar en l'alfabetització en matèria d'IA entre les persones que treballen en el desenvolupament, el funcionament i l'ús de la IA.

(21) Per garantir la igualtat de condicions i la protecció efectiva dels drets i les llibertats de les persones arreu de la Unió, les normes establertes en el present Reglament s'han d'aplicar als proveïdors de sistemes d'IA sense discriminació, amb independència de si estan establerts a la Unió o en un tercer país i, també, als responsables del desplegament de sistemes d'IA establerts a la Unió.

(22) Atès el caràcter digital, hi ha sistemes d'IA que han d'entrar en l'àmbit d'aplicació del present Reglament encara que no s'introdueixin en el mercat, es posin en servei ni es facin servir a la Unió. És el cas, per exemple, quan un operador establert a la Unió signa, amb un operador establert en un tercer país, un contracte per a la prestació de determinats serveis en relació amb una activitat que es durà a terme per un sistema d'IA que es consideraria d'alt risc. En les circumstàncies descrites, el sistema d'IA emprat en un tercer país per l'operador podria tractar les dades obtingudes lícitament a la Unió i transferides des del seu territori, i proporcionar a l'operador contractant situat a la Unió els resultats de sortida generats pel sistema d'IA que resultin del tractament sense que el sistema d'IA de què es tracti s'introdueixi al mercat, es posi en servei o es faci servir a la Unió. Per evitar-ne l'elusió i garantir una protecció efectiva de les persones físiques ubicades a la Unió, el present Reglament també s'ha d'aplicar a proveïdors i responsables del desplegament de sistemes d'IA establerts en un tercer país, en la mesura en què els resultats de sortida que els sistemes IA generin s'hagin de fer servir a la Unió. Tanmateix, per tenir en compte els acords existents i les necessitats especials de cooperació futura amb socis estrangers amb els quals s'intercanvien informació i proves, el present Reglament no s'ha d'aplicar a les autoritats públiques d'un tercer país ni a organitzacions internacionals quan actuïn en el marc d'acords internacionals o de cooperació subscrits a escala nacional o de la Unió amb finalitats de cooperació judicial i de garantia del compliment de la llei amb la Unió o els seus estats membres si el tercer país o l'organització internacional corresponent ofereix prou garanties pel que fa a la protecció dels drets i les llibertats fonamentals de les persones. Si és el cas, això pot cobrir les activitats d'entitats a les quals els tercers països hagin encomanat tasques específiques en suport judicial i de garantia del compliment de la llei. El marc de cooperació o els acords s'han establert amb caràcter bilateral entre els estats membres i els tercers països o entre la Unió Europea, l'Europol i altres organismes de la Unió i tercers països i organitzacions internacionals. Les autoritats competents per a la supervisió de les autoritats garanteixes del compliment de la llei i judicials en virtut del Reglament han d'avaluar si els marcs de cooperació o els acords internacionals inclouen prou garanties pel que fa a la protecció dels drets i les llibertats fonamentals de les persones físiques. Les autoritats nacionals i les institucions i els òrgans i organismes de la Unió que siguin destinataris dels resultats de sortida i que la facin servir a la Unió continuen sent responsables de garantir que l'ús que en fan és conforme amb el dret de la Unió. Quan, en el futur, els acords internacionals es revisin o se'n formalitzin d'altres, les parts contractants han de fer tot el que els sigui possible perquè els acords s'ajustin als requisits del present Reglament.

(23) El present Reglament també s'ha d'aplicar a les institucions, òrgans i organismes de la Unió quan actuïn com a proveïdors o responsables del desplegament d'un sistema d'IA.

(24) En cas i en la mesura que s'introdueixin en el mercat, es posin en servei o s'utilitzin, amb modificació o sense, amb finalitats militars, de defensa o de seguretat nacional, els sistemes d'IA s'han d'excloure de l'àmbit d'aplicació del present Reglament, independentment del tipus d'entitat que dugui a terme aquestes activitats, per exemple, amb independència que es tracti d'una entitat pública o d'una entitat privada. Pel que fa a les finalitats de militars i de defensa, l'exclusió la justifiquen tant l'article 4, apartat 2, del TUE, com les especificitats de la política de defensa dels estats membres i de la política comuna de defensa de la Unió a què el títol V, capítol 2, del TUE, es refereix. Aquestes activitats estan subjectes al dret internacional públic, el qual, per tant, és el marc jurídic més adequat per a la regulació dels sistemes d'IA en el context de l'ús de la força letal i d'altres sistemes d'IA en el context de les activitats militars i de defensa. Pel que fa a les finalitats de seguretat nacional, l'exclusió es justifica tant pel fet que la seguretat nacional continua sent responsabilitat exclusiva dels estats membres d'acord amb l'article 4, apartat 2, del TUE, com per la naturalesa específica i les necessitats operatives de les activitats de seguretat nacional i les normes nacionals específiques que els són aplicables. No obstant això, si un sistema d'IA desenvolupat, introduït en el mercat, posat en servei o utilitzat amb finalitats militars, de defensa o de seguretat nacional, s'utilitza fora d'aquests àmbits temporalment o de forma permanent per a altres finalitats (per exemple, amb finalitats civils o humanitàries, per a la garantia del compliment de la llei o per a la seguretat pública), aquest sistema entraria en l'àmbit d'aplicació del present Reglament. En aquest cas, l'entitat que utilitzi el sistema d'IA amb finalitats que no siguin militars, de defensa o de seguretat nacional ha de garantir que el sistema d'IA compleix el que disposa aquest Reglament, llevat que el sistema ja ho faci. Els sistemes d'IA introduïts en el mercat o posats en servei per a un fi exclòs (militar, de defensa o de seguretat nacional) i un o diversos de no exclòs (civils o de garantia del compliment de la llei) entren en l'àmbit d'aplicació del present Reglament i els proveïdors d'aquests sistemes n'han de garantir el compliment. En aquests casos, el fet que un sistema d'IA pugui entrar en l'àmbit d'aplicació del present Reglament no ha d'afectar la possibilitat que les entitats que duen a terme activitats militars, de defensa i de seguretat nacional, independentment del tipus d'entitat que les dugui a terme, utilitzin sistemes d'IA amb finalitats de seguretat nacional, militars i de defensa, l'ús dels quals està exclòs de l'àmbit d'aplicació del present Reglament. Un sistema d'IA introduït en el mercat amb finalitats civils o de garantia del compliment de la llei que s'utilitzi, amb modificacions o sense, amb finalitats militars, de defensa o de seguretat nacional no ha d'entrar en l'àmbit d'aplicació del present Reglament, independentment del tipus d'entitat que dugui a terme aquestes activitats.

(25) El present Reglament ha de donar suport a la innovació, respectar la llibertat de ciència i no socavar l'activitat de recerca i desenvolupament. Per tant, cal excloure'n de l'àmbit d'aplicació els sistemes i models d'IA desenvolupats específicament i posats en servei únicament amb finalitats de recerca i desenvolupament científics. A més, cal garantir que el present Reglament no afecti d'una altra manera l'activitat de recerca i desenvolupament científics sobre sistemes o models d'IA abans que s'introdueixin al mercat o es posin en servei. Pel que fa a l'activitat de recerca, prova i desenvolupament orientada a productes en relació amb sistemes o modes d'IA, les disposicions del present Reglament tampoc no s'han d'aplicar abans que els sistemes o models esmentats es posin en servei o s'introdueixin en el mercat. L'exclusió s'entén sense perjudici de l'obligació de complir el Reglament quan, com a resultat de l'activitat de recerca i desenvolupament, s'introdueixi o es posi en servei

un sistema d'IA que entri en l'àmbit d'aplicació del Reglament, o de l'aplicació de disposicions sobre espais controlats de proves per a la IA i proves en condicions reals. A més, sense perjudici de l'exclusió dels sistemes d'IA específicament desenvolupats i posats en servei amb l'única finalitat de la recerca i el desenvolupament científic, qualsevol altre sistema d'IA que es pugui fer servir per dur a terme una activitat de recerca i desenvolupament ha de quedar subjecte a les disposicions del present Reglament. En qualsevol cas, tota activitat de recerca i desenvolupament s'ha de dur a terme d'acord amb normes ètiques i professionals reconegudes per a la recerca científica i d'acord, també, amb el dret de la Unió aplicable.

(26) Per introduir un conjunt proporcionat i eficaç de normes vinculants per als sistemes d'IA, s'ha de seguir un enfocament basat en el risc clarament definit, que adapti el tipus i el contingut de les normes a la intensitat i l'abast dels riscos que els sistemes d'IA poden generar. Per tant, cal prohibir certes pràctiques d'IA inacceptables, establir requisits per als sistemes d'IA d'alt risc i obligacions aplicables als operadors pertinents, a més d'imposar obligacions de transparència per a determinats sistemes d'IA.

(27) Tot i que l'enfocament basat en el risc és la base d'un conjunt proporcionat i eficaç de normes vinculants, convé recordar Directrius ètiques per a una IA fiable, de 2019, desenvolupades pel Grup independent d'experts d'alt nivell sobre IA creat per la Comissió. En aquestes directrius, el Grup independent d'experts d'alt nivell sobre IA va desenvolupar set principis ètics no vinculants per a la IA que tenen com a finalitat contribuir a garantir la fiabilitat i la solidesa ètica de la IA. Els set principis són: acció i supervisió humanes, solidesa tècnica i seguretat, gestió de la privadesa i de les dades, transparència, diversitat, no discriminació i equitat; benestar social i ambiental, i rendició de comptes. Sense perjudici dels requisits jurídicament vinculants del present Reglament i de qualsevol altra legislació aplicable de la Unió, les directrius contribueixen al disseny d'una IA coherent, fiable i centrada en la persona, d'acord amb la Carta i els valors fundacionals de la Unió. D'acord amb les directrius del Grup independent d'experts d'alt nivell sobre IA, "acció i supervisió humanes" té a veure amb el fet que els sistemes d'IA es desenvolupen i empren com a eina al servei de les persones, que respecta la dignitat humana i l'autonomia personal i que funciona d'una manera que els éssers humans poden controlar i supervisar de manera adequada. Per "solidesa tècnica i seguretat" cal entendre que els sistemes d'IA es desenvolupen i fan servir de manera que siguin sòlids en cas de problemes i resilients davant els intents d'alterar-ne l'ús o el rendiment per permetre l'ús il·legal per part de tercers, i minimitzar danys no desitjats. Per "gestió de la privadesa i de les dades" s'entén que els sistemes d'IA es desenvolupen i es fan servir de conformitat amb normes que regeixen la protecció de la privadesa i de les dades, mentre tracten dades que compleixen normes estrictes en termes de qualitat i integritat. Per "transparència" s'entén que els sistemes d'IA es desenvolupen i fan servir de manera que siguin possibles una traçabilitat i explicabilitat adequades i que, alhora, faci que les persones siguin conscients que es comuniquen o interactuen amb un sistema d'IA i informi degudament els responsables del desplegament sobre les capacitats i limitacions del sistema d'IA i les persones afectades sobre els drets que tenen. Per "diversitat, no discriminació i equitat" s'entén que els sistemes d'IA es desenvolupen i es fan servir d'una manera que inclou diversos agents i promou la igualtat d'accés, la igualtat de gènere i la diversitat cultural, tot evitant els efectes discriminatoris i els biaixos injustos prohibits pel dret nacional o pel dret de la Unió. "Benestar social i ambiental" vol dir que els sistemes d'IA

es desenvolupen i fan servir de manera sostenible i respectuosa amb el medi ambient i, a més, en benefici de tots els éssers humans, alhora que se segueixen i s'avaluen els efectes a llarg termini en les persones, la societat i la democràcia. Quan sigui possible, l'aplicació d'aquests principis s'ha de reflectir en el disseny i l'ús de models d'IA. En tot cas, han de servir de base per a l'elaboració de codis de conducta d'acord amb el present Reglament. Es convida totes les parts interessades, incloses la indústria, el món acadèmic, la societat civil i les organitzacions de normalització, a tenir en compte, segons correspongui, els principis ètics per al desenvolupament de normes i millors pràctiques voluntàries.

(28) Al marge dels múltiples usos beneficiosos que se'n poden fer, la IA també es pot emprar de manera indeguda i facilitar poderoses eines per dur a terme pràctiques de manipulació, explotació i control social. Es tracta de pràctiques especialment nocives i incorrectes que s'han de prohibir, ja que van en contra dels valors de la Unió de respecte a la dignitat humana, la llibertat, la igualtat, la democràcia i l'estat de dret i els drets fonamentals consagrats en la Carta, inclòs el dret a la no discriminació, a la protecció de dades i a la privadesa i els drets de l'infant.

(29) Les tècniques de manipulació que la IA possibilita es poden emprar per persuadir les persones que adoptin comportaments no desitjats o per enganyar-les empenyent-les a prendre decisions d'una manera que en soccava i perjudica l'autonomia, la presa de decisions i la capacitat de triar lliurement. Són especialment perillosos i, per tant, se n'ha de prohibir la introducció en el mercat, la posada en servei o la utilització d'alguns en particular amb l'objectiu o a l'efecte d'alterar de manera substancial el comportament humà, amb la consegüent probabilitat que es produeixin perjudicis considerables, en particular perjudicis amb efectes adversos prou importants en la salut física o mental o en els interessos financers. Utilitzen components subliminars, com ara estímuls d'àudio, imatge o vídeo que són imperceptibles per a l'individu, ja que van més enllà de la percepció humana. O bé fan servir altres tècniques de manipulació o engany que subverteixen o perjudiquen l'autonomia i la capacitat de decidir o de triar lliurement, i ho fan de manera que l'individu no és conscient de les tècniques o, tot i ser-ne, pot ser víctima de l'engany o incapaç de controlar-les o resistir-s'hi. Això es podria facilitar, per exemple, mitjançant interfícies cervell-màquina o realitat virtual, ja que permeten un grau més elevat de control dels estímuls que es presenten a les persones, en la mesura que en poden distorsionar substancialment el comportament d'una manera que comporti un perjudici considerable. A més, els sistemes d'IA també poden explotar les vulnerabilitats d'una persona o d'un col·lectiu específic de persones per raó d'edat, discapacitat en el sentit de la Directiva (UE) 2019/882 del Parlament Europeu i del Consell [\(16\)](#), o d'una situació social o econòmica específica que és probable que les faci més propícies per a l'explotació, com és el cas de les persones que viuen en pobresa extrema, minories ètniques o religioses. Es poden introduir en el mercat, posar en servei o emprar amb l'objectiu de distorsionar de manera substancial la conducta d'una persona, i d'una manera que provoqui –o de la qual es pugui esperar que li provocarà– perjudicis considerables a la persona mateixa o a una altra persona o a un col·lectiu; inclosos perjudicis que es poden acumular al llarg del temps. Per tant, s'han de prohibir. No es pot pressuposar que hi hagi intenció de distorsionar el comportament quan la distorsió resulta de factors aliens al sistema d'IA que escapen al control del proveïdor o del responsable del desplegament, factors que no és lògic preveure i que, en conseqüència, ni el proveïdor ni el

responsable del desplegament del sistema d'IA poden mitigar. En qualsevol cas, no cal que el proveïdor o el responsable del desplegament tinguin la intenció de causar un perjudici considerable, sempre que el perjudici resulti de les pràctiques de manipulació o explotació que la IA fa possibles. La prohibició d'aquestes pràctiques d'IA complementa les disposicions de la Directiva 2005/29/CE del Parlament Europeu i del Consell [\(17\)](#), en particular la prohibició, en qualsevol circumstància, de les pràctiques comercials deslleials que causen perjudicis econòmics o financers als consumidors, hagin estat establertes mitjançant sistemes d'IA o d'una altra manera. La prohibició de les pràctiques de manipulació i explotació en el Reglament no ha d'afectar les pràctiques lícites en el context de tractament mèdic; per exemple, el tractament psicològic d'una malaltia mental o la rehabilitació física, quan es desenvolupen d'acord amb la llei i les normes mèdiques aplicables; per exemple, havent obtingut el consentiment explícit de la persona afectada o de qui n'ostenti la representació legal. Així mateix, no s'ha de considerar que les pràctiques comercials comunes i legítimes (per exemple, en el camp de la publicitat) que compleixin la legislació aplicable són, en si mateixes, pràctiques de manipulació perjudicials que la IA fa possibles.

(30) S'han de prohibir els sistemes de categorització biomètrica basats en dades biomètriques de les persones físiques, com ara la cara o les impressions dactilars d'una persona, per deduir-ne o inferir-ne les opinions polítiques, la pertinença sindical, les creences religioses o filosòfiques, la raça i la vida o l'orientació sexual. La prohibició no s'ha d'aplicar a l'etiquetatge, al filtratge ni a la categorització lícits de conjunts de dades biomètriques adquirides de conformitat amb el dret nacional o de la Unió en funció de dades biomètriques, com és el cas de la classificació d'imatges en funció del color dels cabells o del color d'ulls, que es poden fer servir, per exemple, en l'àmbit de la garantia del compliment de la llei.

(31) Els sistemes d'IA que permeten a agents públics o privats establir una puntuació social de les persones físiques poden tenir resultats discriminatoris i abocar a l'exclusió a determinats col·lectius. Poden menyscar el dret a la dignitat i a la no discriminació i els valors de la igualtat i la justícia. Aquests sistemes d'IA avaluen o classifiquen les persones o grups naturals de persones basant-se en múltiples punts de dades relacionats amb el seu comportament social en múltiples contextos o característiques personals conegudes, inferides o predites durant determinats períodes de temps. La puntuació social que se n'obté pot comportar un tracte perjudicial o desfavorable per a persones físiques individuals o per a col·lectius sencers en contextos socials, contextos que no tenen a veure amb el context en què les dades es van generar o recollir inicialment. També poden menar a un tracte perjudicial fora de mesura o injustificat atesa la gravetat de la seva conducta social. Per tant, s'han de prohibir els sistemes d'IA que impliquen aquestes pràctiques inacceptables de puntuació i que ocasionen aquests resultats perjudicials o desfavorables. La prohibició no ha d'afectar pràctiques lícites d'avaluació de les persones que es facin per a una finalitat específica de conformitat amb el dret de la Unió i el dret nacional.

(32) L'ús de sistemes d'IA per a la identificació biomètrica remota "en temps real" de persones físiques en espais d'accés públic amb finalitats de garantia del compliment de la llei envaeix de manera especialment greu els drets i les llibertats de les persones afectades, en la mesura

en què pot afectar la vida privada d'una part important de la població, provocar la sensació d'estar sota vigilància constant i dissuadir indirectament els ciutadans d'exercir la llibertat de reunió i altres drets fonamentals. Les imprecisions tècniques dels sistemes d'IA destinats a la identificació biomètrica remota de les persones físiques pot causar resultats esbiaixats i tenir efectes discriminatoris. Els uns i els altres són especialment pertinents pel que fa a l'edat, l'ètnia, la raça, el sexe o la discapacitat. A més, la immediatesa de les conseqüències i les oportunitats escasses de fer comprovacions o correccions addicionals en relació amb sistemes que operen en temps real augmenten el risc que els sistemes d'IA comporten per als drets i les llibertats de les persones afectades en el context d'activitats de garantia del compliment de la llei o de les persones a qui aquestes afecten.

(33) Per tant, cal prohibir-ne l'ús per a les finalitats de garantia del compliment de la llei, i autoritzar-lo només per a situacions comptades, determinades amb precisió, en què fer-ne ús sigui estrictament necessari per a l'assoliment d'un interès públic essencial que, per la importància que té, compensi el risc. Són situacions com ara la cerca de determinades víctimes d'un delictes, incloses persones desaparegudes, determinades amenaces per a la vida o per a la seguretat física de les persones físiques o amenaces d'atemptat terrorista; i la localització o identificació dels autors o sospitosos dels delictes que s'enumeren en un annex del present Reglament, quan les infraccions a què es refereixen es castiguen a l'estat membre afectat amb una mesura privativa de llibertat que tingui una durada màxima de quatre anys, i segons es defineixen en la llei de l'estat membre esmentat. Fixar el líndar per a la pena o la mesura de seguretat privatives de llibertat d'acord amb la llei nacional contribueix a garantir que la infracció sigui prou greu per arribar a justificar l'ús de sistemes d'identificació biomètrica "en temps real". A més, la llista de delictes que es facilita en un annex del present Reglament es basa en els 32 delictes que s'enumeren en la Decisió marc 2002/584/JAI del Consell (18), per bé que cal tenir en compte que, en la pràctica, pot passar que n'hi hagi de més rellevants d'altres en el sentit que és previsible que recórrer a la identificació biomètrica remota "en temps real" podria ser necessari i proporcionat en graus molt diversos per localitzar o identificar els autors o sospitosos de les infraccions enumerades, i que pot passar que hi hagi diferències en la gravetat, la probabilitat i la magnitud dels perjudicis o de les conseqüències negatives possibles. Una amenaça imminent per a la vida o la seguretat física de les persones físiques també podria ser el resultat d'una greu pertorbació de la infraestructura crítica, tal com es defineix en l'article 2, punt 4, de la Directiva (UE) 2022/2557 del Parlament Europeu i del Consell (19), quan la interrupció o pertorbació de la infraestructura crítica comporti una amenaça imminent per a la vida o la seguretat física d'una persona, també en perjudicar de manera greu el subministrament de productes bàsics a la població o l'exercici d'una funció essencial de l'estat. A més, el present Reglament ha de preservar la capacitat de les autoritats garants del compliment de la llei, de control fronterer, de la immigració o de l'asil per dur a terme controls d'identitat en presència de la persona afectada, de conformitat amb les condicions establertes en el dret de la Unió i en el dret nacional per a aquests controls. En particular, les autoritats esmentades han de poder fer servir sistemes d'informació, de conformitat amb la legislació de la Unió o nacional, per identificar les persones que, durant un control d'identitat, s'oposen al fet que se les identifiqui o no poden declarar o demostrar la identitat, sense que per a aquesta finalitat el present Reglament exigeixi que s'obtingui una autorització prèvia. Per exemple, podria ser el cas de persona involucrada en un delictes que no vulgui o que, per causa d'un accident o

un estat de salut en particular, no pugui revelar la identitat pròpia a les autoritats garants del compliment de la llei.

(34) Per vetllar perquè aquests sistemes s'utilitzin de manera responsable i proporcionada, també és important establir que, en aquestes situacions enumerades de manera limitativa i definides amb precisió, es tinguin en compte determinats elements; en particular, pel que fa a la naturalesa de la situació que doni lloc a la sol·licitud, a les conseqüències que fer-ne ús pot tenir sobre els drets i les llibertats de totes les persones implicades, i a les garanties i condicions que n'acompanyin l'ús. A més, l'ús de sistemes d'identificació biomètrica remota en "temps real" en espais d'accés públic amb la finalitat de garantir el compliment de la llei només s'ha d'aplicar per confirmar la identitat de l'individu específicament objectiu i sense anar més enllà del que és estrictament necessari en relació amb el període de temps i l'àmbit geogràfic i personal, tenint en compte en particular les proves o indicacions relatives a les amenaces, les víctimes o els autors. L'ús del sistema d'identificació biomètrica remota en temps real en espais d'accés públic només s'ha d'autoritzar si l'autoritat garant del compliment de la llei ha avaluat l'impacte en els drets fonamentals i, llevat que es disposi el contrari en el present Reglament, ha registrat el sistema en la base de dades tal com s'estableix en el Reglament mateix. La base de dades de persones de referència ha de ser adequada per a cada supòsit d'ús en cadascuna de les situacions esmentades.

(35) Tot ús d'un sistema d'identificació biomètrica remota "en temps real" en espais d'accés públic amb finalitats de garantia del compliment de la llei ha d'haver estat autoritzat de manera expressa i específica per una autoritat judicial o per una autoritat administrativa independent d'un estat membre amb facultat de decisió vinculant. En principi, l'autorització s'ha d'obtenir abans de fer ús del sistema d'IA per identificar una o més persones. S'han de permetre excepcions a la norma en situacions degudament justificades per motius d'urgència; és a dir, en situacions en què la necessitat de fer servir els sistemes de què es tracti sigui tan imperiosa que resulti efectivament i objectivament impossible obtenir una autorització abans de començar a fer servir el sistema d'IA. En aquestes situacions d'urgència, l'ús s'ha de limitar al mínim imprescindible i complir les garanties i condicions oportunes, segons el que la legislació nacional determina i s'especifica en el context de cada cas d'ús urgent individual per part de l'autoritat garant del compliment de la llei. A més, en les situacions esmentades, les autoritats garants del compliment de la llei han de demanar l'autorització i indicar per què no ho han pogut fer abans, sense demora indeguda i, en tot cas, sense que hagin passat més de 24 hores. Si l'autorització es denega, l'ús de sistemes d'identificació biomètrica en temps real vinculats a l'autorització s'ha d'interrompre amb efecte immediat, i totes les dades relacionades amb l'ús de què es tracti s'han de rebutjar i suprimir. D'aquestes dades, n'hi ha que inclouen les d'entrada directament adquirides per un sistema d'IA durant l'ús del sistema, i també els resultats i la informació de sortida de l'ús vinculats a l'autorització esmentada. No ha d'incloure la informació d'entrada adquirida legalment de conformitat amb un altre acte del dret nacional o de la Unió. En qualsevol cas, no s'ha de prendre cap decisió que produeixi efectes adversos en una persona basant-se únicament en els resultats de sortida del sistema d'identificació biomètrica remota.

(36) Per exercir les funcions pròpies de conformitat amb els requisits establerts en el Reglament, i en la normativa nacional, s'ha de notificar a l'autoritat de vigilància del mercat pertinent i a l'autoritat nacional de protecció de dades cada ús del sistema d'identificació biomètrica en temps real. Les autoritats de vigilància del mercat i les autoritats nacionals de protecció de dades que hagin rebut una notificació han de presentar a la Comissió un informe anual sobre l'ús de sistemes d'identificació biomètrica en temps real.

(37) A més, en el marc exhaustiu que el present Reglament estableix, convé disposar que aquest ús en el territori d'un estat membre de conformitat amb el Reglament només ha de ser possible quan l'estat membre de què es tracti hagi decidit contemplar expressament la possibilitat d'autoritzar-lo en les normes detallades del dret nacional propi, i en la mesura que ho hagi contemplat. En conseqüència, d'acord amb el present Reglament els estats membres continuen tenint la llibertat de no oferir aquesta possibilitat en absolut o d'oferir-la únicament en relació amb alguns dels objectius que poden justificar un ús autoritzat conforme al present Reglament. Les normes nacionals s'han de notificar a la Comissió en el termini de trenta dies des que s'hagin adoptat.

(38) L'ús de sistemes d'IA per a la identificació biomètrica remota en temps real de persones físiques en espais d'accés públic per a la garantia del compliment de la llei requereix necessàriament el tractament de dades biomètriques. Amb excepcions basades en l'article 16 del TFUE, les normes del present Reglament que prohibeixen aquest ús s'han d'aplicar com a *lex specialis* respecte de les normes sobre el tractament de dades biomètriques que figuren a l'article 10 de la Directiva (UE) 2016/680, amb la qual cosa es regulen de manera exhaustiva aquest ús i el tractament de les dades biomètriques corresponents. Per tant, l'ús i el tractament només poden ser possibles en la mesura que siguin compatibles amb el marc establert pel present Reglament, sense que, fora del marc, hi hagi marge perquè les autoritats competents, quan actuïn per a la garantia del compliment de la llei, facin servir els sistemes i tractin les dades relacionades basant-se en els motius que consten en l'article 10 de la Directiva (UE) 2016/680. En aquest context, el Reglament no té per objecte proporcionar la base legal per al tractament de dades personals en virtut de l'article 8 de la Directiva (UE) 2016/680. No obstant això, l'ús de sistemes d'identificació biomètrica remota en temps real en espais d'accés públic per a finalitats diferents de la garantia del compliment de la llei, incloses les autoritats competents, no ha d'estar subjecte al marc específic que aquest Reglament estableix pel que fa a l'ús dels sistemes amb finalitats de garantia del compliment de la llei. Per tant, fer-ne ús amb finalitats diferents de la garantia del compliment de la llei no ha d'estar subjecte al requisit d'obtenir una autorització que el Reglament preveu ni a les normes de desenvolupament aplicables del dret nacional que puguin fer efectiva l'autorització esmentada.

(39) Qualsevol tractament de dades biomètriques i altres dades personals que intervinguen en l'ús de sistemes d'IA per a la identificació biomètrica, que no sigui en relació amb l'ús de sistemes d'identificació biomètrica remots en temps real en espais d'accés públic a efectes de garantia del compliment de la llei i regulats pel Reglament, ha de continuar complint tots els requisits derivats de l'article 10 de la Directiva (UE) 2016/680. L'article 9, apartat 1, del Reglament (UE) 2016/679 i l'article 10, apartat 1, del Reglament (UE) 2018/1725 prohibeixen el

tractament de dades biomètriques amb finalitats diferents de la garantia del compliment de la llei, amb les excepcions limitades que els articles mateixos preveuen. En l'aplicació de l'article 9, apartat 1, del Reglament (UE) 2016/679, l'ús de la identificació biomètrica remota per a finalitats diferents de la garantia del compliment de la llei ja ha estat objecte de decisions de prohibició per part de les autoritats nacionals de protecció de dades.

(40) De conformitat amb l'article 6 bis del Protocol 21 sobre la posició del Regne Unit i d'Irlanda respecte de l'Espai de Llibertat, Seguretat i Justícia, annex al TUE i al TFUE, les normes establertes a l'article 5, apartat 1, subapartat primer, lletra g), en la mesura que s'aplica a l'ús de sistemes de categorització biomètrica per a activitats en l'àmbit de la cooperació policial i la cooperació judicial en matèria penal, l'article 5, apartat 1, subapartat primer, lletra d), en la mesura que s'aplica a l'ús de sistemes d'IA compresos en l'àmbit d'aplicació de l'esmentat article, l'article 5, apartat 1, subapartat primer, lletra h), i apartats 2 a 6, i l'article 26, apartat 10, del present Reglament, adoptades basant-se en l'article 16 del TFUE que es refereixen al tractament de dades de caràcter personal pels estats membres en l'exercici de les activitats compreses en l'àmbit d'aplicació de la tercera part, títol V, capítols 4 o 5, del TFUE només són vinculants per a Irlanda en la mesura que siguin vinculants per a aquest Estat normes de la Unió que regulin formes de cooperació judicial en matèria penal i de cooperació policial en el marc de les quals s'hagin de respectar les disposicions establertes segons l'article 16 del TFUE.

(41) De conformitat amb el que disposen els articles 2 i 2 bis del Protocol 22 sobre la posició de Dinamarca, annex al TUE i al TFUE, les normes establertes a l'article 5, apartat 1, paràgraf primer, lletra g), en la mesura que s'aplica a l'ús de sistemes de categorització biomètrica per a activitats en l'àmbit de la cooperació policial i la cooperació judicial en matèria penal, l'article 5, apartat 1, paràgraf primer, lletra d), en la mesura que s'apliquen a l'ús de sistemes d'IA compresos en l'àmbit d'aplicació de l'article esmentat, l'article 5, apartat 1, paràgraf primer, lletra h), i apartats 2 a 6, i l'article 26, apartat 10, del present Reglament, adoptades sobre la base de l'article 16 del TFUE que es refereixen al tractament de dades de caràcter personal pels estats membres en l'exercici de les activitats compreses en l'àmbit d'aplicació de la tercera part, títol V, capítols 4 o 5, de l'esmentat Tractat, no vinculen Dinamarca ni li són aplicables.

(42) En consonància amb la presumpció d'innocència, les persones físiques de la Unió sempre han de ser jutjades considerant-ne el comportament real. Mai no se les ha de poder jutjar partint de comportaments predits per una IA basats únicament en l'elaboració dels seus perfils, en els trets o les característiques de la seva personalitat, com ara nacionalitat, lloc de naixement, lloc de residència, nombre de fills, nivell d'endeutament o mena de vehicle, sense una valoració humana i sense que hi hagi una sospita raonable, basada en fets objectius comprovables, de la implicació de la persona en qüestió en una activitat delictiva. Cal, per tant, prohibir les avaluacions de riscos fetes respecte de persones físiques per avaluar la probabilitat que cometin un delictes o per predir la comissió d'un delictes real o potencial basant-se únicament en l'elaboració de perfils d'aquestes persones físiques o l'avaluació dels trets i les característiques de la seva personalitat. En qualsevol cas, la prohibició no es refereix ni pertoca a les anàlisis de riscos que no es basin en l'elaboració de

perfils de persones o en els trets i característiques de la personalitat de les persones, com és el cas dels sistemes d'IA que utilitzen les anàlisis de riscos per avaluar la probabilitat de frau financer per part d'empreses sobre la base de transaccions sospitoses o les eines d'anàlisi de risc per predir la probabilitat de localització d'estupefaents i mercaderies il·lícites per part de les autoritats duaneres, per exemple, basant-se en les rutes de tràfic conegudes.

(43) La introducció en el mercat, la posada en servei per a aquesta finalitat concreta o la utilització de sistemes d'IA que creïn bases de dades de reconeixement facial o n'ampliïn mitjançant l'extracció no selectiva d'imatges facials a partir d'internet o d'imatges de circuit tancat de televisió han d'estar prohibides, ja que són pràctiques que agreugen el sentiment de vigilància massiva i poden donar lloc a greus violacions dels drets fonamentals, inclòs el dret a la privadesa.

(44) Hi ha gran preocupació respecte de la base científica dels sistemes d'IA que procuren detectar o deduir les emocions, especialment perquè l'expressió de les emocions varia de forma considerable entre cultures i situacions; fins i tot, en una mateixa persona. Entre les deficiències clau d'aquests sistemes hi ha la fiabilitat limitada, la manca d'especificitat i la capacitat de generalització limitada. Per tant, els sistemes d'IA que detecten o dedueixen les emocions o les intencions de les persones físiques a partir de les seves dades biomètriques poden tenir resultats discriminatoris i en poden envair els drets i les llibertats. Atès el desequilibri de poder en el context laboral o educatiu, unit al caràcter intrusiu que els caracteritza, aquests sistemes podrien resultar en un tracte perjudicial o desfavorable de determinades persones físiques o col·lectius sencers. Per tant, la introducció en el mercat, la posada en servei o l'ús de sistemes d'IA destinats a fer-se servir l'estat emocional dels individus en situacions relacionades amb el lloc de treball i l'educació s'ha de prohibir. La prohibició no ha de cobrir els sistemes d'IA introduïts en el mercat estrictament per raons mèdiques o de seguretat, com ara els sistemes destinats a l'ús terapèutic.

(45) El present Reglament no ha d'afectar les pràctiques prohibides pel dret de la Unió, inclòs el dret de la Unió en matèria de protecció de dades, de no discriminació, de protecció dels consumidors i sobre competència.

(46) Els sistemes d'IA d'alt risc només es poden introduir en el mercat de la Unió, posar-se en servei o fer-se servir si compleixen certs requisits obligatoris. Es tracta de requisits que han d'assegurar que els sistemes d'IA d'alt risc que hi ha disponibles a la Unió o hi produeixen resultats de sortida no plantegen riscos inacceptables per als interessos públics importants de la Unió que el dret d'aquesta protegeix. Sobre la base del nou marc legislatiu, tal com s'aclareix en la Comunicació de la Comissió titulada «Guia blava sobre l'aplicació de la normativa europea relativa als productes, de 2022» [\(20\)](#), la norma general és que més d'un acte legislatiu de la legislació d'harmonització de la Unió, com els Reglaments 2017/745 [\(21\)](#) i (UE) 2017/746 [\(22\)](#) del Parlament Europeu i del Consell o la Directiva 2006/42/CE del Parlament Europeu i del Consell [\(23\)](#) puguin aplicar-se a un producte, atès que la introducció en el mercat o la posada en servei només poden tenir lloc quan el

producte compleix tota la legislació d'harmonització de la Unió aplicable. Per garantir la coherència i evitar càrregues administratives o costos innecessaris, els proveïdors d'un producte que contingui un o diversos sistemes d'IA d'alt risc, als quals s'apliquin els requisits del present Reglament i de la legislació d'harmonització de la Unió inclosa en una llista d'un annex del present Reglament, han de ser flexibles pel que fa a les decisions operatives relatives a la manera de garantir la conformitat d'un producte que contingui un o diversos sistemes d'IA amb tots els requisits aplicables de la legislació d'harmonització de la Unió de manera òptima. La classificació d'un sistema d'IA com «d'alt risc» s'ha de limitar als sistemes d'IA que tinguin un efecte perjudicial considerable en la salut, la seguretat i els drets fonamentals de les persones de la Unió, i aquesta limitació ha de reduir al mínim qualsevol possible restricció del comerç internacional.

(47) Els sistemes d'IA poden tenir un efecte advers en la salut i la seguretat de les persones; en particular, quan funcionen com a components de seguretat de productes. D'acord amb els objectius de la legislació d'harmonització de la Unió, de facilitar la lliure circulació de productes en el mercat interior i de vetllar perquè només arribin al mercat els productes que siguin segurs i conformes, cal prevenir i mitigar degudament els riscos de seguretat que un producte, en conjunt, pugui generar a causa dels seus components digitals, entre els quals hi pot haver sistemes d'IA. Per exemple, els robots cada vegada més autònoms que s'utilitzen a les fàbriques o amb finalitats d'assistència i atenció personal han de poder funcionar i exercir les funcions de manera segura en entorns complexos. De la mateixa manera, en el sector sanitari, en què hi pot haver repercussions especialment importants en la vida i la salut, els sistemes de diagnòstic i de suport a les decisions humanes –cada vegada més sofisticats– han de ser fiables i precisos.

(48) L'abast de l'efecte advers causat pel sistema d'IA en els drets fonamentals protegits per la Carta és de particular rellevància a l'hora de classificar un sistema d'IA com a d'alt risc. Aquests drets inclouen el dret a la dignitat humana, el respecte a la vida privada i familiar, la protecció de dades personals, la llibertat d'expressió i informació, la llibertat de reunió i d'associació, el dret a la no discriminació, el dret a l'educació, la protecció del consumidor, els drets dels treballadors, els drets de les persones amb discapacitat, la igualtat de gènere, els drets de propietat intel·lectual, el dret a la tutela judicial efectiva i a un jutge imparcial, el dret de defensa i presumpció d'innocència, i el dret a una bona administració. A més d'aquests drets, convé posar en relleu el fet que els menors posseeixen uns drets específics consagrats a l'article 24 de la Carta i a la Convenció sobre els Drets de l'Infant de les Nacions Unides, que es desenvolupen amb més detall en l'observació general 25 de la Convenció sobre els Drets de l'Infant de Nacions Unides relativa als drets dels infants en relació amb l'entorn digital. Ambdós instruments exigeixen que es tinguin en consideració les vulnerabilitats dels menors i que se'ls aporti la protecció i l'assistència necessàries per al seu benestar. Quan s'avalui la gravetat del perjudici que un sistema d'IA pot ocasionar, també pel que fa a la salut i la seguretat de les persones, s'ha de tenir en compte, a més, el dret fonamental a un nivell elevat de protecció del medi ambient, consagrat a la Carta i aplicat en les polítiques de la Unió.

(49) Pel que fa als sistemes d'IA d'alt risc que són components de seguretat de productes o sistemes, o que en ells mateixos són productes o sistemes que entren en l'àmbit d'aplicació del Reglament (CE) 300/2008 del Parlament Europeu i del Consell [\(24\)](#), Reglament (UE) 167/2013 del Parlament Europeu i del Consell [\(25\)](#), Reglament (UE) 168/2013 del Parlament Europeu i del Consell [\(26\)](#), Directiva 2014/90/UE del Parlament Europeu i del Consell [\(27\)](#), Directiva (UE) 2016/797 del Parlament Europeu i del Consell [\(28\)](#), Reglament (UE) 2018/858 del Parlament Europeu i del Consell [\(29\)](#), Reglament (UE) 2018/1139 del Parlament Europeu i del Consell, i el Reglament (UE) 2019/2144 del Parlament Europeu i del Consell [\(31\)](#), convé modificar aquests actes per garantir que, en adoptar els actes delegats o d'execució pertinents que s'hi basin, la Comissió tingui en compte els requisits obligatoris per als sistemes d'IA d'alt risc previstos en el Reglament, atenent les particularitats tècniques i reglamentàries dels diferents sectors i sense interferir amb els mecanismes i les autoritats de governança, avaluació de la conformitat i control del compliment vigents establerts en aquests actes.

(50) Pel que fa als sistemes d'IA que són components de seguretat dels productes, o que en ells mateixos són productes, i que pertanyen a l'àmbit d'aplicació de determinades lleis d'harmonització de la Unió enumerades en un annex del present Reglament, escau classificar-los com a d'alt risc en virtut del Reglament si el producte afectat se sotmet al procediment d'avaluació de la conformitat amb un organisme d'avaluació de la conformitat de tercers d'acord amb la legislació d'harmonització de la Unió corresponent. En particular, els productes són màquines, joguines, ascensors, equip i sistemes de protecció per a ús en entorns potencialment explosius, equips radioelèctrics, equips de pressió, equips d'embarcacions d'esbarjo, instal·lacions de transport per cable, aparells que cremen combustibles gasosos, productes sanitaris, productes sanitaris per a diagnòstic in vitro, automoció i aviació.

(51) El fet que un sistema d'IA es classifiqui d'alt risc en virtut del Reglament no significa per força que el producte de què sigui component de seguretat, o el sistema d'IA mateix com a producte, es consideri d'alt risc conforme als criteris establerts en la legislació d'harmonització corresponent de la Unió que s'apliqui al producte. És el cas, en particular, dels Reglaments (UE) 2017/745 i (UE) 2017/746, que preveuen una avaluació de la conformitat de tercers dels productes de risc mitjà i alt.

(52) Pel que fa als sistemes d'IA independents –els sistemes d'IA d'alt risc que no són components de seguretat dels productes, o que són productes en ells mateixos– escau classificar-los com d'alt risc si, a la llum de la finalitat que tenen prevista, representen un alt risc de dany per a la salut i la seguretat o els drets fonamentals de les persones, tenint en compte tant la gravetat dels possibles danys com la probabilitat d'ocurrència, i se'n fa ús en una sèrie d'àrees predefinides específicament especificades en el present Reglament. Per identificar-los, s'empren la mateixa metodologia i els mateixos criteris previstos per a la possible modificació futura de la llista de sistemes d'IA d'alt risc, que la Comissió ha d'estar facultada per adoptar, mitjançant actes delegats, per tenir en compte el ràpid ritme del desenvolupament tecnològic i els possibles canvis en l'ús dels sistemes d'IA.

(53) També cal aclarir que hi pot haver casos específics en què els sistemes d'IA referits en àmbits predefinits especificats en el present Reglament no comportin un risc considerable de perjudicar interessos jurídics emparats pels àmbits esmentats, ja que no influeixen de manera substancial en la presa de decisions ni perjudiquen de manera substancial els interessos. A efectes del present Reglament, per sistema d'IA que no influeix substancialment en el resultat de la presa de decisions s'ha d'entendre un sistema d'IA que no afecta l'essència ni, consegüentment, el resultat de la presa de decisions, sia humana o automatitzada. Un sistema d'IA que no influeixi de manera substancial en el resultat de la presa de decisions podria incloure situacions en què es compleixin una o més de les condicions que s'exposen a continuació. La primera condició ha de ser que el sistema d'IA estigui destinat a fer una funció de procediment delimitada, com un sistema d'IA que transformi dades no estructurades en dades estructurades, un sistema d'IA que classifiqui els documents entrants en categories o un sistema d'IA que s'utilitzi per detectar duplicats entre un gran nombre d'aplicacions. Són funcions de naturalesa tan limitada que només comporten riscos limitats que no s'incrementen amb l'ús d'un sistema d'IA en un context que figura com un ús d'alt risc en un annex del present Reglament. La segona condició ha de ser que la funció exercida pel sistema d'IA estigui destinada a millorar el resultat d'una activitat humana ja completada que pugui ser rellevant per als usos d'alt risc enumerats en un annex del present Reglament. Tenint en compte les característiques esmentades, el sistema d'IA només afegeix una capa addicional a una activitat humana, de manera que el risc que comporta és menor. Aquesta condició s'aplicaria, per exemple, als sistemes d'IA destinats a millorar el llenguatge utilitzat en documents ja redactats, per exemple, pel que fa a l'ús d'un to professional o d'un registre lingüístic acadèmic o a l'adaptació del text a una comunicació de marca en particular. La tercera condició ha de ser que el sistema d'IA estigui destinat a detectar patrons de presa de decisions o desviacions respecte dels patrons de presa de decisions anteriors. Com que el sistema d'IA es fa servir després que ja s'hagi fet una valoració humana i no té per finalitat substituir-la ni influir-hi sense que l'hagi revisada de manera adequada un ésser humà, el risc seria menor. Per exemple, entre els sistemes d'IA d'aquesta mena, hi ha els que es poden fer servir per comprovar a posteriori si un professor es pot haver desviat del patró de qualificació habitual, per cridar-li l'atenció sobre possibles incoherències o anomalies. La quarta condició ha de ser que el sistema d'IA estigui destinat a fer una funció que només sigui preparatòria per a una avaluació pertinent als efectes dels sistemes d'IA enumerats en un annex del present Reglament. Així, la possible repercussió dels resultats de sortida del sistema seria molt minsa en termes de representar un risc per a l'avaluació subsegüent. Es tracta d'una condició que, entre altres, comprèn solucions intel·ligents per a la gestió d'arxius, en què s'inclouen diverses funcions com ara la indexació, la cerca, el tractament de text i de veu o la vinculació de dades a altres fonts de dades, o sistemes d'IA emprats per a la traducció dels documents inicials. En qualsevol cas, cal considerar que els sistemes d'IA utilitzats en casos d'alt risc enumerats en un annex del present Reglament presenten un risc significatiu de menyscabar la salut i la seguretat o els drets fonamentals si el sistema d'IA comporta l'elaboració de perfils en el sentit de l'article 4, punt 4, del Reglament (UE) 2016/679, de l'article 3, punt 4, de la Directiva (UE) 2016/680 o de l'article 3, punt 5, del Reglament (UE) 2018/1725. Per garantir la traçabilitat i la transparència, els proveïdors que, partint de les condicions esmentades, considerin que un sistema d'IA no és d'alt risc, han de documentar l'avaluació abans d'introduir-lo en el mercat o de posar-lo en servei i facilitar l'avaluació documentada a les autoritats nacionals

competents quan aquestes ho demanin. Ha de ser obligatori per als proveïdors de registrar el sistema en la base de dades de la UE creada en virtut del Reglament. Per facilitar orientació addicional per a l'aplicació pràctica de les condicions en què l'ús dels sistemes d'IA enumerats en un annex del present Reglament, excepcionalment, no són d'alt risc, la Comissió, havent-ho consultat amb el Consell d'IA, ha de proporcionar orientacions que especifiquin l'aplicació pràctica, tot completant-ho amb una llista completa d'exemples pràctics de casos d'ús de sistemes d'IA que són d'alt risc i casos d'ús que no ho són.

(54) Atès que les dades biomètriques constitueixen una categoria de dades personals sensibles, escau classificar com a d'alt risc diversos casos d'ús crítics de sistemes biomètrics, en la mesura en què fer-ne ús estigui permès d'acord amb el dret de la Unió i el dret nacional corresponent. Les imprecisions tècniques dels sistemes d'IA destinats a la identificació biomètrica remota de les persones físiques pot causar resultats esbiaixats i tenir efectes discriminatoris. El risc dels resultats esbiaixats i efectes discriminatoris és especialment rellevant pel que fa a l'edat, l'ètnia, la raça, el sexe o les discapacitats. Així, atesos els riscos esmentats, cal classificar els sistemes d'identificació biomètrica remota com a d'alt risc. Se n'exclouen els sistemes d'IA que tenen per finalitat la verificació biomètrica, inclosa l'autenticació, quan l'única finalitat és confirmar que una persona física és qui diu que és i confirmar la identitat d'una persona física per a l'objectiu únic de poder accedir a un servei, desbloquejar un dispositiu o accedir de manera segura a unes instal·lacions. A més, s'han de classificar com d'alt risc els sistemes d'IA destinats a fer-los servir per a la categorització biomètrica conforme a atributs o característiques sensibles protegits en virtut de l'article 9, apartat 1, del Reglament (UE) 2016/679 partint de dades biomètriques, en la mesura que no estiguin prohibits en virtut del present Reglament, i els sistemes de reconeixement d'emocions que no estiguin prohibits d'acord amb el present Reglament. Els sistemes biomètrics que només s'hagin de fer servir per possibilitar la ciberseguretat i les mesures de protecció de les dades personals no s'han de considerar sistemes d'IA d'alt risc.

(55) Pel que fa a la gestió i el funcionament d'infraestructures crítiques, escau incloure com a d'alt risc els sistemes d'IA de què s'ha de fer ús com a components de seguretat en la gestió i el funcionament de les infraestructures digitals crítiques que s'enumeren en l'annex, punt 8, de la Directiva (UE) 2022/2557; del trànsit rodat i del subministrament d'aigua, gas, calefacció i electricitat, ja que, en cas de fallada o mal funcionament, es pot produir un perill per a la vida i la salut de les persones a gran escala i alterar de manera significativa el desenvolupament habitual de les activitats socials i econòmiques. Els components de seguretat de les infraestructures crítiques, com ara les infraestructures digitals crítiques, són sistemes que serveixen per protegir directament la integritat física de les infraestructures crítiques o la salut i la seguretat de les persones i els béns, sense que siguin necessaris per al funcionament del sistema. El fet que aquests components no funcionin o funcionin malament pot comportar directament riscos per a la integritat física de les infraestructures crítiques i, per tant, per a la salut i la seguretat de les persones i els béns. Els components que només s'han de fer servir amb finalitats de ciberseguretat no entren en la classificació de components de seguretat. Dels components de seguretat de les infraestructures crítiques, en són exemples els sistemes de seguiment de la pressió de l'aigua o els sistemes de control de les alarmes contra incendis als centres de computació al núvol.

(56) El desplegament de sistemes d'IA en l'educació és important per fomentar l'educació i la formació digitals d'alta qualitat i per permetre que tots els estudiants i professors adquireixin i comparteixin les habilitats i competències digitals necessàries, inclosa l'alfabetització mediàtica i el pensament crític, per prendre part activa en l'economia, la societat i en els processos democràtics. Tanmateix, s'han de considerar sistemes d'IA d'alt risc els que es fan servir en l'ensenyament o en la formació professional; en particular, els que determinen l'accés o l'admissió, distribueixen les persones entre diferents institucions educatives i de formació professional o programes de tots els nivells i n'avaluen els resultats de l'aprenentatge, avaluen el nivell adequat d'educació d'una persona i influeixen de manera substancial en el nivell d'educació i formació que les persones rebran o a què podran accedir, o segueixen i detecten conductes prohibides dels estudiants durant les proves, ja que poden decidir la trajectòria formativa i professional d'una persona i, per tant, en pot afectar la capacitat per assegurar-los la subsistència. Quan es dissenyen i es fan servir de manera inadequada, aquests sistemes poden ser particularment intrusius i poden violar el dret a l'educació i a la formació, i el dret a no ser discriminats, i perpetuar patrons històrics de discriminació; per exemple, contra dones, determinats grups d'edat, persones amb discapacitat o persones de determinats orígens racials o ètnics o de determinada orientació sexual.

(57) També cal considerar d'alt risc els sistemes d'IA que es fan servir en els àmbits de l'ocupació, la gestió dels treballadors i l'accés a l'autoocupació; en particular, per a la contractació i la selecció de personal, per a la presa de decisions que afecten les condicions de les relacions de caràcter laboral, la promoció i la rescissió de relacions contractuals de caràcter laboral, per a l'assignació de funcions a partir de conductes individuals o trets o característiques personals i per al seguiment o l'avaluació de les persones en el marc de les relacions contractuals de caràcter laboral, ja que poden afectar de manera considerable les futures perspectives laborals, els mitjans de subsistència de les persones esmentades i els drets dels treballadors. Les relacions contractuals relacionades amb el treball han d'incloure, principalment, el personal i les persones que presten serveis a través de plataformes, com indica el programa de treball de la Comissió per a 2021. Durant tot el procés de contractació i en l'avaluació, promoció o retenció de persones en les relacions contractuals de caràcter laboral, aquests sistemes poden perpetuar patrons històrics de discriminació; per exemple, contra les dones, determinats grups d'edat, persones amb discapacitat o persones d'orígens racials o ètnics concrets o amb una orientació sexual determinada. Els sistemes d'IA emprats per controlar el rendiment i el comportament d'aquestes persones també en poden soscar els drets fonamentals a la protecció de dades i la privadesa.

(58) L'accés a determinats serveis i prestacions essencials, de caràcter públic i privat, necessaris perquè les persones puguin participar de ple en la societat i millorar el nivell de vida, i el gaudi de certs serveis i prestacions, és un altre àmbit en què cal parar atenció especial a l'ús de sistemes d'IA. En particular, les persones físiques sol·licitants o perceptores de les prestacions i els serveis d'assistència pública que concedeixen les autoritats públiques – serveis d'assistència sanitària, prestacions de seguretat social, serveis socials que garanteixen una protecció en casos com ara la maternitat, la malaltia, els accidents laborals,

la dependència o la vellesa i la pèrdua d'ocupació, l'assistència social i els ajuts a l'habitatge—solen dependre dels serveis i les prestacions i, en general, estan en una posició de vulnerabilitat respecte de les autoritats responsables. L'ús de sistemes d'IA per decidir si les autoritats han de concedir, denegar, reduir o revocar les prestacions o serveis o reclamar-ne la devolució, la qual cosa inclou decidir, per exemple, si els beneficiaris tenen legítimament dret a rebre'ls, podria tenir un efecte considerable en els mitjans de subsistència de les persones i vulnerar-ne els drets fonamentals, com ara el dret a la protecció social, a la no discriminació, a la dignitat humana o a la tutela judicial efectiva. Per tant, s'han de classificar com d'alt risc. El present Reglament, però, no pot ser un obstacle per al desenvolupament i l'ús d'enfocaments innovadors en l'Administració, els quals es podrien veure afavorits per una utilització més àmplia de sistemes d'IA conformes i segurs, sempre que aquests no representin un risc alt per a les persones tant físiques com jurídiques. A més, cal considerar d'alt risc els sistemes d'IA emprats per avaluar la qualificació creditícia o la solvència de les persones físiques, ja que decideixen si aquestes poden accedir a recursos financers o serveis essencials, com ara l'habitatge, l'electricitat i els serveis de telecomunicacions. L'ús dels sistemes d'IA amb aquestes finalitats pot comportar la discriminació de determinades persones o col·lectius i perpetuar patrons històrics de discriminació; per exemple, per motius d'origen racial o ètnic, gènere, discapacitat, edat o orientació sexual. També poden generar noves formes de discriminació. Tanmateix, els sistemes d'IA previstos pel dret de la Unió per detectar frau en l'oferta de serveis financers i, a efectes prudencials, per calcular els requisits de capital de les entitats de crèdit i les empreses d'assegurança no s'han de considerar d'alt risc segons el present Reglament. A més, els sistemes d'IA destinats a què se'n faci ús per avaluar riscos i la fixació de preus en relació amb les persones físiques en el cas de les assegurances de vida i de salut també poden afectar de manera considerable els mitjans de subsistència de les persones i, si no es dissenyen, desenvolupen i fan servir de la manera deguda, en poden vulnerar els drets fonamentals i poden tenir conseqüències greus per a la vida i la salut de les persones, com ara l'exclusió financera i la discriminació. Finalment, els sistemes d'IA emprats per avaluar i classificar trucades d'emergència de persones físiques o l'enviament o l'establiment de prioritats en l'enviament de serveis de primera intervenció en situacions d'emergència, inclosos policia, bombers i serveis d'assistència mèdica, i també sistemes de triatge de pacients per a l'assistència sanitària d'emergència, també s'han de considerar d'alt risc, ja que adopten decisions en situacions del tot crítiques per a la vida i la salut i la propietat de les persones.

(59) Atesa la seva funció i responsabilitat, les accions de les autoritats garants del compliment de la llei que involucren certs usos dels sistemes d'IA es caracteritzen per un grau significatiu de desequilibri de poder i poden conduir a la vigilància, detenció o privació de la llibertat d'una persona física, i a altres efectes adversos sobre els drets fonamentals garantits en la Carta. En particular, si no està entrenat amb dades de qualitat superior, no compleix els requisits adequats pel que fa al rendiment, la precisió o la solidesa, o no està dissenyat i provat correctament abans que s'introdueixi en el mercat o es posi en servei d'una altra manera, el sistema d'IA pot assenyalar les persones d'una manera discriminatòria, incorrecta o injusta. A més, podria impedir l'exercici d'importants drets processals fonamentals, com és el dret a la tutela judicial efectiva i a un jutge imparcial i, també, el dret a la defensa i a la presumpció d'innocència, principalment quan el sistema d'IA no sigui prou transparent i explicable ni estigui prou ben documentat. Per tant, en la mesura en què se'n permeti l'ús d'acord amb el dret de la Unió i el dret nacional aplicable, escau classificar com a d'alt risc diversos sistemes

d'IA adreçats a què se'n faci ús amb finalitats de garantia del compliment de la llei, quan la seva precisió, fiabilitat i transparència siguin especialment importants per evitar efectes adversos, conservar la confiança de la població i garantir la rendició de comptes i unes vies de recurs efectives. Atesa la naturalesa de les activitats i dels riscos connexos, entre els sistemes d'IA d'alt risc s'han d'incloure, en particular, els sistemes d'IA destinats a què les autoritats garants del compliment de la llei o, en nom seu, les institucions, òrgans o organismes de la Unió que els donen suport, en facin ús per avaluar el risc que una persona física sigui víctima de delictes, com ara els polígrafs i altres eines similars, per avaluar la fiabilitat de les proves durant la investigació o el processament judicial de delictes i, en la mesura que el Reglament no ho prohibeixi, per avaluar el risc que una persona física delinqueixi o reincideixi, no només sobre la base de l'elaboració de perfils de persones físiques o l'avaluació de trets i característiques de la personalitat o comportaments delictius passats de persones físiques o grups de persones, o per elaborar perfils durant la detecció, la investigació o el processament judicial de delictes. Els sistemes d'IA destinats específicament a ser utilitzats en processos administratius per les autoritats fiscals i duaneres i les unitats d'intel·ligència financera que exerceixen tasques administratives d'anàlisi d'informació de conformitat amb el dret de la Unió en matèria de lluita contra el blanqueig de capitals no s'han de classificar com a sistemes d'IA d'alt risc usats per les autoritats garants del compliment de la llei per prevenir, detectar, investigar i enjudiciar delictes. L'ús d'eines d'IA per part de les autoritats garants del compliment de la llei i altres autoritats competents no pot esdevenir un factor de desigualtat o d'exclusió. Cal no ignorar l'impacte de l'ús d'eines d'IA en els drets de defensa dels sospitosos; en particular, la dificultat per obtenir informació rellevant sobre el funcionament dels sistemes i la dificultat consegüent per impugnar-ne els resultats davant els tribunals; en particular, per part de les persones físiques investigades.

(60) Els sistemes d'IA emprats en la migració, l'asil i la gestió del control fronterer afecten persones que sovint estan en una situació especialment vulnerable i que depenen del resultat de l'actuació de les autoritats competents. Per això és del tot important que els sistemes d'IA que es facin servir en aquests contextos siguin precisos, no discriminatoris i transparents, per garantir que es respectin els drets fonamentals de les persones afectades i, en particular, que se'n respecti el dret a la lliure circulació, a la no discriminació, a la intimitat personal i la protecció de les dades personals, a la protecció internacional i a una bona administració. Així, en la mesura en què se'n permeti l'ús segons el dret de la Unió o nacional aplicable, cal considerar d'alt risc els sistemes d'IA que s'hagin de fer servir per, o nom de, les autoritats competents o per les institucions, òrgans, oficines o organismes de la Unió encarregats de funcions en els àmbits de la gestió de migracions, asil i control fronterer (per exemple, polígrafs i altres eines semblants) per avaluar determinats riscos que les persones físiques que entren en el territori d'un estat membre o que sol·liciten visat o asil; com a ajuda per a les autoritats competents en l'examen, inclosa l'avaluació relacionada de la fiabilitat de les proves aportades, de peticions d'asil, visat i permís de residència i les reclamacions associades en relació amb l'aptitud de les persones físiques que sol·liciten un reconeixement d'estatus, als efectes de detectar, reconèixer o identificar les persones físiques en el context de la gestió de migracions, asils i control fronterer, exceptuant-ne la verificació dels documents de viatge. Els sistemes d'IA en l'àmbit de la migració, l'asil i la gestió del control fronterer subjectes al Reglament han de complir els requisits procedimentals pertinents establerts pel Reglament (CE) 810/2009 del Parlament Europeu i

del Consell (32), la Directiva 2013/32/UE del Parlament Europeu i del Consell (33) i altres lleis de la Unió. L'ús dels sistemes d'IA en la migració, l'asil i la gestió del control fronterer no pot, en cap cas, servir als estats membres o les institucions, òrgans o organismes de la Unió com a mitjà per eludir les obligacions internacionals que els corresponen en virtut de la Convenció de les Nacions Unides sobre l'Estatut dels Refugiats, feta a Ginebra el 28 de juliol de 1951, modificada pel Protocol de 31 de gener de 1967. Tampoc no pot servir per infringir el principi de no devolució ni per negar vies legals segures i efectives d'accés al territori de la Unió, inclòs el dret a la protecció internacional.

(61) Certs sistemes d'IA destinats a l'administració de justícia i processos democràtics s'han de classificar com a d'alt risc, tenint-ne en compte els efectes potencialment significatius en la democràcia, l'estat de dret, les llibertats individuals i el dret a la tutela judicial efectiva i a un jutge imparcial. En particular, per afrontar el risc de possibles biaixos, errors i opacitats, escau classificar com a d'alt risc els sistemes d'IA destinats a què se'n faci ús per una autoritat judicial, o en nom seu, per ajudar les autoritats judicials en la investigació i interpretació dels fets i el dret i a aplicar la llei a uns fets concrets. També s'han de considerar d'alt risc els sistemes d'IA destinats a què els utilitzin els organismes de resolució alternativa de litigis amb aquestes finalitats, quan els resultats dels procediments de resolució alternativa de litigis provoquin efectes jurídics per a les parts. L'ús d'eines d'IA pot servir com a suport per al poder de decisió dels jutges o la independència judicial, però no el pot substituir. La presa de decisions final ha de continuar sent una activitat humana. Tanmateix, la classificació dels sistemes d'IA com a d'alt risc no es pot fer extensiva als sistemes d'IA destinats a activitats merament accessòries que no afecten l'administració de justícia en ella mateixa en casos concrets, com ara l'anonimització o la pseudonimització de resolucions judicials, documents o dades, la comunicació entre els membres del personal o les funcions administratives.

(62) Sense perjudici de les normes previstes en el Reglament (UE) 2024/900 del Parlament Europeu i del Consell (34), i amb la finalitat d'abordar els riscos d'interferència externa indeguda amb el dret de vot consagrat en l'article 39 de la Carta, i dels efectes adversos sobre la democràcia i l'estat de dret, s'han de classificar com a sistemes d'IA d'alt risc els sistemes d'IA destinats a fer-ne ús per influir en el resultat d'una elecció o un referèndum, o en el comportament electoral de les persones físiques en l'exercici del vot en eleccions o en referèndums, llevat dels sistemes d'IA amb resultats de sortida en què les persones físiques no estan exposades directament, com les eines utilitzades per organitzar, optimitzar i estructurar campanyes polítiques des d'un punt de vista administratiu i logístic.

(63) El fet que un sistema d'intel·ligència artificial sigui classificat com un sistema d'IA d'alt risc en virtut del Reglament no es pot interpretar com una indicació que l'ús del sistema és legítim en virtut d'altres actes del dret de la Unió o en virtut del dret nacional compatible amb el dret de la Unió; per exemple, en matèria de protecció de les dades personals o la utilització de polígrafs i eines similars o altres sistemes per detectar l'estat emocional de les persones físiques. Tot ús d'aquesta mena s'ha de continuar fent només en consonància amb els requisits oportuns derivats de la Carta i dels actes aplicables al dret derivat de la Unió i el dret nacional. Cal no entendre el Reglament com a un element que estableix la base que legitima el tractament de les dades personals, incloses categories especials de dades

personals, quan correspongui, llevat que s'estableixi específicament el contrari en el Reglament.

(64) Amb l'objectiu de mitigar els riscos que presenten els sistemes d'IA d'alt risc que s'introdueixen en el mercat o es posen en servei, i per garantir un alt nivell de fiabilitat, s'han d'aplicar als sistemes d'IA d'alt risc certs requisits obligatoris que tinguin en compte la finalitat prevista i el context de l'ús del sistema d'IA i estiguin en consonància amb el sistema de gestió de riscos que ha d'establir el proveïdor. Les mesures que els proveïdors adopten per complir els requisits obligatoris del present Reglament han de tenir en compte l'estat actual de la tècnica que generalment es reconeix en matèria d'IA i ser proporcionades i eficaces per assolir els objectius del present Reglament. Sobre la base del nou marc legislatiu, com s'aclareix en la Comunicació de la Comissió titulada "Guia blava" sobre l'aplicació de la normativa europea relativa als productes, de 2022, la norma general és que més d'un acte legislatiu de la legislació d'harmonització de la Unió pot ser aplicable a un producte, ja que la comercialització o la posada en servei només pot tenir lloc quan el producte compleix tota la legislació d'harmonització de la Unió aplicable. Els riscos dels sistemes d'IA coberts pels requisits del present Reglament es refereixen a aspectes diferents dels contemplats en la legislació d'harmonització de la Unió existent i, per tant, els requisits del present Reglament completarien el conjunt existent de legislació d'harmonització de la Unió. Per exemple, les màquines o els productes sanitaris que incorporen un sistema d'IA poden presentar riscos que els requisits essencials de salut i seguretat establerts en la legislació harmonitzada de la Unió no aborden, ja que la llei sectorial no aborda els riscos específics dels sistemes d'IA. Això requereix una aplicació simultània i complementària dels diferents actes legislatius. Per garantir la coherència i estalviar una càrrega administrativa sobrerera i costos innecessaris, els proveïdors d'un producte que contingui un o diversos sistemes d'IA d'alt risc, als quals s'apliquin els requisits del present Reglament i de la legislació d'harmonització de la Unió basats en el nou marc legislatiu i enumerats en un annex del present Reglament, han de ser flexibles pel que fa a les decisions operatives relatives a la manera de garantir la conformitat d'un producte que contingui un o diversos sistemes d'IA amb tots els requisits aplicables de la legislació harmonitzada de la Unió de manera òptima. La flexibilitat, per exemple, podria significar la decisió del proveïdor d'integrar una part dels processos de prova i notificació necessaris, a més de la informació i la documentació que s'exigeixen en virtut del Reglament, en la documentació i els procediments ja existents exigits en virtut de la legislació d'harmonització de la Unió vigent basats en el nou marc legislatiu i enumerats en un annex del Reglament. Això no ha de soscar, de cap manera, l'obligació del proveïdor de complir tots els requisits aplicables.

(65) El sistema de gestió de riscos ha de consistir en un procés continu i iteratiu que es planifica i s'executa durant tot el cicle de vida d'un sistema d'IA d'alt risc. Ha de tenir com a objectiu identificar i mitigar els riscos rellevants dels sistemes d'IA sobre la salut, la seguretat i els drets fonamentals. El sistema de gestió de riscos s'ha de revisar i actualitzar periòdicament per garantir-ne l'eficàcia constant, i també la justificació i la documentació de les decisions i accions significatives adoptades d'acord amb el present Reglament. Aquest procés ha de garantir que el proveïdor determini els riscos o efectes adversos i apliqui mesures de mitigació dels riscos coneguts i raonablement previsibles dels sistemes d'IA per a la salut, la seguretat i els drets fonamentals, tenint-ne en compte la finalitat prevista i l'ús indegut

raonablement previsible, inclosos els possibles riscos derivats de la interacció entre el sistema d'IA mateix i l'entorn en què aquest opera. El sistema de gestió de riscos ha d'adoptar les mesures de gestió de riscos més adequades d'acord amb l'estat de la tècnica en matèria d'IA. En determinar les mesures de gestió de riscos més adequades, el proveïdor ha de documentar i explicar les eleccions fetes i, quan escaigui, tenir la participació d'experts i parts interessades externes. En determinar l'ús indegut raonablement previsible dels sistemes d'IA d'alt risc, el proveïdor ha de tenir en compte els usos dels sistemes d'IA que, encara que no estiguin directament coberts per la finalitat prevista ni establerts en les instruccions d'ús, cal esperar raonablement que es derivin d'un comportament humà fàcilment previsible en el context de les característiques específiques i de l'ús d'un sistema d'IA concret. En les instruccions d'ús que el proveïdor faciliti s'ha d'incloure qualsevol circumstància coneguda o previsible, associada a la utilització del sistema d'IA d'alt risc conforme a la finalitat prevista o a un ús indegut raonablement previsible, que pugui donar lloc a riscos per a la salut i la seguretat o els drets fonamentals. Amb això es vol garantir que el responsable del desplegament en sigui conscient i els tingui en compte en fer servir el sistema d'IA d'alt risc. La identificació i l'aplicació de mesures de reducció del risc en cas d'ús indegut previsible d'acord amb el Reglament no ha de comportar l'exigència, perquè s'escometin, d'entrenament addicional específic per al sistema d'IA d'alt risc per part del proveïdor per afrontar usos indeguts previsibles. No obstant això, es recomana als proveïdors que considerin aquestes mesures d'entrenament addicionals per mitigar els usos indeguts raonables, quan es consideri raonable i oportú.

(66) S'han d'aplicar als sistemes d'IA d'alt risc requisits referents a la gestió de riscos, la qualitat i la pertinència dels conjunts de dades emprats, la documentació tècnica i la conservació de registres, la transparència i la comunicació d'informació als responsables del desplegament, la supervisió humana, la solidesa, la precisió i la ciberseguretat. Es tracta de requisits necessaris per mitigar de forma efectiva els riscos per a la salut, la seguretat i els drets fonamentals. Atesa la manca d'altres mesures menys restrictives del comerç, aquests requisits no són restriccions injustificades al comerç.

(67) Les dades d'alta qualitat i el fet d'accedir-hi desenvolupen un paper essencial en proporcionar una estructura i garantir el funcionament de molts sistemes d'IA; en particular, quan es fan servir tècniques que comporten l'entrenament de models, per garantir que el sistema d'IA d'alt risc funcioni de la manera prevista i en condicions de seguretat, sense esdevenir font de cap mena de discriminació prohibida pel dret de la Unió. Cal instaurar pràctiques adequades de gestió i governança de dades per aconseguir que els conjunts de dades per a l'entrenament, la validació i la prova siguin d'alta qualitat. Els conjunts de dades per a l'entrenament, la validació i les proves, incloses les etiquetes, han de ser rellevants, prou representatius i, fins on sigui possible, han d'estar lliures d'errors i complets tenint en compte la finalitat prevista del sistema. Per facilitar el compliment de la llei de la Unió en matèria de protecció de dades, com el Reglament (UE) 2016/679, les pràctiques de gestió i governança de dades han d'incloure, en el cas de les dades personals, la transparència sobre la finalitat original de la recopilació de dades. Els conjunts de dades també han de tenir les propietats estadístiques adequades, fins i tot pel que fa a les persones o grups de persones en relació amb les quals es vol fer servir el sistema d'IA d'alt risc, amb especial atenció a la mitigació de possibles biaixos en els conjunts de dades, això pot afectar la salut i la seguretat

de les persones, tenir un efecte advers en els drets fonamentals o conduir a la discriminació prohibida en el dret de la Unió, especialment quan els resultats de dades influeixen en les entrades per a futures operacions (bucles de retroalimentació). Els biaixos poden ser, per exemple, inherents als conjunts de dades subjacents, especialment quan s'utilitzen dades històriques, o generades quan els sistemes es despleguen en entorns del món real. Els resultats dels sistemes d'IA podrien estar influenciats per aquests biaixos inherents que tendeixen a augmentar gradualment i, per tant, a perpetuar i amplificar la discriminació existent: en particular, per a les persones que pertanyen a certs grups vulnerables, inclosos els grups racials o ètnics. El requisit que els conjunts de dades siguin complets i lliures d'errors, fins on sigui possible, no ha d'afectar l'ús de tècniques de preservació de la privadesa en el context del desenvolupament i les proves dels sistemes d'IA. En particular, en la mesura que la seva finalitat ho requereixi, els conjunts de dades han de tenir en compte les característiques, els trets o els elements que són particulars de l'entorn geogràfic, contextual, conductual o funcional específic per al qual es vol fer servir el sistema d'IA. Els requisits relacionats amb la governança de dades es poden complir mitjançant el recurs a tercers que ofereixen serveis de compliment certificat, incloent-hi la verificació de la governança de dades, la integritat del conjunt de dades, i pràctiques de formació, validació i proves de dades, en la mesura que es garanteixi el compliment dels requisits de dades del Reglament.

(68) Per al desenvolupament i l'avaluació de sistemes d'IA d'alt risc, certs actors, com ara proveïdors, organismes notificats i altres entitats rellevants –per exemple centres europeus d'innovació digital, instal·lacions d'experimentació i investigadors– han de poder accedir i emprar conjunts de dades d'alta qualitat en els àmbits d'activitats dels actors que estiguin relacionats amb el present Reglament. Els espais comuns de dades europeus establerts per la Comissió i la facilitació de l'intercanvi de dades entre empreses i amb governs d'interès públic seran fonamentals per proporcionar accés fiable, responsable i no discriminatori a dades d'alta qualitat per a la formació, validació i prova de sistemes d'IA. Per exemple, en salut, l'espai europeu de dades de salut ha de facilitar l'accés no discriminatori a les dades de salut i l'entrenament d'algoritmes d'intel·ligència artificial sobre aquests conjunts de dades, de manera que preservi la privadesa, sigui segura, oportuna, transparent i fiable, i amb una governança institucional adequada. Les autoritats competents pertinents, incloses les sectorials, que proporcionen l'accés a les dades o el faciliten, també poden donar suport al subministrament de dades d'alta qualitat per a l'entrenament, la validació i les proves de sistemes d'IA.

(69) El dret a la privadesa i a la protecció de les dades personals s'ha de garantir durant tot el cicle de vida del sistema d'IA. En aquest sentit, quan es tractin les dades personals, els principis de minimització de dades i protecció de dades per disseny i per defecte, segons el que estableix la legislació de protecció de dades de la Unió, són aplicables. Les mesures adoptades pels proveïdors per garantir-ne el compliment, a més d'incloure l'anonimització i el xifratge, també poden incloure l'ús d'una tecnologia que permeti portar els algorismes a les dades i l'entrenament dels sistemes d'IA sense que calgui la transmissió entre les parts ni la còpia de les dades en brut o estructurades; això, sense perjudici dels requisits aplicables en matèria de governança de dades establerts en el Reglament.

(70) A fi de protegir els drets de tercers davant la discriminació que podria provocar el biaix dels sistemes d'IA —amb caràcter excepcional i en la mesura que sigui estrictament necessari per garantir la detecció i correcció dels biaixos associats als sistemes d'IA d'alt risc, amb subjecció a les garanties adequades per als drets i llibertats fonamentals de les persones físiques i després de l'aplicació de totes les condicions aplicables establertes en el present Reglament, a més de les condicions establertes en els Reglaments (UE) 2016/679 i (UE) 2018/1725 i la Directiva (UE) 2016/680— els proveïdors han de poder tractar també categories especials de dades personals, com a qüestió d'interès públic essencial en el sentit de l'article 9, apartat 2, lletra g), del Reglament (UE) 2016/679 i de l'article 10, apartat 2, lletra g), del Reglament (UE) 2018/1725.

(71) Disposar d'informació entenedora sobre com s'han desenvolupat els sistemes d'IA d'alt risc i com funcionen aquests al llarg de la seva vida útil és essencial per permetre'n la traçabilitat, verificar que compleixen els requisits del present Reglament i seguir-ne les operacions i la postcomercialització. Per fer-ho, cal mantenir registres i tenir disponible documentació tècnica, amb la informació necessària per avaluar la conformitat del sistema d'IA amb els requisits pertinents i facilitar-ne el seguiment de postcomercialització. Aquesta informació ha d'incloure les característiques generals, les capacitats i les limitacions del sistema i els algorismes, dades i processos d'entrenament, prova i validació emprats, així com documentació sobre el sistema de gestió de riscos pertinent, elaborada de manera clara i completa. La documentació tècnica s'ha de mantenir degudament actualitzada durant tota la vida útil del sistema d'IA. A més, tècnicament, els sistemes d'IA d'alt risc han de permetre el registre automàtic d'esdeveniments, mitjançant arxius de registre, al llarg de la vida útil del sistema.

(72) Per abordar les preocupacions relacionades amb l'opacitat i la complexitat de certs sistemes d'IA i ajudar els responsables del desplegament a complir les obligacions que els corresponen en virtut del Reglament, s'ha d'exigir transparència als sistemes d'IA d'alt risc abans que s'introdueixin en el mercat o es posin en servei. El disseny dels sistemes d'IA d'alt risc ha de permetre als responsables del desplegament entendre com funciona el sistema d'IA, avaluar-ne la funcionalitat i comprendre'n les fortaleses i limitacions. Els sistemes d'IA d'alt risc s'han d'acompanyar amb informació adequada en forma d'instruccions d'ús. La informació ha d'incloure les característiques, capacitats i limitacions del rendiment del sistema d'IA. Han d'incloure la informació sobre les possibles circumstàncies conegudes i previsibles en relació amb l'ús del sistema d'IA d'alt risc, inclosa l'actuació del responsable del desplegament que pugui influir en el comportament i el funcionament del sistema, en el marc del qual el sistema d'IA pot comportar riscos per a la salut, la seguretat i els drets fonamentals, sobre els canvis que el proveïdor hagi predeterminat i avaluat per comprovar-ne la conformitat i sobre les mesures pertinents de supervisió humana, incloses les mesures per facilitar la interpretació dels resultats de sortida del sistema d'IA per part dels responsables del desplegament. La transparència, que inclou les instruccions d'ús, ha d'ajudar els responsables del desplegament en l'ús del sistema i facilitar-los la presa de decisions informades. Entre altres, els responsables del desplegament han d'estar en una millor posició per escollir correctament el sistema que volen fer servir d'acord amb les obligacions

que els són aplicables, haver rebut formació sobre els usos previstos i exclosos, i fer servir el sistema d'IA correctament i segons correspongui. Per millorar la llegibilitat i l'accessibilitat de la informació inclosa en les instruccions d'ús, si escau, cal incloure exemples il·lustratius; per exemple, sobre les limitacions i sobre els usos previstos i exclosos del sistema d'IA. Els proveïdors han d'assegurar que tota la documentació, incloses les instruccions d'ús, conté informació rellevant, completa, accessible i comprensible, que tingui en compte les necessitats i el coneixement previsible dels responsables del desplegament destinataris. Les instruccions d'ús s'han de posar a disposició en un idioma que els responsables del desplegament destinataris puguin entendre fàcilment, segons el que l'estat membre en qüestió determini.

(73) El disseny i desenvolupament dels sistemes d'IA d'alt risc ha de permetre que les persones físiques en puguin supervisar el funcionament, assegurar-se que l'ús que se'n fa és el que es vol i que al llarg del cicle de vida del sistema se n'aborden els efectes. Amb aquesta finalitat, el proveïdor del sistema ha d'identificar les mesures de supervisió humanes adequades abans d'introduir-lo en el mercat o posar-lo en servei. Quan escaigui, i en concret, les mesures han de garantir que el sistema estigui subjecte a limitacions operatives incorporades en el sistema mateix que aquest no pugui desactivar, que respongui a l'operador humà i que les persones físiques a qui s'hagi encomanat la supervisió humana tinguin les competències, la formació i l'autoritat necessàries per dur a terme la funció. També és essencial, garantir que els sistemes d'IA d'alt risc incloguin mecanismes destinats a orientar i informar les persones físiques a qui s'hagi assignat la supervisió humana perquè prenguin decisions amb coneixement de causa sobre si intervenir, quan fer-ho i de quina manera, a fi d'evitar conseqüències negatives o riscos, o d'aturar el sistema si no funciona segons el previst. Tenint en compte les conseqüències enormes per a les persones en cas d'una correspondència incorrecta feta per determinats sistemes d'identificació biomètrica, cal establir un requisit de supervisió humana reforçada per a aquests sistemes, de manera que el responsable del desplegament no pugui actuar ni prendre cap decisió basant-se en la identificació generada pel sistema, llevat que almenys dues persones físiques l'hagin verificat i confirmat per separat. Aquestes persones podrien procedir d'una o diverses entitats i incloure la persona que explota el sistema o en fa ús. Aquest requisit no ha de comportar una càrrega ni retards innecessaris i n'hi podria haver prou que les verificacions que les diferents persones facin per separat es registrin automàticament en els registres generats pel sistema. Ateses les especificitats de les àrees de garantia del compliment de la llei, migració, control fronterer i asil, no s'ha d'aplicar quan el dret de la Unió o el dret nacional considerin que aplicar-lo és desproporcionat.

(74) Els sistemes d'IA d'alt risc han de funcionar de manera uniforme durant tot el cicle de vida i presentar un nivell adequat de precisió, solidesa i ciberseguretat, a la llum de la finalitat que tenen prevista i d'acord amb l'estat actual de la tècnica generalment reconegut. Es recomana a la Comissió i les organitzacions i parts interessades pertinents que tinguin degudament en compte la mitigació dels riscos i les repercussions negatives del sistema d'IA. El nivell previst dels paràmetres de funcionament s'ha de declarar en les instruccions d'ús amb què s'acompanyin els sistemes d'IA. S'insta els proveïdors que comuniquin aquesta informació als responsables del desplegament de manera clara i fàcilment comprensible, sense malentesos ni afirmacions enganyoses. El dret de la Unió sobre metrologia legal, incloses les

Directives 2014/31/UE [\(35\)](#) i [2014/32/UE \(36\)](#) del Parlament Europeu i del Consell, té com a objectiu garantir l'exactitud de les mesures i contribuir a la transparència i l'equitat de les transaccions comercials. En aquest context, en cooperació amb les parts interessades i organitzacions rellevants, com ara les autoritats de metrologia i de paràmetres de referència, la Comissió ha de fomentar, si escau, el desenvolupament de paràmetres de referència i metodologies de mesurament per als sistemes d'IA. En fer-ho, la Comissió ha de prendre nota dels socis internacionals que treballen en la metrologia i els indicadors de mesurament pertinents relacionats amb la IA i col·laborar-hi.

(75) La solidesa tècnica és un requisit clau per als sistemes d'IA d'alt risc. Han de ser resistents en relació amb comportaments nocius o no desitjables que puguin resultar de limitacions dins els sistemes o l'entorn en què operen els sistemes (per exemple, errors, falles, incoherències, situacions inesperades). Per tant, s'han de prendre mesures tècniques i organitzatives per garantir la solidesa dels sistemes d'IA d'alt risc; per exemple, dissenyant i desenvolupant solucions tècniques adequades per prevenir o minimitzar comportaments nocius o no desitjables. Aquestes solucions tècniques poden incloure, per exemple, mecanismes que permetin al sistema interrompre de manera segura el funcionament (plans de prevenció contra falles) en presència de certes anomalies o quan l'operació tingui lloc fora de certs límits predeterminats. El fet de no adoptar mesures de protecció enfront d'aquests riscos podria tenir conseqüències per a la seguretat o afectar de manera negativa els drets fonamentals; per exemple, a causa de decisions equivocades o resultats de sortida erronis o esbiaixats generats pel sistema d'IA.

(76) La ciberseguretat és fonamental per garantir que els sistemes d'IA resisteixin davant les actuacions de tercers maliciosos que, aprofitant les vulnerabilitats del sistema, tractin d'alterar-ne l'ús, el comportament o el funcionament o de posar-ne en perill les propietats de seguretat. Els ciberatacs contra sistemes d'IA poden dirigir-se contra actius específics de la IA, com ara els conjunts de dades d'entrenament (p. ex., enverinament de dades) o els models entrenats (p. ex., atacs adversaris o inferència de pertinença), o aprofitar les vulnerabilitats dels actius digitals del sistema d'IA o la infraestructura de TIC subjacent. Per tant, per garantir un nivell de ciberseguretat adequat als riscos, els proveïdors de sistemes d'IA d'alt risc han d'adoptar mesures adequades, com ara els controls de seguretat, tenint també en compte, quan escaigui, la infraestructura de TIC subjacent.

(77) Sense perjudici dels requisits relacionats amb la solidesa i la precisió que s'estableixen en el Reglament, els sistemes d'IA d'alt risc que s'inscriguin en l'àmbit d'aplicació d'un reglament del Parlament Europeu i del Consell en matèria de requisits horitzontals de ciberseguretat per als productes amb elements digitals, de conformitat amb el Reglament mateix, poden demostrar que compleixen els requisits essencials de ciberseguretat que s'estableixen en el reglament esmentat. Quan els sistemes d'IA d'alt risc compleixen els requisits essencials de ciberseguretat d'un reglament del Parlament Europeu i del Consell relatiu als requisits horitzontals de ciberseguretat per als productes amb elements digitals, s'ha de presumir que compleixen els requisits de ciberseguretat del Reglament en la mesura que l'acompliment es demostrï en la declaració UE de conformitat emesa d'acord amb el reglament esmentat o amb parts d'aquest. Amb aquesta finalitat, l'avaluació dels riscos de ciberseguretat, associats

a un producte amb elements digitals classificats com a sistema d'IA d'alt risc segons el Reglament, feta en virtut d'un reglament del Parlament Europeu i del Consell sobre els requisits de ciberseguretat horitzontals per als productes amb elements digitals, ha de considerar els riscos per a la ciberresiliència d'un sistema d'IA pel que fa als intents de tercers no autoritzats d'alterar-ne l'ús, el comportament o el rendiment, incloses les vulnerabilitats específiques d'intel·ligència artificial, com ara l'enverinament de dades o els atacs adversaris, així com, si escau, els riscos per als drets fonamentals requerits pel Reglament.

(78) El procediment d'avaluació de la conformitat que el Reglament proporciona s'ha d'aplicar en relació amb els requisits essencials de ciberseguretat d'un producte amb elements digitals regulats per un reglament del Parlament Europeu i del Consell sobre els requisits de ciberseguretat horitzontals per a productes amb elements digitals i classificats com un sistema d'IA d'alt risc en virtut del Reglament. No obstant això, aquesta norma no ha de comportar la reducció del nivell de garantia necessari per als productes crítics amb elements digitals coberts per un reglament del Parlament Europeu i del Consell sobre els requisits de ciberseguretat horitzontal per als productes amb elements digitals. Per tant, com a excepció a la regla, els sistemes d'IA d'alt risc que s'integren en l'àmbit d'aplicació del present Reglament i que també es consideren productes importants i crítics amb elements digitals d'acord amb un reglament del Parlament Europeu i del Consell sobre els requisits de ciberseguretat horitzontals per als productes amb elements digitals i als quals es fa el procediment d'avaluació de la conformitat sobre la base del control intern establert en un annex del present Reglament, estan subjectes a les disposicions d'avaluació de la conformitat d'un reglament del Parlament Europeu i del Consell sobre els requisits de ciberseguretat horitzontals per als productes amb elements digitals en la mesura que es tracti dels requisits essencials de ciberseguretat del reglament en qüestió. En aquest cas, per a tots els altres aspectes que el present Reglament preveu, s'han d'aplicar les disposicions respectives sobre l'avaluació de la conformitat basada en el control intern establert en un annex al present Reglament. Basant-se en el coneixement i l'experiència d'ENISA sobre la política de ciberseguretat i les funcions assignades a ENISA en virtut del Reglament (UE) 2019/881 del Parlament Europeu i del Consell [\(37\)](#), la Comissió ha de cooperar amb ENISA en temes relacionats amb la ciberseguretat dels sistemes d'IA.

(79) És apropiat que una persona física o legal específica, definida com a proveïdora, assumeixi la responsabilitat de la introducció en el mercat o la posada en servei un sistema d'IA d'alt risc, independentment de si aquesta persona física o legal és la persona que va dissenyar o desenvolupar el sistema.

(80) Com a signataris de la Convenció de les Nacions Unides sobre els Drets de les persones amb discapacitat, la Unió i els estats membres estan obligats legalment a protegir les persones amb discapacitat de la discriminació i a promoure'n la igualtat, a garantir-los accés, en igualtat de condicions amb les altres, a les tecnologies i sistemes de la informació i les comunicacions, i a garantir el respecte a la privadesa de les persones amb discapacitat. Tenint en compte la importància i l'ús creixent dels sistemes d'IA, l'aplicació dels principis de disseny universal a totes les noves tecnologies i serveis hauria de garantir un accés ple i igualitari per a totes les persones potencialment afectades o que utilitzin tecnologies

d'intel·ligència artificial, incloses les persones amb discapacitat, d'una manera que en tingui plenament en compte la dignitat i diversitat. Per tant, és essencial que els proveïdors garanteixin el compliment ple dels requisits d'accessibilitat, inclosa la Directiva (UE) 2016/2102 del Parlament Europeu i del Consell [\(38\)](#) i la Directiva (UE) 2019/882. Els proveïdors han de garantir el compliment d'aquests requisits mitjançant el disseny. Per tant, les mesures necessàries s'han d'integrar tant com sigui possible en el disseny del sistema d'IA d'alt risc.

(81) El proveïdor ha d'establir un sistema de gestió de qualitat sòlid, garantir l'acompliment del procediment d'avaluació de la conformitat requerit, redactar la documentació pertinent i establir un sistema de seguiment postcomercialització robust. Els proveïdors de sistemes d'IA d'alt risc que estiguin subjectes a obligacions en matèria de sistemes de gestió de la qualitat en virtut de la legislació sectorial pertinent de la Unió han de tenir la possibilitat d'incloure els elements del sistema de gestió de la qualitat previst en el Reglament com a part del sistema de gestió de qualitat existent previst en l'altra legislació sectorial de la Unió. La complementarietat entre el Reglament i el dret sectorial de la Unió existent també s'ha de tenir en compte en les futures activitats de normalització o orientació adoptades per la Comissió. Les autoritats que posin en servei sistemes d'IA d'alt risc per a ús propi poden adoptar i aplicar les normes per al sistema de gestió de la qualitat com a part del sistema de gestió de la qualitat adoptat a escala nacional o regional, segons correspongui, tenint en compte les especificitats del sector i les competències i organització de l'autoritat pública interessada.

(82) Per permetre l'aplicació del present Reglament i crear un camp de joc equitatiu per als operadors, i, tenint en compte les diferents formes de posada a disposició dels productes digitals, és important assegurar que, en tot cas, una persona establerta a la Unió pugui proporcionar a les autoritats tota la informació necessària sobre el compliment d'un sistema d'IA. Per tant, abans de posar els sistemes d'IA a disposició de la Unió, els proveïdors establerts en tercers països, per mandat escrit, han de nomenar un representant autoritzat establert a la Unió. El representant autoritzat exerceix un paper fonamental en garantir el compliment dels sistemes d'IA d'alt risc introduïts en el mercat o posats en servei a la Unió pels proveïdors que no estiguin establerts a la Unió i que serveixin com a persona de contacte establerta a la Unió.

(83) Atesa la naturalesa i complexitat de la cadena de valor dels sistemes d'IA i d'acord amb el nou marc legislatiu, és essencial garantir la seguretat jurídica i facilitar el compliment del present Reglament. Per tant, cal aclarir el paper i les obligacions específiques dels operadors rellevants al llarg de la cadena de valor, per exemple, el dels importadors i distribuïdors que puguin contribuir al desenvolupament de sistemes d'IA. En determinades situacions, podrien exercir diverses funcions alhora i, en conseqüència, han de complir de manera acumulativa totes les obligacions pertinents que hi estan associades. Per exemple, un operador pot actuar com a distribuïdor i importador al mateix temps.

(84) Per garantir la seguretat jurídica, cal aclarir que, en certes condicions específiques, qualsevol distribuïdor, importador, responsable del desplegament o altre tercer s'ha de considerar un proveïdor d'un sistema d'IA d'alt risc i, per tant, ha d'assumir totes les obligacions pertinents. Aquest seria el cas si aquesta part posa el seu nom o marca en un sistema d'IA d'alt risc ja introduït en el mercat o posat en servei, sense perjudici de les disposicions contractuals que estipulen que les obligacions s'assignen d'una altra manera. Seria també el cas si aquesta part fes una modificació substancial d'un sistema d'IA d'alt risc que ja s'ha introduït en el mercat o posat en servei de manera que continuï sent un sistema d'IA d'alt risc d'acord amb el Reglament, o si modifica la finalitat prevista d'un sistema d'IA, inclòs un sistema d'IA d'ús general, que no ha estat classificat com a d'alt risc i que ja s'ha introduït en el mercat o posat en servei, de manera que el sistema d'IA esdevé un sistema d'IA d'alt risc d'acord amb el Reglament. Aquestes disposicions s'han d'aplicar sense perjudici de les disposicions més específiques establertes en determinades legislacions d'harmonització de la Unió basades en el nou marc legislatiu, juntament amb les quals s'ha d'aplicar el Reglament. Per exemple, l'article 16, apartat 2, del Reglament (UE) 2017/745, pel qual s'estableix que certs canvis no s'han de considerar modificacions d'un dispositiu que puguin afectar el compliment dels requisits aplicables, ha de continuar aplicant-se als sistemes d'IA d'alt risc que siguin productes sanitaris en el sentit del reglament esmentat.

(85) Els sistemes d'IA d'ús general es poden emprar com a sistemes d'IA d'alt risc per ells mateixos o ser components d'altres sistemes d'IA d'alt risc. Per tant, atenent-ne la naturalesa particular i per garantir un repartiment equitatiu de responsabilitat al llarg de la cadena de valor, els proveïdors de tals sistemes, amb independència que altres proveïdors en puguin fer ús com a sistemes d'IA d'alt risc per ells mateixos o com a components de sistemes d'IA d'alt risc, i tret que es disposi el contrari en el present Reglament, han de cooperar estretament amb els proveïdors dels sistemes d'IA d'alt risc corresponents perquè aquests puguin complir les obligacions pertinents en virtut del present Reglament, i també han de cooperar estretament amb les autoritats competents establertes en virtut del present Reglament.

(86) Quan, en les condicions establertes en el Reglament, el proveïdor que inicialment va introduir el sistema d'IA al mercat o el va posar en servei ja no es considerarà proveïdor a l'efecte del present Reglament. I, quan aquest proveïdor no ha exclòs expressament el canvi del sistema d'IA en un sistema d'IA d'alt risc, no obstant això, l'anterior proveïdor ha de cooperar estretament i posar a disposició la informació necessària i proporcionar l'accés tècnic raonablement esperat i altra assistència que es requereix per al compliment de les obligacions establertes en el present Reglament, en particular pel que fa al compliment de l'avaluació de conformitat dels sistemes d'IA d'alt risc.

(87) A més, quan un sistema d'IA d'alt risc que és un component de seguretat d'un producte que està dins l'àmbit de la legislació d'harmonització de la Unió basada en el nou marc legislatiu no s'introdueix en el mercat ni es posa en servei independentment del producte, el fabricant de productes definit en aquesta legislació ha de complir les obligacions del proveïdor

establertes en el Reglament i, en particular, ha de garantir que el sistema d'IA integrat en el producte final compleixi amb els requisits del Reglament.

(88) Al llarg de la cadena de valor d'IA, moltes parts sovint subministren sistemes, eines i serveis d'intel·ligència artificial, i també components o processos que el proveïdor integra en el sistema d'IA amb diversos objectius, inclòs l'entrenament del model, el reentrenament del model, la prova i avaluació del model, la integració en el programari o altres aspectes del desenvolupament de models. Aquestes parts tenen un paper important a jugar en la cadena de valor cap al proveïdor del sistema d'IA d'alt risc en què s'integren els seus sistemes d'IA, eines, serveis, components o processos, i han de proporcionar per escrit a aquest proveïdor informació, capacitats necessàries, accés tècnic i altra assistència basada en l'estat general reconegut de la tècnica, amb la finalitat de permetre al proveïdor complir plenament les obligacions establertes en el Reglament, sense comprometre els drets de propietat intel·lectual o secrets comercials propis.

(89) Els tercers que facin accessibles al públic eines, serveis, processos o components d'intel·ligència artificial diferents dels models d'IA d'ús general, no han de complir els requisits dirigits a les responsabilitats al llarg de la cadena de valor de la IA; en particular, envers el proveïdor que els hagi utilitzat o integrat, quan aquestes eines, serveis, processos, els components d'IA es fan accessibles sota una llicència lliure i de codi obert. S'ha de fomentar en general que els desenvolupadors d'eines, serveis, processos o components d'IA diferents dels models d'IA d'ús general apliquin pràctiques de documentació d'implantació general, com ara les targetes de model i els fulls de dades, com a una manera d'accelerar l'intercanvi d'informació al llarg de la cadena de valor de la IA, i això permet la promoció de sistemes d'IA fiables en la Unió.

(90) La Comissió podria desenvolupar i recomanar termes contractuals model voluntaris entre proveïdors de sistemes d'IA d'alt risc i tercers que subministrin eines, serveis, components o processos que s'utilitzen o s'integren en sistemes d'IA d'alt risc, per facilitar la cooperació al llarg de la cadena de valor. En elaborar clàusules contractual tipus, la comissió també ha de tenir en compte els possibles requisits contractuals aplicables en certs sectors o models de negoci.

(91) Atesa la naturalesa de les característiques dels sistemes d'IA i dels riscos que fer-ne ús comporta per a la seguretat i els drets fonamentals, també pel que fa a la necessitat la vigilància correcta del funcionament d'un sistema d'IA en un entorn real, cal establir les responsabilitats específiques dels responsables del desplegament. En particular, els responsables del desplegament han d'adoptar mesures tècniques i organitzatives adequades per garantir que fan servir els sistemes d'IA d'alt risc segons les instruccions d'ús. I cal, a més definir altres obligacions en relació amb el seguiment del funcionament dels sistemes d'IA i la conservació de registres, segons el cas. A més, els responsables del desplegament han de garantir que les persones a qui s'encomani la posada en pràctica de les instruccions d'ús i la supervisió humana establertes en el Reglament tinguin les competències necessàries; en

particular un nivell adequat d'alfabetització, formació i autoritat en matèria d'IA per dur a terme les tasques de manera adequada. Aquestes obligacions han de ser sense perjudici d'altres obligacions del responsable del desplegament en relació amb els sistemes d'IA d'alt risc previstes en el dret de la Unió o nacional.

(92) El present Reglament s'entén sense perjudici de les obligacions de l'empresa d'informar o d'informar i consultar els treballadors o els representants dels treballadors segons la legislació i la pràctica de la Unió nacional, inclosa la Directiva 2002/14/CE del Parlament Europeu i del Consell [\(39\)](#) sobre les decisions de posar en servei els sistemes d'IA o fer-ne ús. És necessari garantir la informació dels treballadors i els seus representants sobre el desplegament planificat de sistemes d'IA d'alt risc en el lloc de treball quan no es compleixin les condicions per a aquestes obligacions d'informació o informació i consulta en altres instruments legals. A més, aquest dret d'informació és complementari i necessari per a l'objectiu de protegir els drets fonamentals subjacents en el present Reglament. Per tant, s'ha d'establir un requisit d'informació a aquest efecte en el Reglament, sense que això afecti cap dret existent dels treballadors.

(93) Tot i que els riscos relacionats amb els sistemes d'IA poden ser el resultat de la forma en què aquests sistemes estan dissenyats, els riscos també poden derivar de com s'utilitzen aquests sistemes d'IA. Per tant, els responsables del desplegament del sistema d'IA d'alt risc tenen un paper fonamental en garantir que els drets fonamentals estan protegits, complementant les obligacions del proveïdor en el desenvolupament del sistema d'IA. Els responsables del desplegament estan més ben situats per entendre com s'ha de fer servir el sistema d'IA d'alt risc de forma concreta i, per tant, poden identificar riscos significatius potencials que no es van preveure en la fase de desenvolupament, a causa d'un coneixement més precís del context d'ús, les persones o grups de persones que probablement es veuran afectats, inclosos els col·lectius vulnerables. Els responsables del desplegament de sistemes d'IA d'alt risc que figuren en un annex del Reglament també juguen un paper fonamental en informar les persones físiques i, quan prenen decisions o ajuden en la presa de decisions relacionades amb les persones físiques, han d'informar les persones físiques del fet que estan subjectes a l'ús del sistema d'IA d'alt risc. Aquesta informació ha d'incloure la finalitat prevista i la mena de decisions que pren. El responsable del desplegament també ha d'informar les persones físiques sobre el dret que tenen a una explicació prevista en el Reglament. Pel que fa als sistemes d'IA d'alt risc utilitzats per a la garantia del compliment de la llei, aquesta obligació s'ha d'aplicar de conformitat amb l'article 13 de la Directiva (UE) 2016/680.

(94) Qualsevol tractament de dades biomètriques que impliqui l'ús de sistemes d'IA per a la identificació biomètrica a l'efecte de la garantia del compliment de la llei ha de complir l'article 10 de la Directiva (UE) 2016/680, que permet aquest tractament només quan sigui estrictament necessari, subjecte a les garanties adequades per als drets i llibertats de l'interessat, i quan estigui autoritzat pel dret de la Unió o dels estats membres. Quan estigui autoritzat, aquest ús també ha de respectar els principis establerts a l'article 4, apartat 1, de la Directiva (UE) 2016/680, que inclouen la legalitat, l'equitat i la transparència, la limitació de propòsit, l'exactitud i la limitació de l'emmagatzematge.

(95) Sense perjudici del dret aplicable a la Unió, en particular el Reglament (UE) 2016/679 i la Directiva (UE) 2016/680, atesa la naturalesa intrusiva, l'ús de sistemes d'identificació biomètrica remota en diferit ha d'estar subjecte a garanties. Els sistemes d'identificació biomètrica en diferit s'han de fer servir sempre de manera proporcionada i legítima, fins on sigui estrictament necessari i, per tant, de manera selectiva pel que fa a les persones que s'han d'identificar, la ubicació i l'abast temporal i a partir d'un conjunt limitat de dades d'enregistrament de vídeo obtingudes legalment. En qualsevol cas, els sistemes d'identificació biomètrica remota en diferit no s'han de fer servir en el marc de la garantia del compliment de la llei per conduir a una vigilància indiscriminada. Les condicions per a la identificació biomètrica remota en diferit no poden proporcionar en cap cas una base per eludir les condicions de la prohibició i les excepcions estrictes per a la identificació biomètrica remota en temps real.

(96) Per garantir de manera eficient que es protegeixin els drets fonamentals, els responsables del desplegament de sistemes d'IA d'alt risc que són organismes regulats pel dret públic, les entitats privades que prestin serveis públics i els responsables del desplegament de determinats sistemes d'IA d'alt risc que figuren en un annex del Reglament, com ara les entitats bancàries o d'assegurances, han de dur a terme una avaluació d'impacte dels drets fonamentals abans de posar-lo en funcionament. Els serveis importants per a les persones de caràcter públic també els poden prestar entitats privades. Les entitats privades que prestin aquests serveis públics estan vinculades a funcions d'interès públic; per exemple, en l'àmbit de l'educació, l'assistència sanitària, els serveis socials, l'habitatge i l'administració de justícia. L'objectiu de l'avaluació d'impacte dels drets fonamentals és que el responsable del desplegament identifiqui els riscos específics per als drets de les persones o grups de persones que puguin veure's afectades, i que identifiqui les mesures que s'han de prendre si els riscos es materialitzen. L'avaluació d'impacte s'ha de fer abans de desplegar el sistema d'IA d'alt risc, i s'ha d'actualitzar quan el responsable del desplegament considera que algun dels factors rellevants han canviat. L'avaluació d'impacte ha de determinar els processos pertinents del responsable del desplegament en què s'utilitzarà el sistema d'IA d'alt risc en consonància amb la finalitat que tenen prevista i ha d'incloure una descripció del termini i la freqüència en què es vol utilitzar el sistema, i també de les categories concretes de persones físiques i de col·lectius de persones que probablement es veuran afectats per l'ús del sistema d'IA d'alt risc en aquest context d'ús específic. També ha de determinar els riscos de perjudici específics que probablement els afectaran els drets fonamentals. En avaluar, el responsable del desplegament ha de tenir en compte la informació pertinent per a una avaluació adequada de l'impacte, la qual cosa inclou, entre altres, la informació facilitada pel proveïdor del sistema d'IA d'alt risc en les instruccions d'ús. Atesos els riscos identificats, els responsables del desplegament han de determinar les mesures que s'han d'adoptar en cas que els riscos es materialitzin, entre les quals hi ha, per exemple, sistemes de governança per al context d'ús específic, com ara els mecanismes de supervisió humana d'acord amb les instruccions d'ús i els procediments de tramitació de reclamacions i de recurs, ja que poden ser fonamentals per mitigar els riscos per als drets fonamentals en casos d'ús concret. Després de fer l'avaluació d'impacte, el responsable del desplegament ha de notificar a l'autoritat de vigilància del mercat corresponent. Si cal, per recollir informació rellevant necessària per fer l'avaluació d'impacte, els responsables del desplegament d'un sistema

d'IA d'alt risc, en particular quan s'utilitzen sistemes d'IA en el sector públic, podrien involucrar les parts interessades pertinents, inclosos els representants de grups de persones susceptibles de ser afectades pel sistema d'IA, experts independents, i les organitzacions de la societat civil en la pràctica d'aquestes avaluacions d'impacte i en el disseny de mesures que s'han de prendre en el cas de la materialització dels riscos. L'Oficina Europea d'Intel·ligència Artificial (Oficina d'IA) ha de crear un model de qüestionari per facilitar el compliment i reduir la càrrega administrativa per als responsables del desplegament.

(97) El concepte de models d'IA d'ús general s'ha de definir clarament i diferenciar del concepte de sistemes d'IA per garantir la seguretat jurídica. La definició s'ha de basar en les característiques funcionals essencials d'un model d'IA d'ús general; en particular, la generalitat i la capacitat de desenvolupar de manera competent una àmplia varietat de tasques diferenciades. Aquests models solen entrenar-se amb grans volums de dades i a través de diversos mètodes, com l'aprenentatge autosupervisat, no supervisat o per reforç. Els models d'IA d'ús general es poden introduir en el mercat de diverses maneres, per exemple, a través de biblioteques, interfícies de programació d'aplicacions (API), com a descàrrega directa o com a còpia física. Aquests models es poden modificar o perfeccionar i transformar en models nous. Tot i que són components essencials dels sistemes d'IA, els models d'IA no constitueixen sistemes d'IA per si sols. Els models d'IA requereixen l'addició de components addicionals com, per exemple, una interfície d'usuari per convertir-se en sistemes d'IA. Els models d'IA solen estar integrats en els sistemes d'IA i formar-ne part. El Reglament estableix normes específiques per als models d'IA d'ús general i per als models d'IA d'ús general que plantegen riscos sistèmics, que també s'han d'aplicar quan aquests models s'integren en un sistema d'IA o en formen part. S'ha d'entendre que les obligacions dels proveïdors de models d'IA d'ús general s'han d'aplicar una vegada que els models d'IA d'ús general s'introdueixin en el mercat. Quan el proveïdor d'un model d'IA d'ús general integra un model propi en el sistema d'IA propi que es posa a disposició del mercat o es posa en servei, aquest model s'ha de considerar introduït en el mercat i, per tant, les obligacions del Reglament per als models han de continuar aplicant-se a més de les dels sistemes d'IA. Les obligacions establertes per als models no s'han d'aplicar en cap cas quan s'utilitzi un model propi per a processos purament interns que no siguin essencials per al subministrament d'un producte o un servei a tercers i els drets de les persones físiques no es vegin afectats. Tenint-ne en compte els possibles efectes significativament negatius, els models d'IA d'ús general amb risc sistèmic han d'estar sempre subjectes a les obligacions pertinents del present Reglament. La definició no ha de cobrir els models d'IA utilitzats abans que s'introdueixin en el mercat amb l'únic propòsit d'activitats de recerca, desenvolupament i prototipatge. Això s'entén sense perjudici de l'obligació de complir el Reglament quan, seguint aquestes activitats, un model s'introdueixi en el mercat.

(98) Per bé que la generalitat d'un model també es podria determinar, entre altres, mitjançant diversos paràmetres, cal tenir present que els models amb almenys mil milions de paràmetres, i entrenats amb un gran volum de dades mitjançant l'autosupervisió a escala, presenten un grau notable de generalitat i, de manera competent, duen a terme una àmplia varietat de funcions diferenciades.

(99) Els grans models generatius d'IA són un exemple típic d'un model d'IA d'ús general, ja que permeten una generació flexible de continguts –com ara text, àudio, imatges o vídeo– que poden adaptar-se fàcilment a una àmplia gamma de funcions distintives.

(100) Quan un model d'IA d'ús general s'integra o forma part d'un sistema d'IA, aquest sistema ha de ser considerat com un sistema d'IA d'ús general quan, a causa de la integració, té la capacitat de servir a una varietat de propòsits. Un sistema d'IA d'ús general es pot emprar directament o es pot integrar en altres sistemes d'IA.

(101) Els proveïdors de models d'IA d'ús general tenen un paper i una responsabilitat particulars al llarg de la cadena de valor d'IA, ja que els models que proporcionen poden ser la base d'una gamma de sistemes posteriors, sovint proporcionats per proveïdors que necessiten un bon coneixement dels models i les seves capacitats, tant per permetre'n la integració en els seus productes com per complir les obligacions que els corresponen en virtut del present o altres reglaments. Per tant, s'han d'establir mesures de transparència proporcionades, inclosa l'elaboració i el manteniment actualitzats de la documentació, i la informació sobre el model d'IA d'ús general perquè els proveïdors posteriors en facin ús. La documentació tècnica s'ha d'elaborar i actualitzar pel proveïdor de models d'IA d'ús general amb la finalitat de posar-la a disposició, prèvia sol·licitud, de l'Oficina d'IA i de les autoritats nacionals competents. El conjunt mínim d'elements que s'han d'incloure en aquesta documentació s'ha de fixar en annexos específics del Reglament. La Comissió ha de poder modificar aquests annexos mitjançant actes delegats a la llum de l'evolució tecnològica.

(102) El programari i les dades, inclosos els models, publicats sota una llicència lliure i de codi obert que permet que es comparteixin obertament i en què els usuaris poden accedir, fer-ne ús, modificar-los i redistribuir-los o redistribuir-ne versions modificades, pot contribuir a la recerca i la innovació en el mercat i pot proporcionar importants oportunitats de creixement per a l'economia de la Unió. Cal considerar que els models d'IA d'ús general divulgats d'acord amb una llicència lliure i de codi obert garanteixen nivells alts de transparència i obertura i els seus paràmetres, inclosos els pesos, la informació sobre l'arquitectura del model i la informació sobre l'ús del model, es posen a disposició pública. La llicència s'ha de considerar lliure i de codi obert, també quan permeti als usuaris executar, copiar, distribuir, estudiar, canviar i millorar el programari i les dades, inclosos els models, si el proveïdor original del model se cita i es respecten unes condicions de distribució idèntiques o comparables.

(103) Els components d'IA de codi obert i lliure cobreixen el programari i les dades, incloent-hi models i models d'IA d'ús general, eines, serveis o processos d'un sistema d'IA. Els components d'IA de codi obert i lliure es poden proporcionar a través de diferents canals, incloent-ne el desenvolupament en repositoris oberts. A l'efecte del Reglament, els components d'IA que es proporcionen contra un preu o d'una altra manera monetitzats, fins i tot mitjançant la prestació de suport tècnic o altres serveis, fins i tot a través d'una plataforma de programari, relacionada amb el component d'IA, o l'ús de dades

personals per raons diferents de les exclusives per millorar la seguretat, compatibilitat o interoperabilitat del programari, amb l'excepció de les transaccions entre microempreses, no ha de beneficiar-se de les excepcions proporcionades als components d'IA lliures i de codi obert. El fet de fer que els components d'IA estiguin disponibles a través de repositoris oberts no hauria de constituir, en si mateix, una monetització.

(104) Els proveïdors de models d'IA d'ús general que es publiquen sota una llicència lliure i de codi obert, i els paràmetres, inclosos els pesos, la informació sobre l'arquitectura del model, i la informació sobre l'ús del model, que es posin a disposició del públic han d'estar subjectes a excepcions pel que fa als requisits relacionats amb la transparència imposats als models d'IA d'ús general, llevat que es pugui considerar que presenten un risc sistèmic. En aquest cas, la circumstància que el model sigui transparent i acompanyat d'una llicència de codi obert no s'ha de considerar com raó suficient per excloure el compliment de les obligacions del Reglament. En qualsevol cas, atès que la publicació de models d'IA d'ús general sota llicència lliure i de codi obert no revela necessàriament informació substancial sobre el conjunt de dades utilitzat per a l'entrenament o ajust del model i sobre com es va garantir el compliment de la llei de drets d'autor, l'excepció prevista per als models d'IA d'ús general del compliment dels requisits relacionats amb la transparència no ha de preocupar l'obligació de produir un resum sobre el contingut utilitzat per a l'entrenament de models i l'obligació de posar en marxa una política de compliment de la llei de drets d'autor de la Unió, en particular, identificar i complir amb la reserva de drets de conformitat amb l'article 4, apartat 3, de la Directiva (UE) 2019/790 del Parlament Europeu i del Consell [\(40\)](#).

(105) Els models d'IA d'ús general, en particular els grans models generatius d'IA, capaços de generar text, imatges i altres continguts, presenten oportunitats d'innovació úniques, però també reptes, per als artistes, autors i altres creadors i la manera en què es crea, distribueix, utilitza i se'n consumeix el contingut creatiu. El desenvolupament i l'entrenament d'aquests models requereixen l'accés a grans quantitats de text, imatges, vídeos i altres dades. Les tècniques de mineria de text i dades es poden fer servir àmpliament en aquest context per a la recuperació i anàlisi d'aquest contingut, que pot ser protegit per drets d'autor i drets relacionats. Tot ús de contingut protegit per drets d'autor requereix l'autorització del titular dels drets de què es tracti, tret que s'apliquin les excepcions i limitacions corresponents en matèria de drets d'autor. La Directiva (UE) 2019/790 va introduir excepcions i limitacions que permeten reproduccions i extraccions d'obres i altres prestacions amb finalitats de prospecció de textos i dades en circumstàncies determinades. D'acord amb aquestes normes, els titulars de dret poden optar per reservar-se els drets en relació amb les seves obres o altres prestacions per evitar la prospecció de textos i dades, tret que tinguin com a finalitat la recerca científica. Quan el titular de dret s'hagi reservat de manera adequada el dret d'exclusió, els proveïdors de models d'IA d'ús general n'han de tenir l'autorització per dur a terme una prospecció de textos i dades amb aquestes obres.

(106) Els proveïdors que introdueixin models d'IA d'ús general en el mercat de la Unió han de garantir el compliment de les obligacions pertinents en el present Reglament. Amb aquesta finalitat, els proveïdors de models d'IA d'ús general han d'adoptar una política per complir el dret de la Unió en matèria de drets d'autor i drets afins; en particular, per detectar i

complir la reserva de drets expressada pels titulars de drets d'acord amb l'article 4, apartat 3, de la Directiva (UE) 2019/790. El proveïdor que introdueixi un model d'IA d'ús general en el mercat de la Unió ha de complir aquesta obligació, amb independència de quina sigui la jurisdicció on tinguin lloc els actes pertinents en matèria de drets d'autor que sustenten l'entrenament dels models d'IA d'ús general. Es tracta d'una mesura necessària per garantir condicions de competència equitatives entre els proveïdors de models d'IA d'ús general que impedeixin que un proveïdor obtingui un avantatge competitiu en el mercat de la Unió aplicant normes en matèria de drets d'autor menys estrictes que les que hi ha establertes a la Unió.

(107) Per augmentar la transparència en relació amb les dades emprades en el preentrenament i l'entrenament dels models d'IA d'ús general, inclosos els textos i les dades protegides pel dret en matèria de drets d'autor, es cau que els proveïdors dels models elaborin i posin a disposició del públic un resum prou detallat dels continguts emprats per a l'entrenament del model d'IA d'ús general. El resum ha de tenir degudament en compte la necessitat de protegir els secrets comercials i la informació empresarial confidencial i, alhora, ha de ser exhaustiu en general pel que fa a l'abast, en comptes de ser tècnicament detallat, perquè faciliti que les parts amb interessos legítims, inclosos els titulars de drets d'autor exerceixin i facin complir els seus drets en virtut del dret de la Unió; per exemple, enumerant els conjunts o les recopilacions principals de dades que hagin servit per entrenar el model, com ara els grans arxius de dades o bases de dades privades o públiques, i aportant una explicació descriptiva sobre altres fonts de dades emprades. Convé que l'Oficina d'IA faciliti un model per al resum, que sigui senzill i eficaç i permeti que el proveïdor aporti el resum que es requereix de manera descriptiva.

(108) Pel que fa a les obligacions que s'imposen als proveïdors de models d'IA d'ús general d'adoptar directrius per al compliment de la llei de la Unió en matèria de drets d'autor i de posar a disposició del públic un resum dels continguts emprats per a l'entrenament, l'Oficina d'IA ha de supervisar si el proveïdor ha complert les obligacions sense verificar ni avaluar obra per obra les dades d'entrenament pel que fa a l'observança dels drets d'autor. El present Reglament no afecta el compliment efectiu de les normes en matèria de drets d'autor previstes en el dret de la Unió.

(109) El compliment de les obligacions aplicables als proveïdors de models d'IA d'ús general ha de ser proporcional i adequat al tipus de proveïdor de models, eximint de l'obligació de compliment les persones que desenvolupen o fan servir models per a finalitats no professionals o de recerca científica. Tanmateix, cal animar aquestes persones al compliment voluntari. Sense perjudici del dret de la Unió en matèria de drets d'autor, el compliment de les obligacions esmentades ha de tenir en compte l'envergadura del proveïdor i permetre formes simplificades de compliment per a les pimes, incloses les empreses emergents, que no poden comportar un cost excessiu ni desincentivar l'ús dels models. Si es modifica o s'ajusta un model, les obligacions dels proveïdors de models d'IA d'ús general s'han de limitar a l'ajustament o modificació en concret; per exemple, complementant la documentació tècnica que ja hi ha amb informació sobre les

modificacions, incloses les noves fonts de dades d'entrenament, per complir les obligacions relacionades amb la cadena de valor establertes en el Reglament.

(110) Els models d'IA d'ús general poden plantejar riscos sistèmics, com ara qualsevol efecte negatiu real o raonablement previsible en relació amb accidents greus, perturbacions de sectors crítics i conseqüències greus per a la salut i la seguretat públiques, qualsevol efecte negatiu real o raonablement previsible sobre els processos democràtics i la seguretat pública i econòmica o la difusió de continguts il·lícits, falsos o discriminatoris. S'ha de considerar que els riscos sistèmics augmenten amb les capacitats i l'abast del model, poden sorgir al llarg de tot el cicle de vida del model i depenen de les condicions d'ús indegut, fiabilitat del model, equitat de model i seguretat del model, el nivell d'autonomia del model, el seu accés a eines, noves o combinades modalitats, estratègies d'alliberament i distribució, el potencial per eliminar les garanties i altres factors. En particular, els enfocaments internacionals han establert fins a la data la necessitat de parar atenció als riscos derivats de possibles usos indeguts intencionats o de problemes en matèria de control relacionats amb l'harmonització amb la intenció humana no desitjats, als riscos químics, biològics, radiològics i nuclears, com les maneres en què les barreres a l'entrada poden reduir-se, també per al desenvolupament, el disseny, l'adquisició o l'ús d'armes, a les cibercapacitats ofensives, com les maneres en què es poden propiciar el descobriment, l'explotació o l'ús operatiu de vulnerabilitats, als efectes de la interacció i l'ús d'eines, inclosa, per exemple, la capacitat de controlar sistemes físics i interferir en el funcionament d'infraestructures crítiques, als riscos derivats del fet que els models facin còpies de si mateixos o s'«autorepliquin» o entrin a altres models, a les maneres en què els models poden donar lloc a biaixos danyosos i discriminació que comporten riscos per a les persones, les comunitats o les societats, a la facilitació de la desinformació o el menyscabament de la intimitat, que suposen una amenaça per als valors democràtics i els drets humans, al risc que un esdeveniment concret doni lloc a una reacció en cadena amb efectes negatius considerables que podrien afectar fins i tot una ciutat sencera, un àmbit d'activitat sencer o una comunitat sencera.

(111) Convé establir una metodologia per a la classificació dels models d'IA d'ús general com a models d'IA d'ús general amb riscos sistèmics. Atès que els riscos sistèmics es deriven de capacitats especialment altes, cal considerar que un model d'IA d'ús general presenta riscos sistèmics si té capacitats d'alt impacte –avaluades mitjançant eines i metodologies tècniques adequades– o repercussions considerables en el mercat interior per l'abast que tenen. Les capacitats d'alt impacte en models d'IA d'ús general són capacitats que coincideixen o superen les capacitats mostrades pels models d'IA d'ús general més avançats. La gamma completa de capacitats en un model es podria entendre millor després que s'hagi introduït en el mercat o quan els responsables del desplegament hi interactuïn. D'acord amb l'estat de la tècnica en el moment de l'entrada en vigor del present Reglament, la quantitat acumulada de càlcul utilitzada per a l'entrenament del model d'IA d'ús general mesurada en operacions de punt flotant és una de les aproximacions pertinents per a les capacitats del model. La quantitat acumulada de càlcul emprat per a l'entrenament inclou els càlculs emprats en les diferents activitats i mètodes que es destinen a millorar les capacitats del model abans del desplegament, com ara el preentrenament, la generació de dades sintètiques i la introducció d'ajustaments. Per tant, cal fixar un llindar inicial

d'operacions de punt flotant, que, si es compleix amb un model d'IA d'ús general, condueix a la presumpció que el model és un model d'IA d'ús general amb riscos sistèmics. Aquest llistat s'ha d'anar ajustant perquè es reflecteixin els canvis tecnològics i industrials, com ara les millores dels algorismes o l'augment de l'eficiència del maquinari, i s'ha de complementar amb paràmetres de referència i indicadors de la capacitat dels models. Per fonamentar-ho, l'Oficina d'IA ha de col·laborar amb la comunitat científica, la indústria, la societat civil i altres experts. Els llistats, i també les eines i els paràmetres de referència per a l'avaluació de les capacitats d'alt impacte, han de ser predictors sòlids de la generalitat, les capacitats i el risc sistèmic associat dels models d'IA d'ús general, i podrien tenir en compte la manera en què el model s'introduirà en el mercat o el nombre d'usuaris que pugui afectar. Per complementar aquest sistema, la Comissió ha de poder prendre decisions individuals que designin un model d'IA d'ús general com a model d'IA d'ús general amb risc sistèmic si es troba que aquest model té capacitats o un impacte equivalent a les capacitats captades pel llistat establert. La decisió s'ha d'adoptar atenent una avaluació global dels criteris per a la designació de models d'IA d'ús general amb risc sistèmic establerts en un annex del present Reglament, com la qualitat o la mida del conjunt de dades d'entrenament, el nombre d'usuaris professionals i finals, les seves modalitats d'entrada i de sortida, el seu nivell d'autonomia i escalabilitat o les eines a què té accés. Prèvia sol·licitud motivada d'un proveïdor de qui el model s'hagi designat com a model d'IA d'ús general amb risc sistèmic, la Comissió ha de tenir en compte la sol·licitud i poder decidir reavaluar si continua sent possible considerar que el model d'IA presenta riscos sistèmics.

(112) També cal aclarir un procediment per a la classificació d'un model d'IA d'ús general amb riscos sistèmics. Un model d'IA d'ús general que compleixi el llistat aplicable per a les capacitats d'alt impacte s'ha de considerar un model d'IA d'ús general amb risc sistèmic. Sense que hagin passat més de dues setmanes després del compliment dels requisits o se sàpiga que un model d'IA d'ús general complirà els requisits que condueixen a la presumpció, el proveïdor ha de notificar l'Oficina d'IA. Això té rellevància especial en relació amb el llistat de les operacions de punt flotant perquè l'entrenament dels models d'IA d'ús general requereix una planificació considerable que inclou l'assignació inicial de recursos. I, per tant, els proveïdors de models d'IA d'ús general poden saber si el seu model assoliria el llistat abans que l'entrenament es completi. En el context de la notificació, el proveïdor ha de poder demostrar que, per les seves característiques específiques, un model d'IA d'ús general excepcionalment no presenta riscos sistèmics, i que, per tant, no s'ha de classificar com un model d'IA d'ús general amb riscos sistèmics. Es tracta d'una informació valuosa per a l'Oficina d'IA, perquè pugui prevenir la introducció en el mercat de models d'IA d'ús general amb riscos sistèmics i els proveïdors puguin començar a interactuar ben aviat amb l'Oficina d'IA. Aquesta informació és especialment important quan estigui previst divulgar un model d'IA d'ús general com a model de codi obert, atès que, després de la divulgació de models de codi obert, pot resultar més difícil aplicar les mesures necessàries per garantir el compliment de les obligacions establertes en el present Reglament.

(113) Si la Comissió adquireix coneixement del fet que un model d'IA d'interès general compleix els requisits perquè se'l consideri model d'IA d'ús general amb risc sistèmic, prèviament desconegut o del qual el proveïdor corresponent no hagi notificat la Comissió, aquesta ha d'estar facultada per designar-l'hi. Un sistema d'alertes qualificades ha de garantir que

l'Oficina d'IA sigui coneixedora, a través del comitè científic, de l'existència de models d'IA d'ús general que podrien considerar-se models d'IA d'ús general amb risc sistèmic, a més de dur a terme les activitats de supervisió de l'Oficina d'IA.

(114) A més d'estar subjectes a les obligacions que s'imposen als proveïdors de models d'IA d'ús general, els proveïdors de models d'IA d'ús general que presentin riscos sistèmics han d'estar subjectes a obligacions encaminades a detectar i atenuar els riscos esmentats i a garantir un nivell adequat de protecció en matèria de seguretat, amb independència de si els models esmentats s'ofereixen com a models independents o estan integrats en sistemes d'IA o en productes. Per assolir aquests objectius, el present Reglament ha d'exigir als proveïdors que facin les avaluacions de models necessàries, en particular abans que s'introdueixin per primera vegada en el mercat, incloent-hi l'execució i documentació de les proves adversàries dels models, també, si escau, a través de proves externes internes o independents. A més, els proveïdors de models d'IA d'ús general amb riscos sistèmics han d'avaluar i mitigar contínuament els riscos sistèmics, per exemple, mitjançant l'establiment de polítiques de gestió de riscos, com processos de rendició de comptes i governança, la posada en pràctica de la vigilància postcomercialització, l'adopció de mesures adequades durant tot el cicle de vida del model i la cooperació amb els agents pertinents al llarg de la cadena de valor de la IA.

(115) Els proveïdors de models d'IA d'ús general amb riscos sistèmics han d'avaluar i mitigar possibles riscos sistèmics. Si, malgrat els esforços per identificar i prevenir riscos relacionats amb un model d'IA d'ús general que pugui presentar riscos sistèmics, el desenvolupament o l'ús del model provoca un incident greu, el proveïdor de models d'IA d'ús general, sense demora indeguda, ha de fer un seguiment de la informació pertinent i les possibles mesures correctores i comunicar-ho a la Comissió i a les autoritats nacionals competents. A més, els proveïdors han de garantir que el model i la seva infraestructura física, si escau, tinguin un nivell adequat de protecció en matèria de ciberseguretat durant tot el cicle de vida del model. La protecció en matèria de ciberseguretat relacionada amb els riscos sistèmics associats a l'ús malintencionat o als atacs ha de tenir degudament en compte les fugites accidentals de models, les divulgacions no autoritzades, l'elusió de les mesures de seguretat i la defensa contra els ciberatacs, l'accés no autoritzat o el robatori de models. Aquesta protecció podria facilitar-se assegurant els pesos, els algorismes, els servidors i els conjunts de dades del model, per exemple, mitjançant mesures de seguretat operativa per a la seguretat de la informació, mesures específiques en matèria de ciberseguretat, solucions tècniques adequades i establertes i controls d'accés cibernètics i físics, en funció de les circumstàncies pertinents i els riscos existents.

(116) L'Oficina d'IA ha de fomentar i facilitar l'elaboració, revisió i adaptació de codis de bones pràctiques, tenint en compte els enfocaments internacionals. Es podria convidar tots els proveïdors de models d'IA d'ús general a participar-hi. Per assegurar que els codis de bones pràctiques reflecteixen l'estat de la tècnica i tenen en compte degudament un conjunt divers de perspectives, l'Oficina d'IA ha de col·laborar amb les autoritats nacionals competents pertinents i poder, si escau, consultar amb organitzacions de la societat civil i altres parts interessades i experts rellevants, inclòs el comitè científic, per a l'elaboració

dels codis. Els codis de bones pràctiques han de comprendre les obligacions dels proveïdors de models d'IA d'ús general i de models d'IA d'ús general que presentin riscos sistèmics. A més, pel que fa als riscos sistèmics, els codis de bones pràctiques han d'ajudar a establir una taxonomia de riscos en què figurin el tipus i la naturalesa dels riscos sistèmics a escala de la Unió, incloses les seves fonts. Així mateix, els codis de bones pràctiques s'han de centrar en mesures específiques d'avaluació i reducció de riscos.

(117) Els codis de bones pràctiques han de constituir una eina fonamental per al compliment adequat de les obligacions previstes en aquest Reglament per als proveïdors de models d'IA d'ús general. Els proveïdors s'han de poder basar en codis de bones pràctiques per demostrar que compleixen les obligacions. Mitjançant actes d'execució, la Comissió pot decidir aprovar un codi de bones pràctiques i donar-li una validesa general dins la Unió o bé establir normes comunes per a l'aplicació de les obligacions pertinents si, en el moment en què aquest Reglament esdevingui aplicable, no es pot tenir complet un codi de bones pràctiques o aquest no es considera adequat segons l'Oficina d'IA. Un cop s'ha publicat una norma harmonitzada i que l'Oficina d'IA la consideri adequada per cobrir les obligacions pertinents, el compliment d'una norma harmonitzada europea ha de donar als proveïdors la presumpció de conformitat. A més, els proveïdors de models d'IA d'ús general han de poder demostrar que compleixen fent servir mitjans alternatius adequats si no hi ha codis de bones pràctiques o normes harmonitzades disponibles o trien no confiar-hi.

(118) El Reglament regula els sistemes d'IA i els models d'IA imposant certs requisits i obligacions per als actors de mercat rellevants que els estan introduint en el mercat, posant en servei o utilitzant a la Unió. Així es complementen les obligacions dels proveïdors de serveis d'intermediació que incorporin aquests sistemes o models als seus serveis regulats pel Reglament (UE) 2022/2065. En la mesura que estiguin integrats en plataformes en línia molt grans designades o en motors de cerca en línia molt grans, aquests sistemes o models estan subjectes al marc de gestió de riscos previst en el Reglament (UE) 2022/2065. Per tant, s'ha de presumir que s'han complert les obligacions corresponents del present Reglament llevat que sorgeixin riscos sistèmics significatius no coberts pel Reglament (UE) 2022/2065 i es detectin en aquests models. En aquest marc, els proveïdors de plataformes en línia de molt gran envergadura i de motors de recerca en línia molt grans estan obligats a avaluar els possibles riscos sistèmics derivats del disseny, el funcionament i l'ús dels seus serveis, inclosa la manera com el disseny dels sistemes algorítmics utilitzats en el servei hi pot contribuir, i també els riscos sistèmics derivats de possibles usos indeguts. Aquests proveïdors també estan obligats a adoptar les mesures de mitigació adequades en el compliment dels drets fonamentals.

(119) Atès el ràpid ritme d'innovació i l'evolució tecnològica dels serveis digitals en l'àmbit dels diferents instruments de dret de la Unió, tenint en compte, en particular, l'ús i la percepció dels seus destinataris, els sistemes d'IA subjectes al present Reglament poden prestar-se com a serveis intermediaris, o parts d'aquests, en el sentit del Reglament (UE) 2022/2065, que s'ha d'interpretar de manera tecnològicament neutra. Per exemple, els sistemes d'IA es poden fer servir per proporcionar motors de cerca en línia, en particular, en la mesura que un sistema d'IA com un xatbot en línia, en principi, fa cerques de tots els llocs web; a

continuació, incorpora els resultats en el seu coneixement existent i utilitza el coneixement actualitzat per generar un únic resultat de sortida que combina diferents fonts d'informació.

(120) A més, les obligacions imposades als proveïdors i als responsables del desplegament de determinats sistemes d'IA en el present Reglament destinades a permetre que es detecti i divulgui que els resultats de sortida d'aquests sistemes han estat generats o manipulats de manera artificial resulten especialment pertinents per facilitar l'aplicació efectiva del Reglament (UE) 2022/2065. Això s'aplica en particular a les obligacions dels proveïdors de plataformes en línia de gran envergadura o de motors de recerca en línia de molt gran envergadura de detectar i mitigar els riscos sistèmics que poden sorgir de la divulgació de continguts que hagin estat generats o manipulats de manera artificial, en particular el risc dels efectes negatius reals o previsibles sobre els processos democràtics, el discurs cívic i els processos electorals, també a través de la desinformació.

(121) La normalització ha d'exercir un paper fonamental per proporcionar solucions tècniques als proveïdors per garantir el compliment del present Reglament, en consonància amb l'estat actual de la tècnica, per promoure la innovació, i la competitivitat i el creixement en el mercat únic. El compliment de les normes harmonitzades definides a l'article 2, punt 1, lletra c), del Reglament (UE) 1025/2012 del Parlament Europeu i del Consell [\(41\)](#), que generalment s'espera que reflecteixin l'estat actual de la tècnica, ha de ser un mitjà perquè els proveïdors demostrin la conformitat amb els requisits previstos en el present Reglament. Per tant, cal fomentar una representació equilibrada dels interessos de totes les parts interessades pertinents —en particular les pimes, les organitzacions de consumidors i les parts interessades dels àmbits social i mediambiental— en l'elaboració de normes, de conformitat amb els articles 5 i 6 del Reglament (UE) 1025/2012. Per facilitar-ne el compliment, la Comissió ha d'emetre les sol·licituds de normalització sense demora indeguda. En preparar la petició de normalització, la Comissió ha de consultar el fòrum consultiu i el Consell d'IA per recaptar els coneixements especialitzats pertinents. No obstant això, si no hi ha referències pertinents a les normes harmonitzades, la Comissió ha de poder establir, mitjançant actes d'execució i havent consultat el fòrum consultiu, especificacions comunes per a determinats requisits previstos en el present Reglament. Les especificacions comunes han de ser una solució alternativa excepcional per facilitar l'obligació del proveïdor de complir els requisits d'aquest Reglament quan cap de les organitzacions europees de normalització hagi acceptat la petició de normalització, quan les normes harmonitzades pertinents responguin de manera insuficient a les preocupacions en matèria de drets fonamentals, quan les normes harmonitzades no compleixin la petició o quan es produeixin retards en l'adopció d'una norma harmonitzada adequada. Quan els retards en l'adopció d'una norma harmonitzada es deguin a la complexitat tècnica d'aquesta norma, la Comissió ho ha de tenir en compte abans de considerar la possibilitat d'establir especificacions comunes. Es recomana a la Comissió que, a l'hora d'elaborar especificacions comunes, cooperi amb els socis i els organismes internacionals de normalització.

(122) Convé que, sens perjudici de l'ús de normes harmonitzades i especificacions comunes, es presumeixi que els proveïdors d'un sistema d'IA d'alt risc que hagi estat entrenat i provat amb dades que reflecteixen l'entorn geogràfic, conductual, contextual o funcional específic en què estigui previst que s'utilitzi el sistema d'IA compleixen la mesura pertinent prevista en el requisit en matèria de governança de dades establert en el present Reglament. Sens perjudici dels requisits relacionats amb la solidesa i la precisió establerts en el present Reglament, de conformitat amb l'article 54, apartat 3, del Reglament (UE) 2019/881, s'ha de presumir que els sistemes d'IA d'alt risc que comptin amb una certificació o una declaració de conformitat en virtut d'un esquema de certificació de la ciberseguretat d'acord amb aquest Reglament i les referències del qual s'hagin publicat en el Diari Oficial de la Unió Europea compleixen el requisit de ciberseguretat del present Reglament en la mesura que el certificat de ciberseguretat o la declaració de conformitat, o parts d'aquests, contemplin aquest requisit. Això s'entén sens perjudici del caràcter voluntari d'aquest esquema de ciberseguretat.

(123) Per garantir-ne un alt nivell de fiabilitat, els sistemes d'IA d'alt risc han d'estar subjectes a una avaluació de la conformitat abans que s'introdueixin en el mercat o es posin en servei.

(124) Per reduir al mínim la càrrega que han de suportar els operadors i evitar possibles duplicitats, convé, en el cas dels sistemes d'IA d'alt risc associats a productes regulats per la legislació d'harmonització de la Unió vigent basada en el nou marc legislatiu, que la conformitat d'aquests sistemes d'IA amb els requisits establerts en el present Reglament s'avalui en el marc de l'avaluació de la conformitat ja prevista en la legislació esmentada. Per tant, l'aplicabilitat dels requisits del Reglament no ha d'afectar la lògica, la metodologia o l'estructura general específiques de l'avaluació de la conformitat prevista en els actes legislatius d'harmonització pertinents de la Unió.

(125) Donada la complexitat dels sistemes d'IA d'alt risc i els riscos que s'hi associen, és important desenvolupar un procediment adequat d'avaluació de la conformitat per a sistemes d'IA d'alt risc que impliquin organismes notificats, l'avaluació de la conformitat de tercers. No obstant això, tenint en compte l'experiència actual dels professionals que fan la certificació prèvia a la comercialització en el camp de la seguretat dels productes i de la diferent naturalesa dels riscos implicats, escau limitar, almenys en la fase inicial d'aplicació del present Reglament, l'abast de les avaluacions externes de la conformitat amb els sistemes d'IA d'alt risc que no estan associats a productes. En conseqüència, el proveïdor és qui, per norma general, ha de dur a terme l'avaluació de la conformitat d'aquests sistemes assumint-ne ell mateix la responsabilitat, amb l'única excepció dels sistemes d'IA que estan destinats l'ús en la biometria.

(126) Per poder avaluar la conformitat de tercers quan se'ls exigeixi, en virtut del present Reglament, les autoritats nacionals competents han de notificar els organismes notificats, sempre que compleixin una sèrie de requisits, en particular pel que fa a independència, competències i absència de conflictes d'interessos, a més dels requisits de ciberseguretat

adequats. La notificació d'aquests òrgans l'han d'enviar les autoritats nacionals competents a la Comissió i als altres estats membres mitjançant l'eina de notificació electrònica desenvolupada i gestionada per la Comissió de conformitat amb l'article R23 de l'annex i de la Decisió 768/2008/CE.

(127) En consonància amb els compromisos contrets per la Unió en virtut de l'Acord sobre Obstacles Tècnics al Comerç, de l'Organització Mundial del Comerç, és adequat facilitar el reconeixement mutu dels resultats de les avaluacions de la conformitat fetes per organismes d'avaluació de la conformitat competents, amb independència del territori on estiguin establerts, sempre que aquests organismes d'avaluació de la conformitat establerts d'acord amb el Dret d'un tercer país compleixin els requisits aplicables del Reglament i la Unió hagi formalitzat un acord en aquest sentit. En aquest context, la Comissió ha d'explorar activament els possibles instruments internacionals amb aquest propòsit i, en particular, perseguir la conclusió d'acords de reconeixement mutu amb tercers països.

(128) D'acord amb la noció comunament establerta de modificació substancial per als productes regulats per la legislació d'harmonització de la Unió, és apropiat que quan es produeixi un canvi que pugui afectar el compliment d'un sistema d'IA d'alt risc amb el Reglament (per exemple, el canvi de sistema operatiu o l'arquitectura de programari), o quan el propòsit previst del sistema canviï, el sistema d'IA s'ha de considerar un nou sistema d'IA que s'ha de sotmetre a una nova avaluació de conformitat. No obstant això, els canvis que es produeixen en l'algorisme i el funcionament dels sistemes d'IA que continuen "aprenent" després de la introducció en el mercat o la posada en servei —és a dir, l'adaptació automàtica de com es duen a terme les funcions— no han de constituir una modificació substancial, sempre que els canvis hagin estat predeterminats pel proveïdor i avaluats en el moment de l'avaluació de la conformitat.

(129) Els sistemes d'IA d'alt risc han de portar el marcatge CE per acreditar que són conformes amb el Reglament i així poder circular lliurement pel mercat interior. Per a sistemes d'IA d'alt risc integrats en un producte, s'ha de fixar un marcatge CE físic, el qual es pot complementar amb un marcatge CE digital. Per als sistemes d'IA d'alt risc que només s'han proporcionat digitalment, s'ha de fer servir un marcatge CE digital. Els estats membres no han de crear obstacles injustificats per a la introducció en el mercat o la posada en servei de sistemes d'IA d'alt risc que compleixin els requisits establerts en el Reglament i portin el marcatge CE.

(130) En determinades condicions, la ràpida disponibilitat de tecnologies innovadores pot ser crucial per a la salut i la seguretat de les persones, la protecció del medi ambient i el canvi climàtic i per al conjunt de la societat. Per tant, per motius excepcionals de seguretat pública o amb vista a protegir la vida i la salut de persones físiques, el medi ambient i els actius fonamentals de la indústria i de les infraestructures, escau que les autoritats de vigilància del mercat puguin autoritzar la introducció en el mercat o la posada en servei de

sistemes d'IA que no hagin estat sotmesos a una avaluació de la conformitat. En situacions degudament justificades, segons el que preveu el Reglament, les autoritats garants del compliment de la llei o les autoritats de protecció civil poden posar en servei un sistema d'IA d'alt risc específic sense l'autorització de l'autoritat de vigilància del mercat, sempre que l'autorització se sol·liciti durant o després de l'ús sense demora indeguda.

(131) Per facilitar la tasca de la Comissió i dels estats membres en l'àmbit de la IA i, també, per augmentar la transparència envers el públic, s'ha d'exigir dels proveïdors de sistemes d'IA d'alt risc distints dels relacionats amb els productes que s'inscriuen en l'àmbit de la legislació existent de la Unió pertinent –i també dels proveïdors que consideren que un sistema d'IA inclòs entre els casos d'ús d'alt risc en un annex del Reglament no és d'alt risc en virtut d'una revocació– que es registren i registren també informació sobre el seu sistema d'IA en una base de dades de la UE, que la Comissió crearà i gestionarà. Abans de fer servir aquest sistema d'IA enumerat en els casos d'ús d'alt risc en un annex del Reglament, els responsables del desplegament de sistemes d'IA d'alt risc que siguin autoritats, òrgans o organismes públics s'hi han de registrar i han de triar el sistema que vulguin emprar. Els altres responsables del desplegament han de tenir dret a fer-ho de manera voluntària. Aquesta secció de la base de dades de la UE ha de ser d'accés públic i gratuït, amb informació fàcilment navegable i comprensible i llegible per màquina. La base de dades de la UE ha de ser fàcil d'usar; per exemple, oferint funcionalitats de recerca també mitjançant paraules clau, que permetin al públic en general trobar la informació que s'ha de presentar per al registre dels sistemes d'IA d'alt risc i relativa als casos d'ús de sistemes d'IA d'alt risc contemplats en un annex del Reglament, a què corresponen els sistemes d'IA d'alt risc. Qualsevol modificació substancial dels sistemes d'IA d'alt risc també s'ha de registrar a la base de dades de la UE. Pel que fa als sistemes d'IA d'alt risc en l'àmbit de la garantia del compliment de la llei i de la gestió de la migració, l'asil i el control fronterer, les obligacions de registre s'han de complir en una secció segura no pública de la base de dades de la UE. L'accés a la secció no pública segura s'ha de limitar estrictament a la Comissió o a les autoritats de vigilància del mercat en relació amb la seva secció nacional de la base de dades. Els sistemes d'IA d'alt risc en l'àrea de les infraestructures crítiques només s'han de registrar en l'àmbit nacional. La Comissió ha de ser la responsable de la base de dades de la UE, de conformitat amb el Reglament (UE) 2018/1725. Amb vista a garantir la funcionalitat plena de la base de dades de la UE un cop estigui en servei, el procediment per crear-la ha de comprendre el desenvolupament d'especificacions funcionals per part de la Comissió i, a més, la redacció d'un informe d'auditoria independent. En exercir les funcions com a responsable del tractament de la base de dades de la UE, la Comissió ha de tenir en compte els riscos de ciberseguretat. Per maximitzar la disponibilitat i l'ús de la base de dades de la UE per part del públic, la base de dades de la UE i la informació facilitada a través seu han de complir els requisits establerts a la Directiva (UE) 2019/882.

(132) Certs sistemes d'IA destinats a interactuar amb persones físiques o a generar contingut poden comportar riscos específics de suplantació o engany, independentment de si es consideren d'alt risc o no s'hi consideren. Per tant, hi ha circumstàncies determinades en què l'ús d'aquests sistemes ha d'estar subjecte a obligacions específiques de transparència, sense perjudici dels requisits i les obligacions dels sistemes d'IA d'alt risc i subjectes, també, a excepcions específiques per tenir en compte la necessitat especial de la garantia del

compliment de la llei. En particular, cal comunicar a les persones físiques que interactuen amb un sistema d'IA, excepte quan es faci evident des del punt de vista d'una persona física normalment informada i raonablement atenta i perspicaç, tenint en compte les circumstàncies i el context d'ús. En aplicar aquesta obligació, cal tenir en compte les característiques de les persones físiques pertanyents a col·lectius vulnerables per la seva edat o discapacitat, en la mesura que el sistema d'IA estigui destinat també a interactuar-hi. Cal, a més, notificar les persones físiques quan estiguin exposades a sistemes d'IA que, tractant-los les dades biomètriques, en puguin determinar o inferir les emocions o intencions o incloure-les en categories específiques. Aquestes categories específiques es poden relacionar amb aspectes com ara sexe, edat, color dels cabells, color dels ulls, tatuatges, etc., trets personals, origen ètnic, preferències personals i interessos. Aquesta informació i notificacions s'han de proporcionar en formats accessibles per a les persones amb discapacitat.

(133) Hi ha sistemes d'IA que poden generar grans quantitats de continguts sintètics que les persones cada vegada tenen més dificultats per distingir del contingut autèntic generat per éssers humans. L'àmplia disponibilitat i les capacitats en augment d'aquests sistemes tenen incideixen de manera significativa en la integritat de l'ecosistema de la informació i en la confiança que s'hi diposita, fent sortir nous riscos de desinformació i manipulació a escala, frau, suplantació d'identitat i engany als consumidors. En vista d'aquests efectes, el ràpid desenvolupament tecnològic i la necessitat de nous mètodes i tècniques per assegurar la traçabilitat de l'origen de la informació, escau exigir als proveïdors d'aquests sistemes que integrin solucions tècniques que permetin marcar i detectar, en un format llegible per màquina, que la sortida ha estat generada o manipulada per un sistema d'IA i no per un humà. Aquestes tècniques i mètodes han de ser prou fiables, interoperables, eficaços i sòlids, en la mesura que això sigui tècnicament viable, tenint en compte les tècniques disponibles o una combinació d'aquestes tècniques, com ara marques d'aigua, identificacions de metadades, mètodes criptogràfics per demostrar la procedència i l'autenticitat del contingut, mètodes de registre, empremtes dactilars o altres tècniques, segons el cas. En aplicar aquesta obligació, els proveïdors han de tenir en compte també les especificitats i les limitacions dels diferents tipus de continguts i els desenvolupaments tecnològics i de mercat rellevants en l'àmbit, tal com es reflecteix en l'estat de la tècnica generalment reconegut. Aquestes tècniques i mètodes es poden aplicar en l'àmbit del sistema d'IA o en l'àmbit del model d'IA, inclosos els models d'IA d'ús general que generen contingut, i així es facilita el compliment d'aquesta obligació per part del proveïdor posterior del sistema d'IA. Per garantir la proporcionalitat, convé preveure que l'obligació de marcatge no s'apliqui als sistemes d'IA que exerceixin una funció de suport a l'edició normalitzada o no alterin substancialment les dades d'entrada facilitades pel responsable del desplegament o la seva semàntica.

(134) A més de les solucions tècniques emprades pels proveïdors del sistema d'IA, els responsables del desplegament que utilitzin un sistema d'IA per generar o manipular un contingut d'imatge, àudio o vídeo generat o manipulat per una IA que s'assembli molt a persones, objectes, llocs, entitats o successos reals i que pugui induir una persona a pensar, erròniament, que són autèntics o verídics (ultrasuplantacions) també han de fer públic, de manera clara i distingible, que el contingut s'ha creat o manipulat de manera artificial,

etiquetant els resultats de sortida generats per la IA en conseqüència i indicant-ne l'origen artificial. El compliment de l'obligació de transparència no s'ha d'interpretar com un indicador que la utilització del sistema d'IA o dels seus resultats de sortida és un obstacle per al dret a la llibertat d'expressió i el dret a la llibertat de les arts i les ciències, garantits per la Carta; en particular, quan el contingut estigui integrat en una obra o un programa manifestament creatius, satírics, artístics, de ficció o anàlegs, amb subjecció a garanties adequades per als drets i les llibertats de tercers. En aquests casos, l'obligació de transparència dels ultrafalsos que el Reglament estableix es limita a la divulgació de l'existència d'aquest contingut generat o manipulat de manera adequada que no obstaculitzi la visualització o el gaudi de l'obra, inclosa l'explotació i ús normals, tot mantenint la utilitat i la qualitat del treball. A més, també escau preveure una obligació de divulgació similar en relació amb text generat o manipulat per la IA en la mesura que es publiqui amb la finalitat d'informar el públic sobre matèries d'interès general, tret que el contingut generat per IA hagi passat per un procés de revisió o control editorial humà i una persona física o jurídica assumeixi la responsabilitat editorial pel que fa a la publicació del contingut.

(135) Sense perjudici del caràcter obligatori i de la plena aplicabilitat de les obligacions de transparència, la Comissió també pot encoratjar i facilitar l'elaboració de codis de bones pràctiques a escala de la Unió per facilitar l'aplicació efectiva de les obligacions en matèria de detecció i etiquetatge de continguts generats artificialment o manipulats, també per donar suport a mesures pràctiques per fer accessibles els mecanismes de detecció i facilitar la cooperació amb altres actors al llarg de la cadena de valor, difondre contingut o comprovar la seva autenticitat i procedència per permetre al públic distingir eficaçment el contingut generat per IA.

(136) Les obligacions imposades als proveïdors i responsables del desplegament de determinats sistemes d'IA en el present Reglament per permetre la detecció i divulgació que els resultats de sortida d'aquests sistemes es generen o manipulen artificialment són particularment rellevants per facilitar l'aplicació efectiva del Reglament (UE) 2022/2065. Això s'aplica especialment en relació amb les obligacions dels proveïdors de plataformes en línia de gran envergadura o de motors de cerca en línia de gran envergadura per identificar i mitigar els riscos sistèmics que puguin derivar-se de la difusió de continguts que s'hagin generat o manipulat de manera artificial; en particular, el risc dels efectes negatius reals o previsibles sobre els processos democràtics, el discurs cívic i els processos electorals, fins i tot a través de la desinformació. El requisit d'etiquetar el contingut generat pels sistemes d'IA en virtut del present Reglament és sens perjudici de l'obligació de l'article 16, apartat 6, del Reglament (UE) 2022/2065 per als proveïdors de serveis d'allotjament de processar els avisos sobre el contingut il·legal rebut de conformitat amb l'article 16, apartat 1, del Reglament esmentat i no ha d'influir en l'avaluació i la decisió sobre la il·legalitat del contingut específic. Aquesta avaluació s'ha de fer únicament amb referència a les normes que regeixen la legalitat del contingut.

(137) El compliment de les obligacions de transparència per als sistemes d'IA contemplats en el Reglament no s'ha d'interpretar com un indicatiu que l'ús del sistema d'IA o la seva

producció és lícit en virtut del Reglament o d'un altre dret de la Unió i dels estats membres i ha de ser sense perjudici d'altres obligacions de transparència per als responsables del desplegament de sistemes d'IA establerts en la legislació de la Unió o nacional.

(138) La intel·ligència artificial és una família de tecnologies que es desenvolupa ràpidament i requereix supervisió reguladora i un espai segur i controlat per a l'experimentació, alhora que garanteix la innovació responsable i la integració de les salvaguardes i mesures de mitigació de riscos adequades. Per garantir un marc legal que promogui la innovació, sigui a prova de futur i resistent a alteracions, els estats membres han d'assegurar que les seves autoritats nacionals competents estableixin almenys un espai controlat de proves per a la IA en l'àmbit nacional per facilitar el desenvolupament i proves de sistemes d'IA innovadors sota estricta supervisió reguladora abans que aquests sistemes s'introdueixin en el mercat o es posin en servei d'una altra manera. Els estats membres també podrien complir aquesta obligació participant en els espais controlats de proves ja existents o establint un espai de proves conjuntament amb les autoritats competents d'un o més estats membres, en la mesura que aquesta participació proporcioni un nivell de cobertura nacional equivalent per als estats membres participants. Els espais controlats de proves per a la IA podrien establir-se de forma física, digital o híbrida i poden allotjar productes tant físics com digitals. Les autoritats que els creen també han de garantir que els espais controlats de proves per a la IA disposin de recursos adequats per al seu funcionament, inclosos els recursos financers i humans.

(139) Els espais controlats de proves per a la IA han de tenir els objectius d'impulsar la innovació en l'àmbit de la IA establint un entorn d'experimentació i prova controlat en la fase de desenvolupament i prèvia a la comercialització, amb vista a garantir que els sistemes d'IA innovadors compleixin el que disposa el present Reglament i altres disposicions pertinents del Dret de la Unió i nacional. A més, els espais controlats de proves per a la IA han de tenir per objecte millorar la seguretat jurídica de què gaudeixen els innovadors i afavorir la vigilància de les autoritats competents i el coneixement que aquestes tenen de les oportunitats, els riscos emergents i les conseqüències de l'ús de la IA; de facilitar l'aprenentatge normatiu de les autoritats i empreses, també amb vista a futures adaptacions del marc jurídic; donar suport a la cooperació i l'intercanvi de millors pràctiques amb les autoritats que intervenen en l'espai controlat de proves; i, també, accelerar l'accés als mercats, també eliminant els obstacles per a les petites i mitjanes empreses, incloses les empreses emergents. Els espais controlats de proves per a la IA han d'estar àmpliament disponibles arreu de la Unió i cal prestar especial atenció a què siguin accessibles per a les pimes, incloses les empreses emergents. La participació en l'espai controlat de proves per a la IA s'ha de centrar en qüestions que generin inseguretat jurídica i que, per tant, dificultin que els proveïdors i els proveïdors potencials innovin i experimentin amb la IA a la Unió i contribuir a un aprenentatge normatiu basat en dades contrastades. Com a resultat, la supervisió dels sistemes d'IA en l'espai controlat de proves per a la IA n'ha de comprendre desenvolupament, entrenament, prova i validació abans que s'introdueixin en el mercat o es posin en servei, així com el concepte de «modificació substancial» i la seva materialització, que pot fer necessari un nou procediment d'avaluació de la conformitat. Qualsevol risc significatiu detectat durant el procés de desenvolupament i prova d'aquests sistemes d'IA ha de donar lloc a l'adopció de mesures de reducció

adequades i, si no n'hi ha, a la suspensió del procés de desenvolupament i prova. Si escau, les autoritats nacionals competents que estableixin espais controlats de proves per a la IA han de cooperar amb altres autoritats competents, incloses les que supervisen la protecció dels drets fonamentals i poden comprendre altres agents de l'ecosistema de la IA, com ara organitzacions de normalització nacionals o europees, organismes notificats, instal·lacions d'assaig i experimentació, laboratoris de recerca i experimentació, centres europeus d'innovació digital i organitzacions de parts interessades i de la societat civil corresponents. Per garantir una aplicació uniforme a tota la Unió i aconseguir economies d'escala, resulta oportú establir normes comunes per a la creació d'espais controlats de proves per a la IA, així com un marc per a la cooperació entre les autoritats pertinents implicades en la supervisió d'aquests espais. Els espais controlats de proves per a la IA establerts en virtut d'aquest Reglament s'han d'entendre sens perjudici d'altres actes legislatius que permetin l'establiment d'altres espais controlats de proves encaminats a garantir el compliment de legislació diferent d'aquest Reglament. Quan escaigui, les autoritats competents pertinents encarregades d'aquests altres espais controlats de proves han de ponderar els avantatges d'utilitzar-los també per garantir el compliment del present Reglament per part dels sistemes d'IA. Previ acord entre les autoritats nacionals competents i els participants en l'espai controlat de proves per a la IA, les proves en condicions reals també podran gestionar-se i supervisar-se en el marc de l'espai controlat de proves per a la IA.

(140) El present Reglament ha de proporcionar la base jurídica perquè els proveïdors i els proveïdors potencials en l'espai controlat de proves per a la IA utilitzin dades personals recaptades per a altres finalitats per desenvolupar determinats sistemes d'IA en favor de l'interès públic en l'espai controlat de proves per a la IA, únicament en determinades condicions, de conformitat amb l'article 6, apartat 4, i l'article 9, apartat 2, lletra g), del Reglament (UE) 2016/679 i els articles 5, 6 i 10 del Reglament (UE) 2018/1725, i sense perjudici del que disposen l'article 4, apartat 2, i l'article 10 de la Directiva (UE) 2016/680. La resta d'obligacions dels responsables del tractament i drets dels interessats en virtut dels reglaments (UE) 2016/679 i (UE) 2018/1725 i la Directiva (UE) 2016/680 romanen aplicables. En particular, el present Reglament no ha d'oferir una base jurídica en el sentit de l'article 22, apartat 2, lletra b), del Reglament (UE) 2016/679 i de l'article 24, apartat 2, lletra b), del Reglament (UE) 2018/1725. Els proveïdors i els proveïdors potencials en l'espai controlat de proves per a la IA han de proporcionar les garanties adequades i cooperar amb les autoritats competents, també seguint-ne les indicacions i actuant amb rapidesa i de bona fe per mitigar adequadament qualsevol risc considerable per a la seguretat, la salut i els drets fonamentals que es detecti i pugui sorgir durant el desenvolupament, proves i l'experimentació en aquest espai controlat de proves.

(141) A fi d'accelerar el procés de desenvolupament i introducció en el mercat dels sistemes d'IA d'alt risc enumerats en un annex del present Reglament, és important que els proveïdors o proveïdors potencials d'aquests sistemes també puguin beneficiar-se d'un règim específic per provar aquests sistemes en condicions reals, sense participar en un espai controlat de proves per a la IA. No obstant això, en aquests casos, tenint en compte les possibles conseqüències d'aquestes proves per a les persones físiques, s'ha de garantir que el Reglament estableixi garanties i condicions adequades i suficients per als proveïdors o proveïdors potencials. Aquestes garanties haurien d'incloure, entre altres coses, la

sol·licitud del consentiment informat de les persones físiques per participar en proves en condicions reals, excepte pel que fa a la garantia del compliment de la llei quan intentar obtenir el consentiment informat impediria que es provés el sistema d'IA. El consentiment dels subjectes per participar en aquestes proves en virtut del present Reglament és diferent del consentiment dels interessats per al tractament de les seves dades personals d'acord amb el dret pertinent en matèria de protecció de dades i s'entén sens perjudici d'aquest. També és important reduir al mínim els riscos i permetre la supervisió per part de les autoritats competents i, per tant, exigir als proveïdors potencials que presentin a l'autoritat de vigilància del mercat competent un pla de la prova en condicions reals, registrin la prova en les seccions específiques de la base de dades de la UE, sense perjudici d'algunes excepcions limitades, estableixin limitacions sobre el període durant el qual es pot dur a terme la prova i exigeixin garanties addicionals per a les persones pertanyents a determinats col·lectius vulnerables, així com un acord per escrit que defineixi les funcions i responsabilitats dels proveïdors potencials i dels responsables del desplegament i una supervisió eficaç per part de personal competent que intervingui en la prova en condicions reals. A més, és convenient preveure garanties addicionals per garantir que les prediccions, les recomanacions o decisions del sistema d'IA es poden revertir i ignorar eficaçment i que les dades personals estan protegides i s'eliminen quan els subjectes han retirat el consentiment per participar en les proves sense perjudici dels seus drets com a subjectes de dades en virtut de la legislació de protecció de dades de la Unió. Pel que fa a la transferència de dades, també és apropiat preveure que les dades recopilades i tractades amb la finalitat de provar en condicions reals només s'han de transferir a tercers països quan s'apliquin les salvaguardes apropiades i aplicables en virtut del dret de la Unió; en particular, de conformitat amb les bases per a la transferència de dades personals segons la legislació de la Unió Europea en matèria de protecció de dades, mentre que per a les dades no personals es posen mesures de seguretat apropiades d'acord amb el dret de la Unió, Reglament (UE) 2022/868 [\(42\)](#) i (UE) 2023/2854 [\(43\)](#) del Parlament Europeu i del Consell.

(142) Per garantir que la IA condueixi a resultats beneficiosos socialment i ambientalment, es fomenta que els estats membres donin suport i promoguin la recerca i el desenvolupament de solucions d'intel·ligència artificial en suport de resultats beneficiosos socialment i ambientalment, com ara solucions basades en la IA per augmentar l'accessibilitat de les persones amb discapacitat, abordar les desigualtats socioeconòmiques o complir els objectius ambientals, destinant recursos suficients, inclosos els fons públics i de la Unió, i, si escau, sempre que es compleixin els criteris d'elegibilitat i selecció, tenint en compte en particular els projectes que persegueixen aquests objectius. Aquests projectes s'han de basar en el principi de cooperació interdisciplinària entre els desenvolupadors d'IA, experts en la desigualtat i la no discriminació, l'accessibilitat, els drets dels consumidors, el medi ambient i els drets digitals; també, persones del món acadèmic.

(143) Per promoure i protegir la innovació, és important tenir en particular consideració els interessos de les pimes, incloses les empreses emergents, que siguin proveïdors o responsables del desplegament de sistemes d'IA. Amb aquesta finalitat, els estats membres han de desenvolupar iniciatives en matèria de conscienciació i comunicació d'informació, entre altres aspectes, dirigides a aquests operadors. Els estats membres han de

proporcionar a les pimes, incloses les empreses emergents, que tinguin un domicili social o una sucursal a la Unió, un accés prioritari als espais controlats de proves per a la IA, sempre que compleixin les condicions d'admissibilitat i els criteris de selecció i sense impedir que altres proveïdors i proveïdors potencials accedeixin als espais controlats de proves, sempre les condicions i els criteris siguin els mateixos. Els estats membres han d'utilitzar els canals existents i establir, quan escaigui, nous canals de comunicació específics amb les pimes, incloses les empreses emergents, els responsables del desplegament, altres innovadors i, quan escaigui, les autoritats locals, per donar suport a les pimes durant tota la seva trajectòria de desenvolupament oferint orientacions i responant a les preguntes sobre l'aplicació del present Reglament. Si escau, aquests canals han de treballar junts per crear sinergies i garantir l'homogeneïtat de les seves orientacions per a les pimes, incloses les empreses emergents, i els responsables del desplegament. A més, els estats membres han de fomentar la participació de les pimes i altres parts interessades pertinents en els processos de desenvolupament de la normalització. A més, els interessos i necessitats específiques dels proveïdors que són pimes, incloses les empreses emergents, s'han de tenir en compte quan els organismes notificats fixen les taxes d'avaluació de la conformitat. La Comissió ha d'avaluar periòdicament els costos de la certificació i el compliment per a les pimes, incloses les empreses emergents, a través de consultes transparents, i ha de treballar amb els estats membres per reduir aquests costos. Per exemple, els costos de traducció relacionats amb la documentació obligatòria i la comunicació amb les autoritats poden constituir un cost significatiu per als proveïdors i altres operadors, en particular els de menor envergadura. En la mesura del possible, els estats membres han de vetllar perquè una de les llengües en què acceptin que els proveïdors presentin la documentació pertinent i que es pugui fer servir per a la comunicació amb els operadors sigui àmpliament coneguda pel nombre més gran possible de responsables del desplegament transfronterers. Per abordar les necessitats específiques de les pimes, incloses les empreses emergents, la Comissió ha de proporcionar models normalitzats per als àmbits regulats pel present Reglament, prèvia sol·licitud del Consell d'IA. A més, la Comissió ha de complementar els esforços dels estats membres proporcionant una plataforma única d'informació amb informació fàcil d'utilitzar sobre el present Reglament per a tots els proveïdors i responsables del desplegament, organitzant campanyes de comunicació adequades per sensibilitzar sobre les obligacions derivades del present Reglament i avaluant i fomentant la convergència de les millors pràctiques en els procediments de contractació pública en relació amb sistemes d'IA. Les mitjanes empreses que fa poc es consideraven petites empreses en el sentit de l'annex de la Recomanació 2003/361/CE de la Comissió [\(44\)](#) han de tenir accés a aquestes mesures de suport, ja que aquestes noves mitjanes empreses de vegades poden mancar dels recursos jurídics i la formació necessaris per garantir la comprensió i el compliment adequats del present Reglament.

(144) Per promoure i protegir la innovació, la plataforma d'IA a la carta i tots els programes i projectes de finançament de la Unió pertinents, com el programa Europa Digital o Horitzó Europa, executats per la Comissió i els estats membres a escala nacional o de la Unió, quan escaigui, han de contribuir a l'assoliment dels objectius del Reglament.

(145) A fi de reduir al mínim els riscos per a l'aplicació derivats de la falta de coneixements i experiència en el mercat, i amb l'objectiu de facilitar que els proveïdors, en particular les pimes, incloses les empreses emergents, i els organismes notificats compleixin les obligacions que el present Reglament preveu, la plataforma d'IA a la carta, els centres europeus d'innovació digital i les instal·lacions d'assaig i experimentació establerts per la Comissió i els estats membres a escala nacional o de la Unió han de contribuir a l'aplicació del present Reglament. En concret, la plataforma d'IA a la carta, els centres europeus d'innovació digital i les instal·lacions d'assaig i experimentació poden proporcionar als proveïdors i organismes notificats assistència tècnica i científica dins les missions i esferes de competència respectives.

(146) A més, a la llum de la mida molt petita d'alguns operadors i per tal de garantir la proporcionalitat en relació amb els costos d'innovació, convé permetre que les microempreses compleixin una de les obligacions més costoses, a saber, la d'establir un sistema de gestió de la qualitat, de manera simplificada, cosa que reduiria la càrrega administrativa i els costos per a aquestes empreses sense afectar el nivell de protecció ni la necessitat de complir els requisits aplicables als sistemes d'IA d'alt risc. La Comissió ha d'elaborar directrius per especificar els elements del sistema de gestió de la qualitat que les microempreses han de complir d'aquesta manera simplificada.

(147) Cal que, fins on sigui possible, la Comissió faciliti l'accés a les instal·lacions d'assaig i experimentació a organismes, grups o laboratoris establerts o acreditats d'acord amb la legislació d'harmonització pertinent de la Unió i que facin funcions en el marc de l'avaluació de la conformitat de productes o dispositius regulats per aquesta legislació. Aquest és, en particular, el cas dels panells d'experts, laboratoris d'experts i laboratoris de referència en l'àmbit dels productes sanitaris d'acord amb els reglaments (UE) 2017/745 i (UE) 2017/746.

(148) El Reglament ha d'establir un marc de governança que permeti tant coordinar i donar suport a l'aplicació del Reglament a escala nacional com construir capacitats a escala de la Unió i integrar les parts interessades en l'àmbit de la IA. L'aplicació i el compliment efectius del present Reglament requereixen un marc de governança que permeti coordinar i adquirir coneixements especialitzats centrals a escala de la Unió. L'Oficina d'IA es va establir per decisió de la Comissió (45) i té com a missió desenvolupar coneixements i capacitats de la Unió en el camp de la IA i contribuir a l'aplicació del dret de la Unió sobre IA. Els estats membres han de facilitar les funcions de l'Oficina d'IA amb vista a donar suport al desenvolupament de coneixements especialitzats i capacitats a escala de la Unió i a enfortir el funcionament del mercat únic digital. A més, s'ha de crear un Consell d'IA compost per representants dels estats membres, un comitè científic per integrar la comunitat científica i un fòrum consultiu per facilitar les aportacions de les parts interessades a l'aplicació del present Reglament, a escala de la Unió i nacional. El desenvolupament de coneixements especialitzats i capacitats de la Unió també ha d'incloure la utilització dels recursos i coneixements especialitzats existents, en particular a través de sinergies amb estructures creades en el context de l'aplicació a escala de la Unió d'altres actes legislatius i de sinergies

amb iniciatives connexes a escala de la Unió, com l'Empresa Conjunta EuroHPC i les instal·lacions d'assaig i experimentació d'IA en el marc del programa Europa Digital.

(149) Per facilitar una aplicació fluïda, efectiva i harmonitzada del present Reglament s'ha d'establir un Consell d'IA. El Consell d'IA ha de reflectir els diversos interessos de l'ecosistema de la IA i estar format per representants dels estats membres. El Consell d'IA s'ha d'encarregar de diverses funcions d'assessorament. Entre altres, ha d'emetre dictàmens, recomanacions i informes d'assessorament o contribuir a orientacions sobre assumptes relacionats amb l'aplicació del present Reglament, també pel que fa a l'execució, les especificacions tècniques o les normes existents en relació amb els requisits que s'hi preveuen, i assessorar la Comissió i els estats membres, així com les autoritats nacionals competents respectives, en qüestions específiques vinculades a la IA. Per donar certa flexibilitat als estats membres en la designació dels seus representants en el Consell d'IA, qualsevol persona pertanyent a una entitat pública que tingui les competències i facultats pertinents per facilitar la coordinació a escala nacional i contribuir al compliment de les funcions del Consell d'IA ha de poder ser designada representant. El Consell d'IA ha d'establir dos subgrups permanents per tal de proporcionar una plataforma de cooperació i intercanvi entre les autoritats de vigilància del mercat i les autoritats notificadores sobre qüestions relacionades, respectivament, amb la vigilància del mercat i els organismes notificats. El subgrup permanent de vigilància del mercat ha d'actuar com a grup de cooperació administrativa (ADCO) per al Reglament en el sentit de l'article 30 del Reglament (UE) 2019/1020. D'acord amb l'article 33 del Reglament, la Comissió ha de donar suport a les activitats del subgrup permanent de vigilància del mercat mitjançant l'execució d'avaluacions o estudis de mercat, en particular amb la finalitat d'identificar aspectes del Reglament que requereixin una coordinació específica i urgent entre les autoritats de vigilància del mercat. El Consell d'IA pot establir altres subgrups permanents o temporals, segons correspongui, amb la finalitat d'examinar qüestions específiques. El Consell d'IA també ha de cooperar, segons sigui necessari, amb els organismes, grups d'experts i xarxes pertinents de la Unió actius en el context del dret de la Unió pertinent, inclosos, en particular, els actius en virtut del dret de la Unió pertinent en matèria de dades i productes i serveis digitals.

(150) Amb vista a garantir la participació de les parts interessades en l'execució i aplicació del present Reglament, s'ha de crear un fòrum consultiu per assessorar el Consell d'IA i la Comissió i proporcionar-los coneixements tècnics. Per garantir una representació variada i equilibrada de les parts interessades que tingui en compte els interessos comercials i no comercials i, dins la categoria dels interessos comercials, pel que fa a les pimes i altres empreses, el fòrum consultiu ha d'incloure, entre d'altres, la indústria, les empreses emergents, les pimes, el món acadèmic, la societat civil, en particular els interlocutors socials, ai l'Agència dels Drets Fonamentals de la Unió Europea, ENISA, el Comitè Europeu de Normalització (CEN), el Comitè Europeu de Normalització Electrotècnica (Cenelec) i l'Institut Europeu de Normes de Telecomunicacions (ETSI).

(151) Per donar suport a l'aplicació i el compliment del present Reglament, en particular les activitats de seguiment de l'Oficina d'IA pel que fa als models d'IA d'ús general, s'ha de

crear un comitè científic format per experts independents. Els experts independents que constitueixin el comitè científic s'han de seleccionar a partir de coneixements científics o tècnics actualitzats en l'àmbit de la IA i han d'exercir les funcions amb imparcialitat i objectivitat i garantir la confidencialitat de la informació i les dades obtingudes en l'exercici de les funcions i activitats. Per permetre el reforç de les capacitats nacionals necessàries per al compliment efectiu del Reglament, els estats membres han de poder demanar el suport dels experts que constitueixin el comitè científic per a les seves activitats de garantia del compliment.

(152) Per donar suport a una aplicació adequada pel que fa als sistemes d'IA i reforçar les capacitats dels estats membres, s'han de crear i posar a disposició dels estats membres estructures de suport als assajos d'IA de la Unió.

(153) Els estats membres exerceixen un paper clau en l'aplicació i execució del present Reglament. En aquest sentit, cada estat membre ha de designar almenys una autoritat notificadora i almenys una autoritat de vigilància del mercat com a autoritats nacionals competents que s'encarreguin de supervisar-ne l'aplicació i execució. Els estats membres poden decidir designar qualsevol mena d'entitat pública perquè exerceixi les funcions de les autoritats nacionals competents en el sentit del present Reglament, de conformitat amb les seves característiques i necessitats organitzatives nacionals específiques. Per incrementar l'eficiència organitzativa als estats membres i establir un punt de contacte únic oficial amb el públic i altres homòlegs a escala dels estats membres i la Unió, cada estat membre ha de designar una autoritat de vigilància del mercat que actuï com a punt de contacte únic.

(154) Les autoritats nacionals competents han d'exercir els poders de manera independent, imparcial i objectiva, a fi de preservar els principis d'objectivitat de les seves activitats i funcions i garantir l'aplicació i execució del Reglament. Els membres d'aquestes autoritats s'han d'abstenir de tot acte incompatible amb el caràcter de les seves funcions i estar subjectes a les normes de confidencialitat establertes en el Reglament.

(155) Tots els proveïdors de sistemes d'IA d'alt risc han de disposar d'un sistema de seguiment postcomercialització, amb vista a garantir que puguin tenir en compte l'experiència amb l'ús d'aquests sistemes de cara a millorar els seus sistemes i procés de disseny i desenvolupament o que puguin adoptar qualsevol mesura correctora en el moment oportú. Quan escaigui, el seguiment de postcomercialització ha d'incloure una anàlisi de la interacció amb altres sistemes d'IA, inclosos altres dispositius i programari. El seguiment postcomercialització no ha de comprendre les dades operatives sensibles dels responsables del desplegament de sistemes d'IA que siguin autoritats garants del compliment de la llei. Aquest sistema també és fonamental per garantir que els possibles riscos resultants dels sistemes d'IA que continuen "aprenent", després que s'hagin introduït en el mercat o posat en servei, es puguin resoldre d'una manera més eficient i oportuna. En aquest context, escau exigir als proveïdors que també disposin d'un sistema per comunicar a les autoritats

pertinents qualsevol incident greu associat a l'ús dels seus sistemes d'IA, entès com un incident o defecte que tingui com a conseqüència una defunció o danys greus per a la salut, una alteració greu i irreversible de la gestió o el funcionament d'infraestructures crítiques, l'incompliment d'obligacions derivades del dret de la Unió destinades a protegir els drets fonamentals o impedir danys greus en la propietat o al medi ambient.

(156) Amb l'objectiu de garantir el compliment adequat i efectiu dels requisits i les obligacions previstos en el present Reglament, que constitueix legislació d'harmonització de la Unió, s'ha d'aplicar íntegrament el sistema relatiu a la vigilància del mercat i la conformitat dels productes establert pel Reglament (UE) 2019/1020. Les autoritats de vigilància del mercat designades d'acord amb aquest Reglament han de disposar de tots els poders d'execució establerts en el present Reglament i en el Reglament (UE) 2019/1020, i han d'exercir els seus poders i exercir les seves funcions de manera independent, imparcial i objectiva. Tot i que la majoria dels sistemes d'IA no estan subjectes a requisits i obligacions específics d'acord amb el Reglament, les autoritats de vigilància del mercat poden adoptar mesures en relació amb tots els sistemes d'IA quan aquests presentin un risc d'acord amb el Reglament. A causa de la naturalesa específica de les institucions, òrgans i organismes de la Unió que entren en l'àmbit d'aplicació del present Reglament, escau designar-los el Supervisor Europeu de Protecció de Dades com a autoritat de vigilància del mercat competents. Això s'ha d'entendre sense perjudici de la designació d'autoritats nacionals competents per part dels estats membres. Les activitats de vigilància del mercat no han d'afectar la capacitat de les entitats supervisades per dur a terme les funcions de manera independent, quan el dret de la Unió exigeixi aquesta independència.

(157) El present Reglament s'entén sense perjudici de les competències, funcions, poders i independència de les autoritats o organismes públics nacionals pertinents que supervisen l'aplicació del dret de la Unió protegint els drets fonamentals, inclosos els òrgans d'igualtat i les autoritats de protecció de dades. Quan els calgui per al mandat, les autoritats o organismes públics nacionals també han de tenir accés a qualsevol documentació creada en virtut del present Reglament. S'ha d'establir un procediment de salvaguarda específic per garantir una execució adequada i oportuna contra els sistemes d'intel·ligència artificial que presentin un risc per a la salut, la seguretat i els drets fonamentals. El procediment relatiu a aquests sistemes d'IA que presenten un risc s'ha d'aplicar als sistemes d'IA d'alt risc que presentin un risc, als sistemes prohibits que hagin estat introduïts en el mercat, posats en servei o utilitzats contravenint les pràctiques prohibides establertes en el present Reglament i als sistemes d'IA que hagin estat comercialitzats infringint els requisits de transparència establerts en el present Reglament i que presentin un risc.

(158) El Dret de la Unió en matèria de serveis financers conté normes i requisits en matèria de governança interna i gestió de riscos que les entitats financeres regulades han de complir durant la prestació d'aquests serveis, i també quan utilitzin sistemes d'IA. Per garantir l'aplicació i l'execució coherents de les obligacions previstes en el present Reglament, i de les normes i els requisits pertinents dels actes legislatius de la Unió relatius als serveis financers, s'han de designar les autoritats competents pel que fa a la supervisió i la garantia del compliment d'aquests actes legislatius; en particular, les autoritats competents

definides en el Reglament (UE) 575/2013 del Parlament Europeu i del Consell (46) i les directives 2008/48/CE (47), 2009/138/CE (48), 2013/36/UE (49), 2014/17/UE (50) i (UE) 2016/97 (51) del Parlament Europeu i del Consell, dins les competències respectives, com les autoritats competents encarregades de supervisar l'aplicació del present Reglament, també pel que fa a les activitats de vigilància del mercat, en relació amb els sistemes d'IA proporcionats o utilitzats per les entitats financeres regulades i supervisades, llevat que els estats membres decideixin designar una altra autoritat perquè exerceixi aquestes funcions de vigilància del mercat. Aquestes autoritats competents han de disposar de tots els poders previstos en el present Reglament i en el Reglament (UE) 2019/1020 per fer complir els requisits i les obligacions del present Reglament, inclosos els poders per dur a terme activitats de vigilància del mercat postcomercialització que poden integrar-se, si cal, en els seus mecanismes i procediments de supervisió existents en virtut del dret pertinent de la Unió en matèria de serveis financers. Convé preveure que, quan actuïn com a autoritats de vigilància del mercat en virtut del present Reglament, les autoritats nacionals responsables de la supervisió de les entitats de crèdit regulades per la Directiva 2013/36/UE que participin en el Mecanisme Únic de Supervisió establert pel Reglament (UE) 1024/2013 del Consell (52), comuniquin sense demora al Banc Central Europeu tota informació obtinguda en el transcurs de les activitats de vigilància del mercat que pugui ser d'interès per a les funcions de supervisió prudencial del Banc Central Europeu especificades en el Reglament. Amb vista a augmentar la coherència entre el present Reglament i les normes aplicables a les entitats de crèdit regulades per la Directiva 2013/36/UE, convé igualment integrar algunes de les obligacions procedimentals dels proveïdors relatives a la gestió de riscos, el seguiment de postcomercialització i la documentació en les obligacions i els procediments vigents d'acord amb la Directiva 2013/36/UE. Per evitar encavalcaments, també s'han de contemplar excepcions limitades en relació amb el sistema de gestió de la qualitat dels proveïdors i l'obligació de seguiment imposada als responsables del desplegament de sistemes d'IA d'alt risc, en la mesura que aquests s'apliquin a les entitats de crèdit regulades per la Directiva 2013/36/UE. El mateix règim s'ha d'aplicar a les empreses d'assegurances i reassegurances i a les societats de cartera d'assegurances regulades per la Directiva 2009/138/CE, als intermediaris d'assegurances regulats per la Directiva (UE) 2016/97 i a altres tipus d'entitats financeres subjectes a requisits sobre governança, sistemes o processos interns establerts d'acord amb el Dret pertinent de la Unió en matèria de serveis financers a fi de garantir la coherència i la igualtat de tracte en el sector financer.

(159) Cada autoritat de vigilància del mercat per als sistemes d'IA d'alt risc en l'àmbit de la biometria enumerats en un annex del present Reglament, en la mesura que aquests sistemes s'utilitzin amb finalitats de garantia del compliment de la llei, de migració, asil i gestió del control fronterer, o de l'administració de justícia i els processos democràtics, ha de disposar de facultats de recerca i correctores efectives, inclosa almenys la facultat d'obtenir accés a totes les dades personals que s'estiguin tractant i a tota la informació necessària per a l'acompliment de les seves funcions. Les autoritats de vigilància del mercat han de poder exercir els seus poders actuant amb total independència. Qualsevol limitació del seu accés a dades operatives sensibles en virtut del present Reglament s'ha d'entendre sense perjudici dels poders que els confereix la Directiva (UE) 2016/680. Cap exclusió en la divulgació de dades a les autoritats nacionals de protecció de dades en virtut del present

Reglament ha d'afectar les competències actuals o futures d'aquestes autoritats fora de l'àmbit d'aplicació del Reglament.

(160) Les autoritats de vigilància del mercat i la Comissió han de poder proposar activitats conjuntes, incloses investigacions conjuntes, que les autoritats de vigilància del mercat, per elles mateixes, o juntament amb la Comissió han de dur a terme, amb l'objectiu de fomentar el compliment, detectar incompliments, sensibilitzar i oferir orientacions en relació amb el present Reglament respecte de les categories específiques de sistemes d'IA d'alt risc que representen un risc greu en dos o més estats membres. Aquestes activitats conjuntes per fomentar el compliment s'han de dur a terme de conformitat amb l'article 9 del Reglament (UE) 2019/1020. L'Oficina d'IA ha de donar suport de coordinació a les investigacions conjuntes.

(161) Cal aclarir les responsabilitats i competències a escala de la Unió i nacional pel que fa als sistemes d'IA que es basen en models d'IA d'ús general. Per evitar l'encavalcament de competències, quan un sistema d'IA es basi en un model d'IA d'ús general i el model i el sistema siguin subministrats pel mateix proveïdor, la supervisió s'ha de dur a terme a escala de la Unió a través de l'Oficina d'IA, que ha de tenir a aquests efectes les facultats d'una autoritat de vigilància del mercat en el sentit del Reglament (UE) 2019/1020. En tots els altres casos, les autoritats nacionals de vigilància del mercat continuen sent responsables de la supervisió dels sistemes d'IA. No obstant això, en el cas dels sistemes d'IA d'ús general que puguin ser utilitzats directament pels responsables del desplegament amb almenys una finalitat classificada com d'alt risc, les autoritats de vigilància del mercat han de cooperar amb l'Oficina d'IA per dur a terme avaluacions de la conformitat i informar-ne el Consell d'IA i altres autoritats de vigilància del mercat. A més, les autoritats de vigilància del mercat han de poder sol·licitar l'assistència de l'Oficina d'IA quan l'autoritat de vigilància del mercat no pugui concloure una investigació sobre un sistema d'IA d'alt risc a causa de la seva incapacitat per accedir a determinada informació relacionada amb el model d'IA d'ús general en el qual es basa el sistema d'IA d'alt risc. En aquests casos, s'ha d'aplicar mutatis mutandis el procediment d'assistència mútua transfronterera previst en el capítol VI del Reglament (UE) 2019/1020.

(162) Per aprofitar al màxim la centralització de coneixements especialitzats i les sinergies que es generen a escala de la Unió, s'han d'atribuir a la Comissió les competències de supervisió i de control del compliment de les obligacions dels proveïdors de models d'IA d'ús general. L'Oficina d'IA ha de poder dur a terme totes les accions necessàries per supervisar l'aplicació efectiva del present Reglament pel que fa als models d'IA d'ús general. Ha de poder investigar possibles infraccions de les normes relatives als proveïdors de models d'IA d'ús general, tant per iniciativa pròpia, arran dels resultats de les seves activitats de seguiment, com a petició de les autoritats de vigilància del mercat, de conformitat amb les condicions establertes en el present Reglament. Per promoure l'eficàcia del seguiment, l'Oficina d'IA ha de preveure la possibilitat que els proveïdors posteriors presentin reclamacions sobre possibles infraccions de les normes relatives als proveïdors de sistemes i models d'IA d'ús general.

(163) Per complementar els sistemes de governança dels models d'IA d'ús general, el comitè científic ha de contribuir a les activitats de seguiment de l'Oficina d'IA i, en determinats casos, pot proporcionar alertes qualificades a l'Oficina d'IA que activin actuacions consecutives, com ara investigacions. Així ha de ser quan el comitè científic tingui motius per sospitar que un model d'IA d'ús general planteja un risc concret i identificable en l'àmbit de la Unió. També ha de ser així quan el comitè científic tingui motius per sospitar que un model d'IA d'ús general compleix els criteris que portarien a classificar-lo com a model d'IA d'ús general amb risc sistèmic. Per facilitar al comitè científic la informació necessària per a l'acompliment d'aquestes funcions, cal un mecanisme que permeti al comitè científic sol·licitar a la Comissió que demani documentació o informació a un proveïdor.

(164) L'Oficina d'IA ha de poder adoptar les mesures necessàries per controlar l'aplicació efectiva i el compliment de les obligacions dels proveïdors de models d'IA d'ús general establertes en el present Reglament. L'Oficina d'IA ha de poder investigar possibles infraccions d'acord amb les competències previstes en aquest Reglament, fins i tot sol·licitant documentació i informació, fent avaluacions i demanant mesures als proveïdors de models d'IA d'ús general. En avaluar, per disposar de coneixements especialitzats independents, l'Oficina d'IA ha de poder recórrer a experts independents perquè avaluïn en nom seu. S'ha de poder exigir el compliment de les obligacions mitjançant, entre altres coses, sol·licituds d'adopció de mesures adequades, entre les quals s'inclouen mesures de reducció del risc en cas que es detectin riscos sistèmics, així com la restricció de la comercialització, la retirada o la recuperació del model. Com a salvaguarda, quan sigui necessari, a més dels drets procedimentals previstos en el present Reglament, els proveïdors de models d'IA d'ús general han de tenir els drets procedimentals previstos a l'article 18 del Reglament (UE) 2019/1020, que s'han d'aplicar mutatis mutandis, sense perjudici dels drets processals més específics previstos en el present Reglament.

(165) El desenvolupament de sistemes d'IA diferents dels sistemes d'IA d'alt risc d'acord amb els requisits del Reglament pot conduir a una major adopció d'IA ètica i fiable a la Unió. Cal instar els proveïdors de sistemes d'IA que no són d'alt risc a crear codis de conducta, entre els quals s'inclouen els corresponents mecanismes de governança, destinats a impulsar l'aplicació voluntària de la totalitat o part dels requisits aplicables als sistemes d'IA d'alt risc, adaptats tenint en compte la finalitat prevista dels sistemes i el menor risc plantejat i tenint en compte les solucions tècniques disponibles i les millors pràctiques del sector, com ara les targetes de model i de dades. Així mateix, s'ha d'animar els proveïdors i, si escau, els responsables del desplegament de tots els sistemes d'IA, ja siguin o no d'alt risc, i dels models d'IA, a aplicar, amb caràcter voluntari, requisits addicionals relatius, per exemple, als elements de les orientacions ètiques de la Unió per a IA fiable, sostenibilitat mediambiental, mesures d'alfabetització en matèria d'IA, inclusivitat i diversitat en el disseny i el desenvolupament dels sistemes d'IA, la qual cosa inclou tenir en compte les persones vulnerables i l'accessibilitat de les persones amb discapacitat, la involucració de les parts interessades, amb la participació, segons escaigui, de les parts interessades pertinents, com les organitzacions empresarials i de la societat civil, el món acadèmic, els

organismes de recerca, els sindicats i les organitzacions de protecció dels consumidors, en el disseny i el desenvolupament dels sistemes d'IA, i la diversitat dels equips de desenvolupament, també pel que fa a la paritat de gènere. Per garantir-ne l'eficàcia, els codis de conducta voluntaris s'han de basar en objectius clars i indicadors clau de rendiment per mesurar-ne l'assoliment. També s'han de desenvolupar de manera inclusiva, segons correspongui, amb la participació de les parts interessades pertinents, com ara organitzacions empresarials i de la societat civil, el món acadèmic, les organitzacions de recerca, els sindicats i l'organització de protecció del consumidor. La Comissió pot desenvolupar iniciatives, fins i tot de caràcter sectorial, per facilitar la reducció de les barreres tècniques que dificulten l'intercanvi transfronterer de dades per al desenvolupament de la IA, incloent-hi la infraestructura d'accés a dades, la interoperabilitat semàntica i tècnica de diferents tipus de dades.

(166) És important que els sistemes d'IA associats a productes que el present Reglament no considera d'alt risc i que, per tant, no estan obligats a complir els requisits establerts per als sistemes d'IA d'alt risc, siguin, no obstant això, segurs una vegada introduïts en el mercat o posats en servei. Per contribuir a aquest objectiu, el Reglament (UE) 2023/988 del Parlament Europeu i del Consell [\(53\)](#) s'ha d'aplicar com a xarxa de seguretat.

(167) Per garantir la cooperació fiable i constructiva de les autoritats competents en l'àmbit de la Unió i nacional, totes les parts implicades en l'aplicació del Reglament han de respectar la confidencialitat de la informació i les dades obtingudes en l'exercici de les seves funcions, de conformitat amb el dret de la Unió o el dret nacional. Han d'exercir les funcions i activitats pròpies de manera que es protegeixin, en particular, els drets de propietat intel·lectual i industrial, la informació empresarial confidencial i els secrets comercials, l'aplicació efectiva del Reglament, els interessos de seguretat pública i nacional, la integritat dels procediments penals i administratius i la integritat de la informació classificada.

(168) El compliment del Reglament ha de ser exigible mitjançant la imposició de sancions i altres mesures de garantia del compliment. Els estats membres han de prendre totes les mesures necessàries per garantir que les disposicions del present Reglament s'apliquin, fins i tot mitjançant l'establiment de sancions efectives, proporcionades i dissuasives per al cas que s'infringeixin, i per respectar el principi de no bis in idem. Per reforçar i harmonitzar les sancions administratives per infracció del Reglament, s'han de fixar els límits superiors per determinar les multes administratives per a determinades infraccions específiques. En determinar la quantia de les multes, els estats membres han de tenir en compte, en cada cas concret, totes les circumstàncies pertinents de la situació de què es tracti, considerant especialment la naturalesa i la gravetat i durada de la infracció i de les seves conseqüències, a més de les dimensions del proveïdor; en particular, si aquest és una pime o una empresa emergent. El Supervisor Europeu de Protecció de dades ha de tenir el poder d'imposar multes a les institucions, els òrgans i els organismes de la Unió que estiguin en l'àmbit d'aplicació del Reglament.

(169) El compliment de les obligacions imposades als proveïdors de models d'IA d'ús general imposats en virtut del Reglament s'ha de poder exigir, entre altres coses, mitjançant multes. Així, també s'han d'establir nivells adequats de multes per infracció d'aquestes obligacions, en què s'inclou l'incompliment de les mesures sol·licitades per la Comissió d'acord amb el Reglament, subjectes a terminis de prescripció adequats d'acord amb el principi de proporcionalitat. Totes les decisions preses per la Comissió en virtut del present Reglament estan subjectes a revisió pel Tribunal de Justícia de la Unió Europea de conformitat amb el TFUE, inclosa la competència jurisdiccional il·limitada del Tribunal de Justícia pel que fa a les sancions de conformitat amb l'article 261 TFUE.

(170) La Unió Europea i el dret nacional ja proporcionen recursos efectius a les persones físiques i jurídiques els drets i llibertats de les quals es veuen afectats negativament per l'ús de sistemes d'IA. Sense perjudici d'aquests recursos, qualsevol persona física o legal que tingui motius per considerar que s'ha produït una infracció del Reglament ha de tenir dret a presentar una reclamació davant l'autoritat de vigilància del mercat pertinent.

(171) Les persones afectades han de tenir dret a obtenir una explicació quan la decisió d'un responsable del desplegament es basa principalment en la sortida de determinats sistemes d'IA d'alt risc que entren en l'àmbit del present Reglament i quan aquesta decisió produeix efectes legals o afecta de manera significativa aquestes persones de manera que considerin que els provoca repercussions negatives en la salut, la seguretat o els drets fonamentals. L'explicació ha de ser clara i significativa i ha de servir de base sobre la qual les persones afectades puguin exercir els drets. El dret a obtenir una explicació no s'ha d'aplicar a la utilització de sistemes d'IA per als quals es deriven excepcions o restriccions d'acord amb el dret nacional o de la Unió, i només s'ha d'aplicar en la mesura que aquest dret no estigui ja previst en el dret de la Unió.

(172) Les persones que informin sobre infraccions del present Reglament han de quedar protegides pel dret de la Unió. La Directiva (UE) 2019/1937 del Parlament Europeu i del Consell (54), per tant, ha d'aplicar-se a la comunicació d'infraccions d'aquest Reglament i a la protecció de les persones que comuniquen.

(173) A fi de garantir que el marc reglamentari es pugui adaptar quan sigui necessari, s'han de delegar a la Comissió els poders per adoptar actes d'acord amb l'article 290 del TFUE de manera que pugui modificar les condicions en què un sistema d'IA no s'ha de considerar un sistema d'alt risc, la llista de sistemes d'IA d'alt risc, les disposicions relatives a la documentació tècnica, el contingut de la declaració UE de conformitat, les disposicions relatives als procediments d'avaluació de la conformitat, les disposicions que estableixen a quins sistemes d'IA d'alt risc s'ha d'aplicar el procediment d'avaluació de la conformitat basat en l'avaluació del sistema de gestió de la qualitat i en l'avaluació de la documentació tècnica, el llistar, els paràmetres de referència i els indicadors, la qual cosa inclou la possibilitat de complementar aquests paràmetres de referència i indicadors, de les normes de classificació dels models d'IA d'ús general amb risc sistèmic, els criteris per classificar un

model com a model d'IA d'ús general amb risc sistèmic, la documentació tècnica per als proveïdors de models d'IA d'ús general i la informació sobre transparència per als proveïdors de models d'IA d'ús general. Revesteix especial importància que la Comissió dugui a terme les consultes oportunes durant la fase preparatòria, en particular amb experts, i que aquestes consultes es facin de conformitat amb els principis establerts en l'Acord interinstitucional de 13 d'abril de 2016 sobre la millora de la legislació [\(55\)](#). En particular, per garantir una participació equitativa en la preparació dels actes delegats, el Parlament Europeu i el Consell reben tota la documentació alhora que els experts dels estats membres, i els seus experts tenen accés sistemàticament a les reunions dels grups d'experts de la Comissió que s'ocupen de la preparació d'actes delegats.

(174) Tenint en compte els ràpids avenços tecnològics i dels coneixements tècnics necessaris per aplicar-lo de manera efectiva, la Comissió ha d'avaluar i revisar el present Reglament no més tard del 2 d'agost de 2029 i, posteriorment, cada quatre anys i informar el Parlament Europeu i el Consell. A més, ateses les implicacions pel que fa a l'àmbit d'aplicació del present Reglament, la Comissió ha d'avaluar la necessitat de modificar la llista de sistemes d'IA d'alt risc i la llista de pràctiques prohibides un cop l'any. Així mateix, no més tard del 2 d'agost de 2028 i posteriorment cada quatre anys, la Comissió ha d'avaluar i comunicar al Parlament Europeu i al Consell la necessitat de modificar la llista d'àmbits d'alt risc que figura a l'annex del present Reglament, els sistemes d'IA inclosos en l'àmbit d'aplicació de les obligacions de transparència, l'eficàcia del sistema de supervisió i governança i els avenços en el desenvolupament de documents de normalització sobre el desenvolupament eficient des del punt de vista energètic de models d'IA d'ús general, inclosa la necessitat de mesures o accions addicionals. Finalment, no més tard del 2 d'agost de 2028 i posteriorment cada tres anys, la Comissió ha d'avaluar la repercussió i l'eficàcia dels codis de conducta voluntaris per fomentar l'aplicació dels requisits establerts per als sistemes d'IA d'alt risc als sistemes d'IA que no siguin sistemes d'IA d'alt risc i, possiblement, altres requisits addicionals per a aquests sistemes d'IA.

(175) Per garantir unes condicions uniformes per a l'execució del Reglament, les competències d'execució s'han d'atribuir a la Comissió. Aquestes competències s'han d'exercir de conformitat amb el Reglament (UE) 182/2011 del Parlament Europeu i del Consell [\(56\)](#).

(176) Atès que l'objectiu del present Reglament —millorar el funcionament del mercat interior i promoure l'adopció d'una IA centrada en l'ésser humà i fiable, garantint alhora un elevat nivell de protecció de la salut, la seguretat i els drets fonamentals consagrats a la Carta, inclosos la democràcia, l'estat de dret i la protecció del medi ambient, enfront dels efectes perjudicials dels sistemes d'IA a la Unió, i també contribuir a la innovació— no es poden assolir de manera suficient per als estats membres, sinó que, per les seves dimensions i efectes, es poden assolir millor a escala de la Unió, aquesta pot adoptar mesures d'acord amb el principi de subsidiarietat establert a l'article 5 del TUE. D'acord amb el principi de proporcionalitat establert en aquest article, el present Reglament no excedeix del necessari per aconseguir aquest objectiu.

(177) Per garantir la seguretat jurídica, assegurar un període d'adaptació adequat per als operadors i evitar perturbacions del mercat, també garantint la continuïtat de l'ús dels sistemes d'IA, és convenient que el present Reglament s'apliqui als sistemes d'IA d'alt risc que s'hagin introduït en el mercat o s'hagin posat en servei abans de la data general d'aplicació del Reglament només si, a partir d'aquesta data, aquests sistemes es veuen sotmesos a canvis significatius en el disseny o la finalitat prevista. Convé aclarir que, referent a això, la noció de canvi significatiu es pot considerar substancialment equivalent a la de modificació substancial, que només s'aplica als sistemes d'IA d'alt risc de conformitat amb el present Reglament. Amb caràcter excepcional i a efectes de la rendició pública de comptes, els operadors de sistemes d'IA que siguin components de sistemes informàtics de gran magnitud establerts pels actes legislatius enumerats en un annex del present Reglament i els operadors de sistemes d'IA d'alt risc destinats a l'ús per les autoritats públiques han d'adoptar, respectivament, les mesures necessàries per complir els requisits del present Reglament abans del final de 2030 i, a tot tardar, el 2 d'agost de 2030.

(178) Es recomana als proveïdors de sistemes d'IA d'alt risc que comencin a complir, de forma voluntària, les obligacions pertinents del present Reglament ja durant el període transitori.

(179) El present Reglament s'ha d'aplicar a partir del 2 d'agost de 2026. No obstant això, tenint en compte el risc inacceptable associat a determinades formes d'ús de la IA, les prohibicions, i també les disposicions generals del present Reglament, s'han d'aplicar ja des del 2 de febrer de 2025. Tot i que aquestes prohibicions no són plenament efectives fins després de l'establiment de la governança i l'aplicació del present Reglament, és important preveure l'aplicació de les prohibicions per tenir en compte els riscos inacceptables i adaptar altres procediments, per exemple, en l'àmbit del dret civil. A més, la infraestructura relacionada amb la governança i el sistema d'avaluació de la conformitat han d'estar operatius abans del 2 d'agost de 2026, raó per la qual les disposicions sobre els organismes notificats i l'estructura de governança s'han d'aplicar des del 2 d'agost de 2025. Atesa la ràpida evolució tecnològica i l'elevat ritme d'adopció de models d'IA d'ús general, les obligacions dels proveïdors de models d'IA d'ús general s'han d'aplicar des del 2 d'agost de 2025. Els codis de bones pràctiques han d'estar llestos abans del 2 de maig de 2025 per permetre als proveïdors demostrar que compleixen dins el termini previst. L'Oficina d'IA ha d'assegurar-se que les normes i els procediments de classificació estiguin actualitzats d'acord amb els avenços tecnològics. Així mateix, els estats membres han d'establir i comunicar a la Comissió les normes referents a les sancions, incloses les multes administratives, i assegurar-se que, a la data d'aplicació del present Reglament, s'apliquin de manera adequada i efectiva. Per tant, les disposicions sobre sancions s'han d'aplicar a partir del 2 d'agost de 2025.

(180) El Supervisor Europeu de Protecció de Dades i el Comitè Europeu de Protecció de Dades, als quals es va consultar d'acord amb l'article 42, apartats 1 i 2, del Reglament (UE) 2018/1725, van emetre dictamen conjunt el 18 de juny de 2021.

HAN ADOPTAT EL PRESENT REGLAMENT:

CAPÍTOL I

DISPOSICIONS GENERALS

Article 1

Objecte

1. La finalitat del present Reglament és millorar el funcionament del mercat interior i promoure l'adopció de la intel·ligència artificial centrada en l'ésser humà i fiable, tot garantint un alt nivell de protecció de la salut, la seguretat, els drets fonamentals consagrats en la Carta, incloent-hi la democràcia, l'estat de dret i la protecció del medi ambient contra els efectes nocius dels sistemes d'IA a la Unió Europea i el suport a la innovació.

2. El Reglament estableix:

(a) normes harmonitzades per a la introducció en el mercat, la posada en servei i l'ús de sistemes d'IA a la Unió;

(b) prohibició de certes pràctiques d'IA;

(c) requisits específics per als sistemes d'IA d'alt risc i obligacions per als operadors d'aquests sistemes;

(d) normes harmonitzades de transparència per a determinats sistemes d'IA;

(i) normes harmonitzades per a la introducció en el mercat de models d'IA d'ús general;

(f) normes sobre el seguiment del mercat, la vigilància del mercat, la governança i la garantia del compliment;

(g) mesures en suport de la innovació, prestant especial atenció a les pimes, incloses les empreses emergents.

Article 2

Àmbit d'aplicació

1. El Reglament s'aplica a:

(a) proveïdors que introdueixen en el mercat o posen en servei sistemes d'IA o que comercialitzen models d'IA d'ús general a la Unió, independentment de si s'estableixen o estan dins la Unió o en un tercer país;

(b) els responsables del desplegament de sistemes d'IA que tinguin el lloc d'establiment o estiguin a la Unió;

(c) proveïdors i responsables del desplegament de sistemes d'IA que tinguin el lloc d'establiment o estiguin en un tercer país, on s'utilitzin els resultats de sortida generats pel sistema d'IA a la Unió;

(d) importadors i distribuïdors de sistemes d'IA;

(i) fabricants de productes que comercialitzen o posen en servei un sistema d'IA juntament amb el seu producte i sota el nom o la marca propis;

(f) representants autoritzats dels proveïdors, que no estiguin establerts a la Unió;

(g) persones afectades que estan a la Unió.

2. Per als sistemes d'IA classificats com a sistemes d'IA d'alt risc d'acord amb l'article 6, apartat 1, relatiu als productes coberts per la legislació d'harmonització de la Unió enumerada a l'annex I, secció B, només s'apliquen l'article 6, apartat 1, els articles 102 a 109 i l'article 112. L'article 57 només s'aplica en la mesura que els requisits per als sistemes d'IA d'alt risc en virtut del present Reglament s'han integrat en aquesta legislació d'harmonització de la Unió.

3. El Reglament no s'aplica als àmbits que quedin fora de l'àmbit d'aplicació del Dret de la Unió i, en qualsevol cas, no ha d'afectar les competències dels estats membres en matèria de seguretat nacional, independentment del tipus d'entitat a la qual els estats membres hagin encomanat l'acompliment de tasques en relació amb les competències esmentades.

El present Reglament no s'aplica als sistemes d'IA que –i en la mesura que sigui– s'introdueixin en el mercat, es posin en servei o s'utilitzin, amb modificacions o sense, exclusivament amb finalitats militars, de defensa o de seguretat nacional, independentment del tipus d'entitat que dugui a terme les activitats.

El Reglament no s'aplica als sistemes d'IA que no s'introdueixin en el mercat ni es posin en servei a la Unió, quan se'n facin servir els resultats de sortida a la Unió exclusivament amb finalitats militars, de defensa o de seguretat nacional, independentment del tipus d'entitat que faci les activitats.

4. El Reglament no s'aplica a les autoritats d'un tercer país ni a les organitzacions internacionals que estan en l'àmbit d'aplicació del present Reglament, de conformitat amb l'apartat 1, quan les autoritats o organitzacions utilitzin sistemes d'IA en el marc de la cooperació o acords internacionals per a la garantia del compliment de la llei i la cooperació judicial amb la Unió o amb un o més estats membres, sempre que aquest tercer país o organització internacional proporcioni garanties adequades respecte a la protecció dels drets i llibertats fonamentals de les persones.

5. El present Reglament no afecta l'aplicació de les disposicions sobre la responsabilitat dels proveïdors de serveis intermediaris que s'inclouen en el capítol II del Reglament (UE) 2022/2065.
6. El Reglament no s'aplica als sistemes d'IA ni als models d'IA, en què se n'inclouen els resultats de sortida, específicament desenvolupats i posats en servei amb l'únic propòsit de la recerca i el desenvolupament científic.
7. La legislació de la Unió sobre protecció de dades personals, privadesa i confidencialitat de les comunicacions s'aplica a les dades personals tractades en relació amb els drets i les obligacions establerts en el Reglament. El Reglament no afecta els reglaments (UE) 2016/679 o (UE) 2018/1725, ni la Directiva 2002/58/CE o (UE) 2016/680, sense perjudici de l'article 10, apartat 5, i l'article 59 del present Reglament.
8. El present Reglament no s'aplica a cap activitat de recerca, prova o desenvolupament sobre sistemes d'IA o models d'IA abans que s'introdueixin en el mercat o es posin en servei. Es tracta d'activitats que s'han de dur a terme de conformitat amb la legislació de la Unió que els sigui aplicable. Les proves en condicions reals no estan cobertes per aquesta exclusió.
9. El present Reglament s'ha d'entendre sense perjudici de les normes establertes per altres actes legislatius de la Unió relatius a la protecció del consumidor i a la seguretat dels productes.
10. El Reglament no s'aplica a les obligacions dels responsables del desplegament que siguin persones físiques que utilitzin sistemes d'IA en el curs d'una activitat no professional purament personal.
11. El present Reglament no impedeix que la Unió o els estats membres mantinguin o introdueixin disposicions legals, reglamentàries o administratives més favorables per als treballadors en matèria de protecció dels seus drets en relació amb l'ús dels sistemes d'IA per part dels empresaris, o fomentar o permetre l'aplicació de convenis col·lectius més favorables per als treballadors.
12. El Reglament no s'aplica als sistemes d'IA publicats sota llicències lliures i de codi obert, llevat que s'introdueixin en el mercat o es posin en servei com a sistemes d'IA d'alt risc o com a sistema d'IA que es trobi en virtut de l'article 5 o 50.

Article 3

Definicions

A l'efecte del Reglament s'apliquen les definicions següents:

- (1) "sistema IA": un sistema basat en una màquina que s'ha dissenyat per funcionar amb diferents nivells d'autonomia i que pot mostrar capacitat d'adaptació després del desplegament; que, per objectius explícits o implícits, infereix de la informació d'entrada que rep la manera de generar resultats de sortida; per exemple, prediccions, continguts, recomanacions o decisions, amb capacitat per influir en entorns físics o virtuals;
- (2) "risc": combinació de la probabilitat que es produeixi un dany i la gravetat d'aquest dany;
- (3) "proveïdor": persona física o jurídica, autoritat pública, òrgan o organisme que desenvolupi o tingui desenvolupat un sistema d'IA o un model d'IA d'ús general o que tingui un sistema d'IA

o un model d'IA d'ús general i l'introdueixi en el mercat o el posi en servei en nom propi o sota la marca registrada pròpia, mitjançant pagament o de forma gratuïta;

- (4) “responsable del desplegament”: una persona física o legal, autoritat pública, òrgan o un altre organisme que utilitza un sistema d'IA sota la seva autoritat, excepte quan el sistema d'IA s'utilitza en el curs d'una activitat personal no professional.
- (5) “representant autoritzat”: una persona física o jurídica ubicada o establerta a la Unió que hagi rebut i acceptat el mandat per escrit d'un proveïdor d'un sistema d'IA o d'un model d'IA d'ús general per complir les obligacions i dur a terme els procediments establerts en el present Reglament en representació d'aquest proveïdor;
- (6) “importador”: persona física o jurídica ubicada o establerta a la Unió que introdueix en el mercat un sistema d'IA que porta el nom o la marca d'una persona física o jurídica establerta en un tercer país;
- (7) “distribuïdor”: persona física o jurídica de la cadena de subministrament, diferent del proveïdor o de l'importador, que posa a disposició del mercat de la Unió un sistema d'IA;
- (8) “operador”: un proveïdor, fabricant de productes, responsable del desplegament, representant autoritzat, importador o distribuïdor;
- (9) “introducció en el mercat”: la primera posada a disposició d'un sistema d'IA o un model d'IA d'ús general en el mercat de la Unió;
- (10) “comercialització”: subministrament d'un sistema d'IA o d'un model d'IA d'ús general per distribuir-lo o fer-ne ús en el mercat de la Unió en el curs d'una activitat comercial, a canvi de pagament o de forma gratuïta;
- (11) “posada en servei” significa el subministrament d'un sistema d'IA per al primer ús directament al responsable del desplegament o per a ús propi a la Unió per a la finalitat que tenen prevista;
- (12) “finalitat prevista”: l'ús per al qual un sistema d'IA està destinat pel proveïdor, inclòs el context i les condicions específiques d'ús, tal com s'especifica en la informació subministrada pel proveïdor en les instruccions d'ús, els materials i les declaracions promocionals o de vendes o la documentació tècnica;

- (13) “ús indegut raonablement previsible”: l'ús d'un sistema d'IA d'una manera que no és conforme amb la seva finalitat prevista, però que pot resultar d'un comportament o interacció humana raonablement previsible amb altres sistemes, inclosos altres sistemes d'IA.
- (14) “component de seguretat”: component d'un producte o d'un sistema d'IA que compleix una funció de seguretat per a aquest producte o sistema d'IA, o el fracàs o mal funcionament del qual posa en perill la salut i la seguretat de les persones o béns;
- (15) “instruccions d'ús”: la informació proporcionada pel proveïdor per informar el responsable del desplegament de, en particular, el propòsit i l'ús adequat d'un sistema d'IA;
- (16) “recuperació d'un sistema d'IA”: qualsevol mesura que tingui com a objectiu aconseguir la devolució al proveïdor o la retirada del servei o la desactivació de l'ús d'un sistema d'IA posat a disposició dels responsables del desplegament;
- (17) “retirada d'un sistema d'IA”: qualsevol mesura que tingui com a objectiu evitar que un sistema d'IA en la cadena de subministrament estigui disponible al mercat;
- (18) “rendiment d'un sistema d'IA”: la capacitat d'un sistema d'IA per aconseguir la finalitat que té prevista;
- (19) “autoritat notificadora”: l'autoritat nacional encarregada d'establir i dur a terme els procediments necessaris per a l'avaluació, la designació i la notificació dels òrgans d'avaluació de la conformitat i el seu seguiment;
- (20) “avaluació de la conformitat”: el procés de demostrar si s'han complert els requisits establerts al capítol III, secció 2, relatius a un sistema d'IA d'alt risc.
- (21) “organisme d'avaluació de la conformitat” significa un organisme que fa activitats d'avaluació de la conformitat de tercers, incloses les proves, la certificació i la inspecció.
- (22) “organisme notificat” significa un organisme d'avaluació de la conformitat notificat d'acord amb el Reglament i amb la resta de la legislació d'harmonització de la Unió.

- (23) “modificació substancial”: un canvi en un sistema d'IA després de la introducció en el mercat o la posada en servei que no està previst o programat en l'avaluació inicial de conformitat feta pel proveïdor i com a resultat del qual el compliment del sistema d'IA amb els requisits establerts en el capítol III, la secció 2 es veu afectat o resulta en una modificació de la finalitat prevista per a la qual s'ha avaluat el sistema d'IA;
- (24) “marcatge CE”: un marcatge amb què un proveïdor indica que un sistema d'IA és conforme amb els requisits establerts en el capítol III, secció 2, i altra legislació d'harmonització de la Unió aplicable que en preveu l'adhesió;
- (25) “sistema de seguiment postcomercialització”: totes les activitats que els proveïdors de sistemes d'IA fan per recollir i revisar l'experiència obtinguda a partir de l'ús dels sistemes d'IA que introdueixen en el mercat o posen en servei amb la finalitat d'identificar la necessitat d'aplicar immediatament les accions correctores o preventives necessàries;
- (26) “autoritat de vigilància del mercat”: autoritat nacional que fa les activitats i pren les mesures de conformitat amb el Reglament (UE) 2019/1020;
- (27) “norma harmonitzada”: una norma harmonitzada tal com es defineix a l'article 2, apartat 1, lletra c), del Reglament (UE) 1025/2012;
- (28) “especificació comuna”: un conjunt d'especificacions tècniques tal com es defineix a l'article 2, punt (4) del Reglament (UE) 1025/2012, que proporciona mitjans per complir certs requisits establerts en virtut del present Reglament;
- (29) “dades d'entrenament”: les dades utilitzades per a l'entrenament d'un sistema d'IA ajustant-ne els paràmetres d'aprenentatge.
- (30) “dades de validació”: les dades utilitzades per proporcionar una avaluació del sistema d'IA entrenat i adaptar-ne els paràmetres no entrenables i el procés d'aprenentatge amb la finalitat, entre altres, d'evitar un ajustament insuficient o excessiu;
- (31) “conjunt de dades de validació”: un conjunt de dades independent o una part del conjunt de dades d'entrenament, que s'ha obtingut mitjançant una divisió fixa o variable;

- (32) "dades de prova": les dades usades per proporcionar una avaluació independent del sistema d'IA, per confirmar-ne el funcionament previst abans d'introduir-lo en el mercat o posar-lo en servei;
- (33) "dades d'entrada": les dades que es proporcionen a un sistema d'IA o que el sistema mateix adquireix directament, a partir de les quals el sistema produeix un resultat de sortida;
- (34) "dades biomètriques": les dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física, com ara imatges facials o dades dactiloscòpiques;
- (35) "identificació biomètrica": el reconeixement automatitzat de característiques humanes de caràcter físic, fisiològic, conductual o psicològic per determinar la identitat d'una persona física comparant-ne les dades biomètriques amb les dades biomètriques de persones emmagatzemades en una base de dades;
- (36) "verificació biomètrica": la verificació automatitzada i individualitzada, inclosa l'autenticació, de la identitat de les persones físiques comparant-ne les dades biomètriques amb dades biomètriques facilitades prèviament;
- (37) "categories especials de dades personals": les categories de dades personals a què es refereixen l'article 9, apartat 1, del Reglament (UE) 2016/679, l'article 10 de la Directiva (UE) 2016/680 i l'article 10, apartat 1, del Reglament (UE) 2018/1725;
- (38) "dades operatives sensibles": dades operatives relacionades amb activitats de prevenció, detecció, investigació o enjudiciament de delictes, quan el fet de divulgar-les podria posar en perill la integritat dels procediments penals;
- (39) "sistema de reconeixement d'emocions": sistema d'IA destinat a identificar o inferir emocions o intencions de les persones físiques a partir de les seves dades biomètriques;
- (40) "sistema de categorització biomètrica": sistema d'IA que té per finalitat assignar les persones físiques a categories específiques en funció de les seves dades biomètriques, llevat que sigui accessori a un altre servei comercial i estrictament necessari per raons tècniques objectives.
- (41) "sistema d'identificació biomètrica remota": un sistema d'IA destinat a identificar les persones físiques sense que hi participin de manera activa i generalment a distància

comparant-ne les dades biomètriques amb les dades que figuren en una base de dades de referència;

(42) “sistema d'identificació biomètrica remota en temps real”: sistema d'identificació biomètrica remota, en el qual la recollida de les dades biomètriques, la comparació i la identificació es produeixen sense una demora significativa; engloba no només la identificació instantània, sinó també, per tal d'evitar l'elusió, demores mínimes limitades;

(43) “sistema d'identificació biomètrica remota en diferit”: qualsevol sistema d'identificació biomètrica remota que no sigui un sistema d'identificació biomètrica remota en temps real;

(44) “espai d'accés públic”: qualsevol lloc físic, de propietat privada o pública, al qual pugui accedir un nombre indeterminat de persones físiques, amb independència que s'hagin de complir determinades condicions d'accés i amb independència de les possibles restriccions de capacitat;

(45) “autoritat garant del compliment de la llei” significa:

(a) tota autoritat pública competent per a la prevenció, la investigació, la detecció o l'enjudiciament de delictes o l'execució de sancions penals, incloses la protecció davant amenaces per a la seguretat pública i la prevenció d'aquestes amenaces, o

(b) qualsevol altre organisme o entitat al qual el dret de l'estat membre hagi confiat l'exercici de l'autoritat i les competències públiques a efectes de prevenció, investigació, detecció o enjudiciament de delictes o execució de sancions penals, incloses la protecció davant amenaces per a la seguretat pública i la prevenció d'aquestes amenaces;

(46) “garantia del compliment de la llei” es refereix a les activitats dutes a terme per les autoritats policials o en nom seu per a la prevenció, investigació, detecció o enjudiciament de delictes penals o l'execució de sancions penals, inclosa la salvaguarda i la prevenció d'amenaces a la seguretat pública;

(47) “Oficina d'IA”: la funció de la Comissió de contribuir a l'aplicació, el seguiment i la supervisió dels sistemes d'IA i els models d'IA d'ús general, i la governança de la IA, prevista en la decisió de la Comissió de 24 de gener de 2024; les referències del present Reglament a l'Oficina d'IA s'han de considerar referències a la Comissió;

(48) “autoritat nacional competent” significa una autoritat notificadora o una autoritat de vigilància del mercat; pel que fa als sistemes d'IA posats en servei o utilitzats per institucions,

òrgans, oficines i organismes de la Unió, les referències a autoritats nacionals competents o autoritats de vigilància del mercat en el Reglament s'han de considerar referències al Supervisor Europeu de Protecció de dades;

(49) Un incident greu és un incident o un mal funcionament d'un sistema d'IA que, directament o indirectament, condueix a qualsevol dels següents:

(a) mort d'una persona o dany greu per a la seva salut;

(b) alteració greu i irreversible de la gestió o el funcionament d'infraestructures crítiques;

(c) la infracció de les obligacions previstes en el dret de la Unió per a la protecció dels drets fonamentals;

(d) danys greus a la propietat o el medi ambient;

(50) "dades personals": les dades personals, tal com es defineixen a l'article 4, punt (1), del Reglament (UE) 2016/679;

(51) "dades no personals": les dades que no siguin dades personals tal com es defineixen a l'article 4, punt 1, del Reglament (UE) 2016/679;

(52) "elaboració de perfils": l'elaboració de perfils tal com es defineix a l'article 4, punt (4), del Reglament (UE) 2016/679;

(53) "pla de la prova en condicions reals": un document que descriu els objectius, la metodologia, l'àmbit geogràfic, poblacional i temporal, el seguiment, l'organització i la pràctica de la prova en condicions reals;

(54) «pla de l'espai controlat de proves»: un document acordat entre el proveïdor participant i l'autoritat competent en què es descriuen els objectius, les condicions, el calendari, la metodologia i els requisits per a les activitats fetes en l'espai controlat de proves;

(55) «espai controlat de proves per a la IA»: un marc controlat establert per una autoritat competent que ofereix als proveïdors i proveïdors potencials de sistemes d'IA la possibilitat de desenvolupar, entrenar, validar i provar, en condicions reals quan escaigui, un sistema d'IA

innovador, d'acord amb un pla de l'espai controlat de proves i durant un temps limitat, sota supervisió reglamentària;

(56) "alfabetització en IA": les capacitats, els coneixements i la comprensió que permeten als proveïdors, responsables del desplegament i altres persones afectades, tenint-ne en compte els drets i obligacions respectius en el context del Reglament, dur a terme un desplegament informat dels sistemes d'IA i prendre consciència de les oportunitats i els riscos que la IA planteja, i també els perjudicis que pot causar;

(57) "prova en condicions reals": la prova temporal d'un sistema d'IA per a la finalitat que té prevista en condicions reals, fora d'un laboratori o un altre entorn de simulació, per recaptar dades sòlides i fiables i avaluar i comprovar la conformitat del sistema d'IA amb els requisits del present Reglament; si es compleixen totes les condicions establertes a l'article 57 o 60, no es considera una introducció en el mercat o una posada en servei del sistema d'IA en el sentit de les disposicions del present Reglament;

(58) "subjecte": als efectes de la prova en condicions reals, una persona física que participa en la prova en condicions reals;

(59) "consentiment informat": expressió lliure, específica, inequívoca i voluntària de la voluntat de participar en una prova particular en condicions reals, després d'haver estat informat de tots els aspectes de les proves que són rellevants per a la decisió de l'interessat de participar.

(60) "ultrafals": un contingut d'imatge, àudio o vídeo generat o manipulat per una IA que s'assembla a persones, objectes, llocs, entitats o successos reals i que pot induir una persona a pensar erròniament que són autèntics o verídics;

(61) "infracció generalitzada": tot acte o omissió contrari al dret de la Unió pel qual es protegeixen els interessos de les persones i que:

(a) hagi perjudicat o pugui perjudicar els interessos col·lectius de persones que resideixen en almenys dos estats membres diferents d'aquell en què:

(i) l'acte o omissió es va originar o va tenir lloc;

(ii) estigui ubicat o establert el proveïdor de què es tracti o, si hi és, el seu representant autoritzat, o

(iii) estigui establert el responsable del desplegament en el moment de cometre la infracció;

(b) hagi perjudicat, perjudiqui o pugui perjudicar els interessos col·lectius de les persones i tingui característiques comunes –incloses la mateixa pràctica il·lícita o la vulneració del mateix interès– i sigui comès simultàniament pel mateix operador en almenys tres estats membres;

(62) "infraestructura crítica": una infraestructura crítica tal com es defineix a l'article 2, punt 4, de la Directiva (UE) 2022/2557;

(63) "model d'IA d'ús general": un model d'IA, també un d'entrenat amb un gran volum de dades utilitzant autosupervisió a gran escala, que presenta un grau considerable de generalitat i és capaç de fer de manera competent una gran varietat de tasques diferents, independentment de la manera com el model s'introdueixi en el mercat, i que pot integrar-se en diversos sistemes o aplicacions posteriors, excepte els models d'IA que s'utilitzen per a activitats de recerca, desenvolupament o creació de prototips abans d'introduir-los en el mercat;

(64) "capacitats de gran impacte": capacitats que igualen o superen les capacitats mostrades pels models d'IA d'ús general més avançats;

(65) «risc sistèmic»: un risc específic de les capacitats de gran impacte dels models d'IA d'ús general, amb repercussions considerables en el mercat de la Unió per l'abast o els efectes negatius reals o raonablement previsibles que tenen en la salut pública, la seguretat, la seguretat pública, els drets fonamentals o la societat en conjunt, que es poden propagar a gran escala al llarg de tota la cadena de valor;

(66) "sistema d'IA d'ús general": sistema d'IA que es basa en un model d'IA d'ús general i que té la capacitat de servir a una varietat de propòsits, tant per a ús directe com per a la integració en altres sistemes d'IA.

(67) "operació de punt flotant": qualsevol operació o tasca matemàtica que impliqui números de punt flotant, que són un subconjunt dels nombres reals normalment representats als ordinadors mitjançant un nombre sencer de precisió fixa elevat per l'exponent sencer d'una base fixa;

(68) "proveïdor de tram final": un proveïdor d'un sistema d'IA, també d'un sistema d'IA d'ús general, que integra un model d'IA, amb independència que el model d'IA el proporcionï ell

mateix i estigui integrat verticalment o el proporcioni una altra entitat en virtut de relacions contractuals.

Article 4

Alfabetització en matèria d'IA

Els proveïdors i responsables del desplegament de sistemes d'IA han d'adoptar mesures per garantir, fins on sigui possible, que el seu personal i altres persones que s'encarreguin en nom seu del funcionament i la utilització de sistemes d'IA tinguin un nivell suficient d'alfabetització en matèria d'IA, tenint-ne en compte coneixements tècnics, experiència, educació i formació professional, així com el context previst d'ús dels sistemes d'IA i les persones o els col·lectius de persones en què s'han de fer servir aquests sistemes.

CAPÍTOL II

PRÀCTIQUES D'IA PROHIBIDES

Article 5

Pràctiques d'IA prohibides

1. Queden prohibides les pràctiques d'IA següents:

(a) la introducció en el mercat, la posada en servei o la utilització d'un sistema d'IA que faci servir tècniques subliminars que transcendeixin la consciència d'una persona o de tècniques deliberadament manipuladores o enganyoses amb l'objectiu o per alterar de manera substancial el comportament d'una persona o un col·lectiu de persones, minvant-ne de manera apreciable la capacitat per prendre una decisió informada i fent que prenguin una decisió que altrament no haurien pres, d'una manera que provoqui, o sigui raonablement probable que provoqui, perjudicis considerables a aquesta persona, a una altra persona o a un col·lectiu de persones;

(b) la introducció en el mercat, la posada en servei o la utilització d'un sistema d'IA que exploti alguna de les vulnerabilitats d'una persona física o un determinat col·lectiu de persones derivades de la seva edat o discapacitat, o d'una situació social o econòmica específica, amb la finalitat o l'efecte d'alterar de manera substancial el comportament d'aquesta persona o d'una persona que pertanyi a aquest col·lectiu d'una manera que provoqui, o sigui raonablement probable que provoqui, perjudicis considerables a aquesta persona o a una altra;

(c) la introducció en el mercat, la posada en servei o la utilització de sistemes d'IA per avaluar o classificar persones físiques o col·lectius de persones durant un període determinat de temps atenant-ne el comportament social o les característiques personals o de la personalitat conegudes, inferides o predites, de manera que la puntuació social resultant provoqui una o més de les situacions següents:

(i) un tracte perjudicial o desfavorable envers determinades persones físiques o col·lectius de persones en contextos socials que no guardin relació amb els contextos en què es van generar o recaptar les dades originalment;

- (ii) un tracte perjudicial o desfavorable envers determinades persones físiques o col·lectius de persones que sigui injustificat o desproporcionat respecte al seu comportament social o la gravetat d'aquest;
- (d) la introducció en el mercat, la posada en servei per a aquest fi específic o l'ús d'un sistema d'IA per avaluar riscos de persones físiques i així valorar o predir el risc que una persona física cometi un delictes basant-se únicament en l'elaboració del perfil d'una persona física o en l'avaluació dels trets i característiques de la seva personalitat; aquesta prohibició no s'aplica als sistemes d'IA utilitzats per donar suport a la valoració humana de la implicació d'una persona en una activitat delictiva que ja es basi en fets objectius i verificables directament relacionats amb una activitat delictiva;
- (i) la introducció en el mercat, la posada en servei per a aquest fi específic o l'ús de sistemes d'IA que creïn o amplii bases de dades de reconeixement facial mitjançant l'extracció no selectiva d'imatges facials d'internet o de circuits tancats de televisió;
- (f) la introducció en el mercat, la posada en servei per a aquest fi específic o l'ús de sistemes d'IA per inferir les emocions d'una persona física en els llocs de treball i en els centres educatius, excepte quan el sistema d'IA estigui destinat a ser instal·lat o introduït en el mercat per motius mèdics o de seguretat;
- (g) la introducció en el mercat, la posada en servei per a aquest fi específic o l'ús de sistemes de categorització biomètrica que classifiquin individualment les persones físiques sobre la base de les seves dades biomètriques per deduir-ne o inferir-ne raça, opinions polítiques, afiliació sindical, conviccions religioses o filosòfiques, vida sexual o orientació sexual; aquesta prohibició no inclou l'etiquetatge o filtratge de conjunts de dades biomètriques adquirides lícitament, com imatges, basat en dades biomètriques ni la categorització de dades biomètriques en l'àmbit de la garantia del compliment de la llei;
- (h) l'ús de sistemes d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei, excepte i en la mesura que aquest ús sigui estrictament necessari per assolir un dels objectius següents:
- (i) la recerca selectiva de víctimes concretes de segrest tracta d'éssers humans o explotació sexual d'éssers humans, així com la recerca de persones desaparegudes;
 - (ii) la prevenció d'una amenaça específica, substancial i imminent per a la vida o la seguretat física de les persones físiques o d'una amenaça real i present o real i previsible d'un atac terrorista;

(iii) la localització o identificació d'una persona sospitosa d'haver comès un delicte a l'efecte de dur a terme una investigació penal o enjudiciament o execució d'una pena per delictes esmentats en l'annex II i punibles en l'estat membre afectat amb una pena de custòdia o una ordre de detenció per un període màxim de quatre anys.

El subapartat primer, lletra h), s'entén sense perjudici de les disposicions de l'article 9 del Reglament (UE) 2016/679 pel que fa al tractament de dades biomètriques amb finalitats diferents de la garantia del compliment de la llei.

2. L'ús de sistemes d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei per a qualsevol dels objectius esmentats a l'apartat 1, subapartat primer, lletra h), s'ha de desplegar per a les finalitats establertes en aquesta lletra, únicament per confirmar la identitat de la persona que constitueix l'objectiu específic, i ha de tenir en compte els aspectes següents:

(a) la naturalesa de la situació que doni lloc al possible ús, i en particular la gravetat, probabilitat i magnitud del perjudici que es produiria de no utilitzar-se el sistema;

(b) les conseqüències que tindria l'ús del sistema en els drets i les llibertats de les persones implicades, i en particular la gravetat, probabilitat i magnitud d'aquestes conseqüències.

A més, l'ús de sistemes d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei per a qualsevol dels objectius esmentats en l'apartat 1, subapartat primer, lletra h), del present article ha de complir garanties i condicions necessàries i proporcionades en relació amb l'ús de conformitat amb el dret nacional que autoritzi aquest ús; en particular, pel que fa a les limitacions temporals, geogràfiques i personals. L'ús del sistema d'identificació biomètrica remota «en temps real» en espais d'accés públic només s'ha d'autoritzar si l'autoritat garant del compliment de la llei ha completat una avaluació d'impacte relativa als drets fonamentals segons el que disposa l'article 27 i ha registrat el sistema a la base de dades de la UE de conformitat amb l'article 49. No obstant això, en casos d'urgència degudament justificats, es pot començar a utilitzar aquests sistemes sense el registre a la base de dades de la UE, sempre que aquest registre es faci sense demora indeguda.

3. Als efectes de l'apartat 1, subapartat primer, lletra h), i l'apartat 2, tot ús d'un sistema d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei s'ha de supeditar a la concessió d'una autorització prèvia per part d'una autoritat judicial o una autoritat administrativa independent, amb poder de decisió vinculant, de l'estat membre on s'hagi d'utilitzar aquest sistema, que s'expedirà prèvia sol·licitud motivada i de conformitat amb les normes detallades del dret nacional esmentades a l'apartat 5. No obstant això, en una situació d'urgència degudament justificada, se'n pot començar a fer ús sense autorització sempre que es demani l'autorització sense demora indeguda, en el termini de 24 hores. En cas de denegació, l'ús s'ha d'aturar amb efecte immediat i totes les dades, així com els resultats i resultats de sortida d'aquest ús, s'han de rebutjar i esborrar immediatament.

L'autoritat judicial competent o una autoritat administrativa independent, amb poder de decisió vinculant, només pot concedir l'autorització quan, sobre la base de proves objectives o d'indicis clars que se li aportin, tingui constància que l'ús del sistema d'identificació biomètrica remota «en temps real» és necessari i proporcionat per assolir algun dels objectius especificats a

l'apartat 1, subapartat primer, lletra h), que s'ha d'indicar a la sol·licitud, i, en particular, es limita a l'estrictament necessari pel que fa al període de temps, així com a l'àmbit geogràfic i personal. En pronunciar-se al respecte, aquesta autoritat ha de tenir en compte els aspectes esmentats a l'apartat 2. No es pot prendre cap decisió que produeixi un efecte jurídic advers sobre una persona sobre la base exclusiva de la sortida del sistema d'identificació biomètrica remota “en temps real”.

4. Sens perjudici de les disposicions de l'apartat 3, tot ús d'un sistema d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei s'ha de notificar a l'autoritat de vigilància del mercat pertinent i a l'autoritat nacional de protecció de dades de conformitat amb les normes nacionals a què l'apartat 5 es refereix. La notificació ha de contenir, com a mínim, la informació especificada a l'apartat 6, sense dades operatives sensibles.

5. Els estats membres poden decidir contemplar la possibilitat d'autoritzar, totalment o parcialment, l'ús de sistemes d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei dins els límits i en les condicions que s'indiquen a l'apartat 1, subapartat primer, lletra h) i els apartats 2 i 3. Els estats membres interessats han d'establir en la legislació nacional les regles necessàries detallades per a la sol·licitud, emissió, exercici i informació relacionades amb les autoritzacions a què l'apartat 3 es refereix. Aquestes regles també han d'especificar en relació amb quin dels objectius esmentats en l'apartat 1, subapartat primer, lletra (h), incloent-hi quin dels delictes que s'esmenten en el punt (iii) de la lletra (h), les autoritats competents poden estar autoritzades per fer servir els sistemes amb la finalitat de garantia del compliment de la llei. Els estats membres han de notificar aquestes normes a la Comissió en el termini de trenta dies després que s'hagin adoptat. De conformitat amb el dret de la Unió, els estats membres poden adoptar lleis més restrictives sobre l'ús de sistemes d'identificació biomètrica remota.

6. Les autoritats nacionals de vigilància del mercat i les autoritats nacionals de protecció de dades dels estats membres a les quals s'hagi notificat l'ús de sistemes d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei d'acord amb l'apartat 4 han de presentar a la Comissió informes anuals sobre aquest ús. Amb aquesta finalitat, la Comissió ha de facilitar als estats membres i a les autoritats nacionals de vigilància del mercat i de protecció de dades un model que inclogui informació sobre el nombre de decisions adoptades per les autoritats judicials competents o una autoritat administrativa independent amb facultat de decisió vinculant en relació amb les sol·licituds d'autorització de conformitat amb l'apartat 3, així com el seu resultat.

7. La Comissió ha de publicar informes anuals sobre l'ús de sistemes d'identificació biomètrica remota «en temps real» en espais d'accés públic amb finalitats de garantia del compliment de la llei elaborats basats en dades agregades relatives als estats membres sobre la base dels informes anuals a què es refereix l'apartat 6. Aquests informes anuals no poden incloure dades operatives sensibles de les activitats de garantia del compliment de la llei connexes.

8. El present article no afecta les prohibicions aplicables quan una pràctica d'IA infringeixi altres disposicions del dret de la Unió.

CAPÍTOL III

SISTEMES D'IA D'ALT RISC

SECCIÓ 1

Classificació dels sistemes d'IA com a sistemes d'alt risc

Article 6

Regles de classificació per a sistemes d'IA d'alt risc

1. Amb independència de si s'ha introduït en el mercat o s'ha posat en servei sense estar integrat en els productes que s'esmenten en les lletres a) i b), un sistema d'IA es considera d'alt risc quan reuneix les dues condicions que s'indiquen a continuació:

(a) El sistema d'IA està destinat a l'ús com a component de seguretat d'un producte que entri en l'àmbit d'aplicació de la legislació d'harmonització de la Unió enumerats a l'annex I, o el sistema d'IA mateix és un d'aquests productes.

(b) El producte de què el sistema d'IA és component de seguretat d'acord amb la lletra a), o el sistema d'IA com a producte, s'ha de sotmetre a una avaluació de la conformitat de tercers per introduir-lo en el mercat o posar-lo en servei d'acord amb els actes legislatius d'harmonització de la Unió que s'enumeren a l'annex I.

2. A més dels sistemes d'IA d'alt risc que l'apartat 1 esmenta, es consideren d'alt risc els sistemes d'IA a què es refereix l'annex III.

3. No obstant les disposicions de l'apartat 2, un sistema d'IA esmentat a l'annex III no es considera d'alt risc quan no planteja un risc important de causar un perjudici a la salut, la seguretat o els drets fonamentals de les persones físiques, també si no influeix de manera substancial en el resultat de la presa de decisions.

El subapartat primer s'ha d'aplicar quan es compleix qualsevol de les condicions següents:

(a) El sistema d'IA està destinat a fer una tasca de procediment limitada.

(b) El sistema d'IA està destinat a millorar el resultat d'una activitat humana feta prèviament.

(c) El sistema d'IA té per finalitat detectar patrons de presa de decisions o desviacions dels patrons de presa de decisions anteriors i no està destinat a reemplaçar l'avaluació humana feta prèviament o influir-hi, sense una revisió humana adequada.

(d) El sistema d'IA està destinat a fer una funció preparatòria per a una avaluació pertinent als efectes dels casos d'ús enumerats a l'annex III.

No obstant el que disposa el subapartat primer, els sistemes d'IA a què l'annex III es refereix sempre es consideren d'alt risc quan el sistema d'IA elabori perfils de persones físiques.

4. Un proveïdor que consideri que un sistema d'IA a què es refereix l'annex III no és d'alt risc n'ha de documentar l'avaluació abans que el sistema s'introdueixi en el mercat o en servei. Aquest proveïdor està subjecte a l'obligació de registre establerta en l'article 49, apartat 2. A

petició de les autoritats nacionals competents, el proveïdor ha de facilitar la documentació de l'avaluació.

5. Prèvia consulta al Consell Europeu d'Intel·ligència Artificial ("Consell"), i no més tard del 2 de febrer de 2026, la Comissió ha de proporcionar directrius que especifiquin l'aplicació pràctica d'aquest article d'acord amb l'article 96, juntament amb una llista exhaustiva d'exemples pràctics de casos d'ús de sistemes d'IA que siguin d'alt risc i que no siguin d'alt risc.

6. La Comissió està facultada per adoptar actes delegats d'acord amb l'article 97 per modificar l'apartat 3, paràgraf segon, del present article, afegint noves condicions que s'hi estableixen, o modificant-les, quan hi hagi proves concretes i fiables de l'existència de sistemes d'IA que entrin en l'àmbit d'aplicació de l'annex III, però que no plantegin un risc important de causar un perjudici a la salut, la seguretat o els drets fonamentals de les persones físiques.

7. La Comissió ha d'adoptar actes delegats d'acord amb l'article 97 amb la finalitat de modificar l'apartat 3, apartat segon, del present article, suprimint qualsevol de les condicions que s'hi estableixen, quan hi hagi proves concretes i fiables que és necessari per mantenir el nivell de protecció de la salut, la seguretat i els drets fonamentals previst en el Reglament.

8. Cap modificació de les condicions establertes a l'apartat 3, subapartat segon, adoptada de conformitat amb els apartats 6 i 7 del present article, no pot reduir el nivell global de protecció de la salut, la seguretat i els drets fonamentals previst en el Reglament, i qualsevol modificació ha de garantir la coherència amb els actes delegats adoptats d'acord amb l'article 7, apartat 1, i ha de tenir en compte l'evolució tecnològica i del mercat.

Article 7

Modificacions de l'annex III

1. La Comissió està facultada per adoptar actes delegats d'acord amb l'article 97 per modificar l'annex III mitjançant l'addició o modificació de casos d'ús de sistemes d'IA d'alt risc quan es compleixen les dues condicions següents:

(a) que els sistemes d'IA estiguin destinats a què se'n faci ús en qualsevol dels àmbits que figuren a l'annex III, i

(b) que els sistemes d'IA plantegin un risc de perjudicar la salut i la seguretat o de tenir repercussions negatives en els drets fonamentals, i que aquest risc sigui equivalent o superior al risc de perjudici o de repercussions negatives que comporten els sistemes d'IA d'alt risc que ja s'esmenten a l'annex III.

2. En avaluar l'estat en virtut de l'apartat 1, lletra b), la Comissió ha de tenir en compte els criteris següents:

(a) la finalitat prevista del sistema d'IA;

(b) la mesura en què s'hagi fet servir o es pugui fer servir un sistema d'IA;

- (c) la naturalesa i la quantitat de les dades tractades i utilitzades pel sistema d'IA, en particular si es tracten categories especials de dades personals;
- (d) el grau d'autonomia amb què el sistema d'IA actua i la possibilitat que un ésser humà anul·li una decisió o recomanacions que puguin donar lloc a un perjudici;
- (i) la mesura en què la utilització d'un sistema d'IA ja hagi causat un perjudici a la salut i la seguretat, hagi tingut repercussions negatives en els drets fonamentals o hagi donat lloc a problemes importants en relació amb la probabilitat d'aquest perjudici o les repercussions negatives, segons demostrin, per exemple, els informes o les alegacions documentades que es presentin a les autoritats nacionals competents o qualsevol altre informe, segons escaigui;
- (f) l'abast potencial d'aquest dany o d'aquest impacte advers, en particular en termes de la intensitat i la capacitat d'afectar múltiples persones o d'afectar desproporcionadament un grup particular de persones;
- (g) la mesura en què les persones que podrien patir aquest perjudici o aquestes repercussions negatives depenguin del resultat generat per un sistema d'IA, en particular perquè, per motius pràctics o jurídics, no sigui raonablement possible renunciar-hi;
- (h) la mesura en què hi hagi un desequilibri de poder o les persones que podrien patir aquest perjudici o les repercussions negatives esmentades estiguin en una posició de vulnerabilitat respecte del responsable del desplegament d'un sistema d'IA, en particular a causa de la seva situació, autoritat, coneixements, circumstàncies econòmiques o socials, o edat;
- (i) la mesura en què sigui fàcil corregir o revertir el resultat generat fent servir un sistema d'IA, tenint en compte les solucions tècniques disponibles per corregir-lo o revertir-lo i sense que s'hagi de considerar que els resultats que afecten negativament la salut, la seguretat o els drets fonamentals són fàcils de corregir o revertir;
- (j) la magnitud i probabilitat de benefici del desplegament del sistema d'IA per a individus, grups o societat en general, incloses les possibles millores en la seguretat dels productes;
- (k) la mesura en què el dret de la Unió vigent estableixi:
- (i) vies de recurs efectives en relació amb els riscos que un sistema d'IA planteja, amb exclusió de les accions per danys i perjudicis;

(ii) mesures eficaces per prevenir o minimitzar notablement aquests riscos.

3. La Comissió està facultada per adoptar actes delegats d'acord amb l'article 97 per modificar la llista de l'annex III mitjançant la supressió de sistemes d'IA d'alt risc quan es compleixen les dues condicions següents:

(a) Els sistemes d'IA d'alt risc de què es tracti ja no comporten riscos considerables per als drets fonamentals, la salut o la seguretat, tenint en compte els criteris enumerats a l'apartat 2.

(b) La supressió no redueix el nivell general de protecció de la salut, la seguretat i els drets fonamentals d'acord amb el dret de la Unió.

SECCIÓ 2

Requisits dels sistemes d'IA d'alt risc

Article 8

Compliment dels requisits

1. Els sistemes d'IA d'alt risc han de complir els requisits establerts en la present secció, tenint en compte les finalitats previstes, així com l'estat actual de la tècnica generalment reconegut en matèria d'IA i tecnologies relacionades amb la IA. En garantir el compliment d'aquests requisits s'ha de tenir en compte el sistema de gestió de riscos a què l'article 9 es refereix.

2. Quan un producte contingui un sistema d'IA al qual s'apliquin els requisits del Reglament, així com els requisits de la legislació d'harmonització de la Unió enumerada a l'annex I, secció A, els proveïdors són responsables de garantir que el seu producte compleixi plenament tots els requisits aplicables en virtut de la legislació d'harmonització de la Unió que siguin aplicables. Per garantir que els sistemes d'IA d'alt risc a què l'apartat 1 es refereix compleixen els requisits establerts en aquesta secció, i per garantir coherència, evitar duplicacions i càrregues addicionals, els proveïdors han de tenir l'opció d'integrar, segons correspongui, els processos de prova i d'elaboració d'informes i la informació i documentació que subministren sobre el seu producte amb documentació i procediments que ja existeixen i que s'exigeixen per la legislació d'harmonització de la Unió que s'esmenta en la secció A de l'annex I.

Article 9

Sistema de gestió de riscos

1. S'ha d'establir, aplicar, documentar i mantenir un sistema de gestió de riscos en relació amb els sistemes d'IA d'alt risc.

2. El sistema de gestió de riscos s'ha d'entendre com un procés iteratiu continu planificat i executat durant tot el cicle de vida d'un sistema d'IA d'alt risc, que requereix revisió i actualització sistemàtiques regulars. Ha de constar de les etapes següents:

(a) identificació i anàlisi dels riscos coneguts i raonablement previsibles que el sistema d'IA d'alt risc pot comportar per a la salut, la seguretat o els drets fonamentals quan el sistema d'IA d'alt risc s'utilitzi d'acord amb la finalitat prevista;

(b) estimació i avaluació dels riscos que poden sorgir quan el sistema d'IA d'alt risc s'utilitza d'acord amb la finalitat que se li ha previst i en condicions d'ús raonablement previsibles;

(c) avaluació d'altres riscos que es puguin derivar, basada en l'anàlisi de les dades recollides del sistema de seguiment postcomercialització a què es refereix l'article 72;

(d) l'adopció de mesures adequades i específiques de gestió de riscos dissenyades per fer front als riscos detectats d'acord amb la lletra a).

3. Els riscos a què l'article es refereix són els que es poden mitigar o eliminar raonablement mitjançant el desenvolupament o el disseny del sistema d'IA d'alt risc, o el subministrament d'informació tècnica adequada.

4. Les mesures de gestió de riscos esmentades a l'apartat 2, lletra d), han de tenir degudament en compte els efectes i la possible interacció derivats de l'aplicació combinada dels requisits establerts en aquesta secció, amb vista a reduir al mínim els riscos de manera més eficaç alhora que s'assoleix un equilibri adequat en l'aplicació de les mesures per complir-los.

5. Les mesures de gestió de riscos esmentades a l'apartat 2, lletra d), han de considerar acceptables els riscos residuals pertinents associats a cada perill, i també el risc residual general dels sistemes d'IA d'alt risc.

En determinar les mesures de gestió de riscos més adequades, cal procurar el següent:

(a) eliminació o reducció dels riscos identificats i avaluats de conformitat amb l'apartat 2, en la mesura que sigui tècnicament possible, mitjançant un disseny i desenvolupament adequats del sistema d'IA d'alt risc;

(b) si escau, aplicació de mesures de mitigació i control adequades per abordar els riscos que no es poden eliminar.

(c) subministrament d'informació requerida de conformitat amb l'article 13 i, si escau, formació per als responsables del desplegament.

Per eliminar o reduir els riscos relacionats amb l'ús del sistema d'IA d'alt risc, s'ha de tenir en compte el coneixement tècnic, l'experiència, l'educació, l'entrenament que s'espera del responsable del desplegament i el context previst per a l'ús del sistema.

6. Els sistemes d'IA d'alt risc s'han de provar amb la finalitat d'identificar les mesures de gestió de riscos més adequades i específiques. Les proves han d'assegurar que els sistemes d'IA d'alt risc funcionin de manera coherent amb la finalitat que se'ls atribueix i que compleixin els requisits establerts en aquesta secció.

7. Els procediments de prova poden incloure proves en condicions reals de conformitat amb l'article 60.

8. Les proves dels sistemes d'IA d'alt risc s'han de fer, segons correspongui, en qualsevol moment durant tot el procés de desenvolupament i, en tot cas, abans que els sistemes

s'introdueixin en el mercat o es posin en servei. Les proves s'han de fer utilitzant paràmetres i llindars de probabilitats definits prèviament que siguin adequats per a la finalitat prevista del sistema d'IA d'alt risc.

9. Quan el sistema de gestió de riscos previst en els apartats 1 a 7 s'implanti, els proveïdors han de prestar atenció a si, atesa la finalitat prevista, és probable que el sistema d'IA d'alt risc afecti negativament les persones menors de divuit anys i, si escau, altres col·lectius vulnerables.

10. En el cas dels proveïdors de sistemes d'IA d'alt risc que estiguin subjectes a requisits relatius a processos interns de gestió de riscos d'acord amb altres disposicions pertinents del dret de la Unió, els aspectes previstos en els apartats 1 a 9 poden formar part dels procediments de gestió de riscos establerts d'acord amb aquest Dret, o combinar-s'hi.

Article 10

Dades i governança de dades

1. Els sistemes d'IA d'alt risc que utilitzen tècniques que impliquen l'entrenament de models d'IA amb dades s'han de desenvolupar a partir de conjunts de dades d'entrenament, validació i prova que compleixin els criteris de qualitat a què els apartats 2 a 5 es refereixen sempre que es facin servir els conjunts de dades esmentats.

2. Els conjunts de dades d'entrenament, validació i prova s'han de sotmetre a pràctiques de governança i gestió de dades adequades per a la finalitat prevista del sistema d'IA d'alt risc. Aquestes pràctiques se centren, en particular, en el següent:

(a) les opcions de disseny pertinents;

(b) els processos de recollida de dades i l'origen de les dades, i en el cas de les dades personals, la finalitat original de la recollida;

(c) les operacions de tractament oportunes per a la preparació de les dades, com ara l'anotació, l'etiquetatge, la depuració, l'actualització, l'enriquiment i l'agregació;

(d) la formulació de supòsits, en particular pel que fa a la informació que s'espera que les dades mesurin i representin;

(i) una avaluació de la disponibilitat, quantitat i idoneïtat dels conjunts de dades que siguin necessaris;

(f) l'examen en vista de possibles biaixos que puguin afectar la salut i la seguretat de les persones, afectar negativament els drets fonamentals o donar lloc a algun tipus de discriminació prohibida pel dret de la Unió, especialment quan els resultats de sortida de dades influeixin en les informacions d'entrada de futures operacions;

(g) mesures adequades per detectar, prevenir i mitigar possibles biaixos detectats d'acord amb la lletra f);

(h) la identificació i abordatge de llacunes o deficiències de dades rellevants que impedeixin el compliment del Reglament.

3. Els conjunts de dades d'entrenament, validació i prova han de ser pertinents, prou representatius i, fins on sigui possible, estar exempts d'errors i complets en vista de la finalitat prevista. A més, han de tenir les propietats estadístiques adequades, per exemple, quan escaigui, pel que fa a les persones o els col·lectius de persones en relació amb els quals es preveu l'ús del sistema d'IA d'alt risc. Els conjunts de dades poden reunir aquestes característiques per a cada conjunt de dades individualment o per a una combinació d'aquestes.

4. En la mesura necessària per a la finalitat prevista, els conjunts de dades han de tenir en compte les característiques o els elements particulars de l'entorn geogràfic, contextual, conductual o funcional específic en què està previst que s'utilitzi el sistema d'IA d'alt risc.

5. En la mesura que sigui estrictament necessari per garantir la detecció i correcció de biaixos en relació amb els sistemes d'IA d'alt risc d'acord amb l'apartat 2, lletres f) i g) d'aquest article, els proveïdors d'aquests sistemes poden tractar excepcionalment categories especials de dades personals, sempre que ofereixin les garanties adequades per als drets i llibertats fonamentals de les persones físiques. A més de les disposicions establertes en els reglaments (UE) 2016/679 i (UE) 2018/1725 i la Directiva (UE) 2016/680, perquè es produeixi aquest tractament, s'han de complir totes les condicions següents:

(a) La detecció i correcció de biaixos no es pot complir efectivament mitjançant el processament d'altres dades, incloses dades sintètiques o anonimitzades.

(b) Les categories especials de dades personals estan subjectes a limitacions tècniques sobre la reutilització de les dades personals, i les mesures de seguretat i preservació de la privadesa de l'última tecnologia, incloent-hi la pseudonimització.

(c) Les categories especials de dades personals estan subjectes a mesures per assegurar que les dades personals tractades estan protegides, subjectes a les garanties adequades, inclosos els controls estrictes i la documentació de l'accés, per evitar un mal ús i garantir que només les persones autoritzades hi tinguin accés amb les obligacions de confidencialitat adequades.

(d) Les categories especials de dades personals no es transmeten ni transfereixen a tercers i aquests no hi poden accedir de cap manera.

(i) Les categories especials de dades personals s'eliminen una vegada corregit el biaix o les dades personals han arribat al final del període de conservació, si la data és anterior.

(f) Els registres de les activitats de tractament d'acord amb els reglaments (UE) 2016/679 i (UE) 2018/1725 i la Directiva (UE) 2016/680 inclouen les raons per les quals el tractament de categories especials de dades personals era estrictament necessari per detectar i corregir biaixos, i per les quals aquest objectiu no es podia assolir mitjançant el tractament d'altres dades.

6. Per al desenvolupament de sistemes d'IA d'alt risc que no utilitzin tècniques d'entrenament de models d'IA, els paràgrafs 2 a 5 s'apliquen només als conjunts de dades de proves.

Article 11

Documentació tècnica

1. La documentació tècnica d'un sistema d'IA d'alt risc s'ha d'elaborar abans que aquest sistema s'introdueixi en el mercat o es posi en servei, i s'ha de mantenir actualitzada.

La documentació tècnica s'ha d'elaborar de manera que es demostrï que el sistema d'IA d'alt risc compleix els requisits establerts en aquesta secció i proporciona a les autoritats competents nacionals i als organismes notificats la informació necessària de manera clara i exhaustiva per avaluar el compliment d'aquests requisits per part del sistema. Ha de contenir, com a mínim, els elements establerts a l'annex IV. Les PIMES, incloses les empreses emergents, poden aportar de forma simplificada els elements de la documentació tècnica especificada a l'annex IV. Amb aquesta finalitat, la Comissió ha d'establir un formulari de documentació tècnica simplificada destinat a les necessitats de les petites i microempreses. Quan opti per proporcionar de manera simplificada la informació requerida a l'annex IV, una pime, inclosa una empresa emergent, ha de fer servir el formulari a què aquest apartat es refereix. Per a l'avaluació de la conformitat, els organismes notificats han d'acceptar el formulari.

2. Quan un sistema d'IA d'alt risc relacionat amb un producte cobert per la legislació d'harmonització de la Unió enumerada a l'annex I, secció A, es comercialitzi o posi en servei, s'ha d'elaborar un únic conjunt de documentació tècnica que contingui tota la informació establerta a l'apartat 1, i també la informació requerida en aquests actes legislatius.

3. La Comissió està facultada per adoptar actes delegats d'acord amb l'article 97 per modificar l'annex IV, quan sigui necessari, per garantir que, en vista dels avenços tècnics, la documentació tècnica proporcionï tota la informació necessària per avaluar si el sistema compleix els requisits establerts en aquesta secció.

Article 12

Conservació de registres

1. Els sistemes d'IA d'alt risc permeten tècnicament el registre automàtic d'esdeveniments (registres) al llarg de la vida del sistema.

2. Per garantir un nivell de traçabilitat del funcionament d'un sistema d'IA d'alt risc que sigui adequat a la finalitat prevista del sistema, les capacitats de registre han de permetre l'enregistrament d'esdeveniments rellevants per:

(a) identificar les situacions que puguin resultar en un sistema d'IA d'alt risc que presenti un risc en el sentit de l'article 79, apartat 1, o en una modificació substancial;

(b) facilitar el seguiment, postcomercialització a què l'article 72 es refereix; i

(c) seguir el funcionament dels sistemes d'IA d'alt risc a què l'article 26, apartat 5, es refereix.

3. Pel que fa als sistemes d'IA d'alt risc a què es refereix el punt 1, lletra a), de l'annex III, les capacitats d'inici de sessió han d'incloure, com a mínim:

(a) registre del període de cada ús del sistema (data d'inici i hora i data de finalització i hora de cada ús);

(b) la base de dades de referència amb què el sistema ha comprovat les dades;

(c) les dades d'entrada per a les quals la cerca ha portat a una correspondència;

(d) la identificació de les persones físiques implicades en la verificació dels resultats que s'esmenten a l'article 14, apartat 5.

Article 13

Transparència i informació als responsables del desplegament

1. Els sistemes d'IA d'alt risc s'han de dissenyar i desenvolupar d'una manera que garanteixi que funcionen amb un nivell de transparència suficient perquè els responsables del desplegament n'interpretin i usin correctament els resultats de sortida. S'ha de garantir un tipus i un nivell de transparència adequats perquè el proveïdor i el responsable del desplegament puguin complir les obligacions previstes a la secció 3.

2. Els sistemes d'IA d'alt risc s'han d'acompanyar amb les instruccions d'ús corresponents en un format digital o d'altre tipus adequat, que incloguin informació concisa, completa, correcta i clara que sigui pertinent, accessible i comprensible per als responsables del desplegament.

3. Les instruccions d'ús han de contenir com a mínim la informació següent:

(a) la identitat i les dades de contacte del proveïdor i, si escau, del seu representant autoritzat;

(b) les característiques, capacitats i limitacions del rendiment del sistema d'IA d'alt risc, incloent-hi el següent:

(i) la finalitat prevista;

(ii) el nivell de precisió (inclosos els paràmetres per mesurar-la), solidesa i ciberseguretat esmentat a l'article 15 respecte al qual s'hagi provat i validat el sistema d'IA d'alt risc i que es pot esperar, així com qualsevol circumstància coneguda i previsible que pugui afectar el nivell de precisió, solidesa i ciberseguretat esperat;

- (iii) qualsevol circumstància, coneguda o previsible, relacionada amb l'ús del sistema d'IA d'alt risc d'acord amb la finalitat que té prevista o en condicions d'ús raonablement previsibles d'ús inadequat, que pugui comportar riscos per a la salut i la seguretat o els drets fonamentals a què es fa referència a l'article 9, apartat 2.
- (iv) quan escaigui, les capacitats tècniques i les característiques del sistema d'IA d'alt risc per proporcionar informació rellevant per explicar-ne els resultats de sortida;
- (v) quan escaigui, el funcionament respecte a determinades persones o determinats col·lectius de persones en relació amb els quals estigui previst utilitzar el sistema,
- (vi) si és el cas, les especificacions de les dades d'entrada, o qualsevol altra informació rellevant en termes dels conjunts de dades d'entrenament, validació i prova utilitzats, tenint en compte la finalitat prevista del sistema d'IA d'alt risc;
- (vii) quan escaigui, informació que permeti als responsables del desplegament interpretar els resultats de sortida del sistema d'IA d'alt risc i fer-los servir de manera adequada;
- (c) els canvis en el sistema d'IA d'alt risc i el seu rendiment, que han estat predeterminats pel proveïdor en el moment de l'avaluació inicial de la conformitat, si n'hi ha;
- (d) les mesures de supervisió humana a què es refereix l'article 14, incloses les mesures tècniques aplicades per facilitar la interpretació dels resultats de sortida dels sistemes d'IA d'alt risc per part dels responsables del desplegament;
- (i) els recursos informàtics i de maquinari necessaris, la vida útil prevista del sistema d'IA d'alt risc i les mesures de manteniment i cura necessàries (incloent-hi la freqüència) per garantir el funcionament correcte d'aquest sistema, també pel que fa a les actualitzacions del programari;
- (f) quan sigui pertinent, una descripció dels mecanismes inclosos en el sistema d'IA d'alt risc que permeti als responsables del desplegament recollir, emmagatzemar i interpretar correctament els arxius de registre d'acord amb l'article 12.

Article 14

Supervisió humana

1. Els sistemes d'IA d'alt risc s'han de dissenyar i desenvolupar de manera que es puguin vigilar de manera efectiva per persones físiques durant el període que estiguin en ús, la qual cosa inclou dotar-los d'eines d'interfície humà-màquina adequades.

2. La supervisió humana té com a objectiu prevenir o minimitzar els riscos per a la salut, la seguretat o els drets fonamentals que puguin sorgir quan un sistema d'IA d'alt risc s'utilitza d'acord amb la finalitat que té prevista o en condicions d'ús raonablement previsible; en particular, quan aquests riscos persisteixen malgrat l'aplicació d'altres requisits establerts en aquesta secció.

3. Les mesures de supervisió han de ser proporcionals als riscos, nivell d'autonomia i context d'ús del sistema d'IA d'alt risc, i s'han d'assegurar mitjançant un o ambdós tipus de mesures:

(a) mesures identificades i construïdes, quan sigui tècnicament factible, en el sistema d'IA d'alt risc per al proveïdor abans de la introducció en el mercat o la posada en servei;

(b) mesures identificades pel proveïdor abans d'introduir en el mercat el sistema d'IA d'alt risc o de posar-lo en servei i que siguin apropiades perquè el responsable del desplegament les apliqui.

4. A l'efecte d'aplicar els paràgrafs 1, 2 i 3, el sistema d'IA d'alt risc s'ha de proporcionar al responsable del desplegament de manera que les persones físiques a qui s'encomana la supervisió humana estiguin habilitades, segons sigui apropiat i proporcionada:

(a) comprendre adequadament les capacitats i limitacions pertinents del sistema d'IA d'alt risc i ser capaç de monitorar degudament el seu funcionament, fins i tot en vista de detectar i abordar anomalies, disfuncions i prestacions inesperades;

(b) mantenir-se al corrent de la possible tendència a dependre automàticament o a dependre en excés del resultat de sortida generat per un sistema d'IA d'alt risc (biaix d'automatització), en particular per als sistemes d'IA d'alt risc utilitzats per proporcionar informació o recomanacions per a les decisions que han de prendre les persones físiques;

(c) interpretar correctament el resultat de sortida del sistema d'IA d'alt risc, tenint en compte, per exemple, les eines i mètodes d'interpretació disponibles;

(d) decidir, en qualsevol situació particular, no fer servir el sistema d'IA d'alt risc o ignorar, anul·lar o revertir el resultat de sortida del sistema d'IA d'alt risc;

(i) intervenir en el funcionament del sistema d'IA d'alt risc o interrompre el sistema a través d'un botó de "parada" o un procediment similar que permeti al sistema aturar-se en un estat segur.

5. Per als sistemes d'IA d'alt risc a què el punt 1, lletra a), de l'annex III es refereix, les mesures esmentades a l'apartat 3 d'aquest article han de ser tals que, a més, garanteixin que el

responsable del desplegament no aplica cap mesura ni pren cap decisió basant-se en la identificació que resulta del sistema, llevat que la identificació s'hagi comprovat de manera independent i l'hagin confirmada almenys dues persones físiques amb la competència, formació i autoritat necessàries.

El requisit de verificació separada per part d'almenys dues persones físiques no s'ha d'aplicar als sistemes d'IA d'alt risc utilitzats a efectes de garantia del compliment de la llei, migració, control de fronteres o asil, quan la legislació de la Unió o nacional consideri que l'aplicació d'aquest requisit és desproporcionada.

Article 15

Precisió, solidesa i ciberseguretat

1. Els sistemes d'IA d'alt risc s'han de dissenyar i desenvolupar de manera que aconseguixin un nivell adequat de precisió, solidesa i seguretat cibernètica, i que actuïn de manera consistent en aquests aspectes durant el seu cicle de vida.
2. Per abordar els aspectes tècnics de com mesurar els nivells adequats de precisió i solidesa establerts en l'apartat 1 i qualsevol altra mètrica de rendiment rellevant, la Comissió, en cooperació amb les parts interessades i organitzacions rellevants com les autoritats de metrologia i de benchmarking, ha d'encoratjar, si escau, a desenvolupar paràmetres de referència i metodologies de mesurament.
3. Els nivells de precisió i les mètriques de precisió rellevants dels sistemes d'IA d'alt risc s'han de declarar en les instruccions d'ús amb què s'acompanyen.
4. Els sistemes d'IA d'alt risc han de ser tan resistents com sigui possible davant errors, falles o inconsistències que puguin ocórrer en el sistema o l'entorn en què el sistema opera, en particular a causa de la interacció amb persones físiques o altres sistemes. En aquest sentit, s'han de prendre mesures tècniques i organitzatives.

La solidesa dels sistemes d'IA d'alt risc es pot aconseguir a través de solucions tècniques de redundància, que poden incloure plans de seguretat o fallades.

Els sistemes d'IA d'alt risc que continuïn aprenent després que s'hagin introduït en el mercat o posat en servei s'han de desenvolupar de manera que s'elimini o redueixi fins on sigui possible el risc de resultats de sortida possiblement esbiaixats que influeixin en l'entrada per a futures operacions (bucles de retroalimentació), i per assegurar que qualsevol d'aquests bucles de retroalimentació es tracta degudament amb les mesures de mitigació adequades.

5. Els sistemes d'IA d'alt risc han de ser resistents als intents de tercers no autoritzats d'alterar-ne l'ús, els resultats de sortida o el rendiment explotant vulnerabilitats del sistema.

Les solucions tècniques que tinguin com a objectiu garantir la ciberseguretat dels sistemes d'IA d'alt risc han de ser adequades a les circumstàncies i els riscos pertinents.

Les solucions tècniques per fer front a vulnerabilitats específiques d'IA han d'incloure, si escau, mesures per prevenir, detectar, respondre i prevenir, resoldre i controlar els atacs que intenten manipular el conjunt de dades d'entrenament (intoxicació de dades), o components preentrenats utilitzats en l'entrenament (intoxicació de models), entrades dissenyades per fer que el model d'IA cometi un error (exemples adversaris o evasió model), atacs de confidencialitat o defectes de model.

SECCIÓ 3

Obligacions dels proveïdors i responsables del desplegament de sistemes d'IA d'alt risc i altres parts

Article 16

Obligacions dels proveïdors de sistemes d'IA d'alt risc

Els proveïdors de sistemes d'IA d'alt risc:

(a) han d'assegurar que els seus sistemes d'IA d'alt risc compleixen els requisits establerts a la secció 2;

(b) han d'indicar, en el sistema d'IA d'alt risc o, si això no és possible, en l'embalatge o la documentació amb què s'acompanya, si escau, el nom, nom comercial registrat o marca registrada i l'adreça a efectes de contacte;

(c) disposar d'un sistema de gestió de la qualitat que compleixi amb l'article 17;

(d) conservar la documentació a què es refereix l'article 18;

(e) quan en tinguin el control, mantenir els registres generats automàticament pels seus sistemes d'IA d'alt risc, d'acord amb l'article 19;

(f) assegurar que el sistema d'IA d'alt risc se sotmet al procediment d'avaluació de la conformitat pertinent, tal com s'esmenta a l'article 43, abans que s'introdueixi en el mercat o es posi en servei;

(g) elaborar una declaració UE de conformitat segons l'article 47;

(h) adjuntar el marcatge CE al sistema d'AI d'alt risc o, si això no és possible, a l'embalatge o la documentació amb què s'acompanya, per indicar la conformitat amb el present Reglament, de conformitat amb l'article 48;

(i) complir les obligacions de registre a què es refereix l'article 49, apartat 1;

(j) adoptar les accions correctores necessàries i proporcionar informació segons els requisits de l'article 20;

(k) a petició motivada d'una autoritat nacional competent, demostrar la conformitat del sistema d'IA d'alt risc amb els requisits establerts a la secció 2;

(l) garantir que el sistema d'IA d'alt risc compleix els requisits d'accessibilitat d'acord amb les Directives (UE) 2016/2102 i (UE) 2019/882.

Article 17

Sistema de gestió de la qualitat

1. Els proveïdors de sistemes d'IA d'alt risc han d'establir un sistema de gestió de la qualitat que garanteixi el compliment del Reglament. Aquest sistema s'ha de documentar de manera sistemàtica i ordenada en forma de polítiques, procediments i instruccions escrites, i ha d'incloure almenys els aspectes següents:

(a) una estratègia per al compliment de la normativa, inclòs el compliment dels procediments d'avaluació de la conformitat i dels procediments de gestió de les modificacions dels sistemes d'IA d'alt risc;

(b) les tècniques, els procediments i les actuacions sistemàtiques que s'utilitzaran en el disseny i el control i la verificació del disseny del sistema d'IA d'alt risc;

(c) les tècniques, els procediments i les actuacions sistemàtiques que s'utilitzaran en el desenvolupament del sistema d'IA d'alt risc i en el control i l'assegurament de la qualitat d'aquest;

(d) procediments d'examen, prova i validació que s'han de dur a terme abans, durant i després del desenvolupament del sistema d'IA d'alt risc, i la freqüència amb què s'han de dur a terme.

(e) especificacions tècniques, incloses les normes, que s'han d'aplicar i, quan les normes harmonitzades pertinents no s'apliquen íntegrament o no cobreixen tots els requisits pertinents establerts a la secció 2, els mitjans que s'han de fer servir per assegurar que el sistema d'IA d'alt risc compleix aquests requisits;

(f) sistemes i procediments per a la gestió de dades, en què s'inclou adquisició, recopilació, anàlisi, etiquetatge, emmagatzematge, filtració, mineria, agregació i retenció de dades i qualsevol altra operació respecte de les dades que faci prèviament i amb la finalitat de la introducció en el mercat o la posada en servei de sistemes d'IA d'alt risc;

(g) el sistema de gestió de riscos a què es refereix l'article 9;

- (h) la creació, aplicació i el manteniment d'un sistema de seguiment postcomercialització, de conformitat amb l'article 72;
- (i) procediments relacionats amb la notificació d'un incident greu de conformitat amb l'article 73;
- (j) el tractament de la comunicació amb les autoritats nacionals competents, altres autoritats competents, incloses les que proporcionen l'accés a les dades o hi contribueixen, organismes notificats, altres operadors, clients o altres parts interessades;
- (k) sistemes i procediments per al registre de tota la documentació i informació pertinents;
- (l) gestió de recursos, incloses les mesures de seguretat de subministrament;
- (m) un marc de rendició de comptes que estableixi les responsabilitats de la direcció i de la resta de personal respecte de tots els aspectes enumerats en aquest apartat.

2. L'aplicació dels aspectes a què es refereix l'apartat 1 ha de ser proporcional a la mida de l'organització del proveïdor. Els proveïdors han de respectar, en tot cas, el grau de rigor i el nivell de protecció necessari per garantir el compliment dels seus sistemes d'IA d'alt risc amb el Reglament.

3. Els proveïdors de sistemes d'IA d'alt risc que estiguin subjectes a obligacions en relació amb els sistemes de gestió de la qualitat o una funció equivalent en virtut de la legislació sectorial pertinent de la Unió poden incloure els aspectes enumerats en l'apartat 1 com a part dels sistemes de gestió de la qualitat d'acord amb aquesta llei.

4. Per als proveïdors que siguin entitats financeres subjectes a requisits relatius a governança interna, mecanismes o processos en virtut del dret dels serveis financers de la Unió, l'obligació de posar en marxa un sistema de gestió de la qualitat, a excepció de l'apartat 1, lletres g), h) i i), d'aquest article, s'ha de considerar satisfeta si es compleixen les regles sobre els sistemes o processos de governança interna de conformitat amb la legislació de serveis financers de la Unió. A aquest efecte, s'han de tenir en compte les normes harmonitzades a què es refereix l'article 40.

Article 18

Conservació de la documentació

1. Durant un període de deu anys a comptar des de la introducció en el mercat o la posada en servei del sistema d'IA d'alt risc, el proveïdor ha de mantenir a disposició de les autoritats nacionals competents:

- (a) la documentació tècnica a què l'article 11 es refereix;

(b) la documentació relativa al sistema de gestió de la qualitat a què l'article 17 es refereix;

(c) la documentació relativa als canvis aprovats pels organismes notificats, si escau;

(d) les decisions i altres documents emesos pels organismes notificats, si escau;

(e) la declaració UE de conformitat a què l'article 47 es refereix.

2. Cada estat membre ha de determinar les condicions en què la documentació a què l'apartat 1 es refereix queda a disposició de les autoritats nacionals competents durant el període indicat en aquest apartat per als casos en què un proveïdor o el seu representant autoritzat establert en el seu territori s'arruïni o cessi l'activitat amb anterioritat al final d'aquest període.

3. Els proveïdors que siguin entitats financeres subjectes a requisits relatius a la seva governança, els seus sistemes o els seus processos interns en virtut del dret de la Unió en matèria de serveis financers han de mantenir la documentació tècnica com a part de la documentació conservada en virtut del dret pertinent de la Unió en matèria de serveis financers.

Article 19

Arxius de registre generats automàticament

1. Els proveïdors de sistemes d'IA d'alt risc han de conservar els arxius de registre a què es refereix l'article 12, apartat 1, que els sistemes d'IA d'alt risc generin automàticament en la mesura que aquests arxius estiguin sota el seu control. Sens perjudici del dret aplicable de la Unió o nacional, els arxius de registre s'han de conservar durant un període de temps adequat per a la finalitat prevista del sistema d'IA d'alt risc, d'almenys sis mesos, llevat que el dret de la Unió o nacional aplicable, en particular el dret de la Unió en matèria de protecció de dades personals, disposi una altra cosa.

2. Els proveïdors que siguin entitats financeres subjectes a requisits relatius a la seva governança interna, els seus sistemes o els seus processos en virtut del dret dels serveis financers de la Unió han de mantenir els registres generats automàticament pels seus sistemes d'IA d'alt risc com a part de la documentació que es mantingui en virtut de la legislació de serveis financers pertinent.

Article 20

Mesures correctores i obligació d'informació

1. Els proveïdors de sistemes d'IA d'alt risc que considerin que un sistema d'IA d'alt risc que han introduït en el mercat o que han posat en servei no és conforme amb el Reglament, o tinguin motius per considerar-ho, han de prendre immediatament les accions correctores necessàries perquè sigui conforme, per retirar-lo, deshabilitar-lo o recuperar-lo, segons correspongui. N'han d'informar els distribuïdors del sistema d'IA d'alt risc en qüestió i, si escau, els responsables del desplegament, el representant autoritzat i els importadors.

2. Quan el sistema d'IA d'alt risc presenti un risc en el sentit de l'article 79, apartat 1, i en tingui coneixement, en col·laboració amb el responsable del desplegament notificador, si és el cas, el

proveïdor ha d'investigar immediatament les causes i informar les autoritats de vigilància del mercat competents per al sistema d'IA d'alt risc en qüestió i, si escau, l'organisme notificat que va emetre un certificat d'aquest sistema d'IA d'alt risc d'acord amb l'article 44, en particular, de la naturalesa de l'incompliment i de qualsevol mesura correctora pertinent adoptada.

Article 21

cooperació amb les autoritats competents

1. Els proveïdors de sistemes d'IA d'alt risc, prèvia sol·licitud motivada per una autoritat competent, han de proporcionar a aquesta autoritat tota la informació i documentació necessària per demostrar la conformitat del sistema d'IA d'alt risc amb els requisits establerts a la secció 2, en una llengua fàcilment comprensible per a l'autoritat i que sigui una de les llengües oficials de les institucions de la Unió, tal com ho indiqui l'estat membre de què es tracti.
2. Prèvia sol·licitud motivada d'una autoritat competent, els proveïdors també han de donar accés a l'autoritat competent que ho sol·liciti als registres generats automàticament del sistema d'IA d'alt risc a què es refereix l'article 12, apartat 1, en la mesura que en tinguin el control.
3. Tota la informació obtinguda per una autoritat competent de conformitat amb aquest article s'ha de tractar d'acord amb les obligacions de confidencialitat establertes en l'article 78.

Article 22

Representants autoritzats dels proveïdors de sistemes d'IA d'alt risc

1. Abans de comercialitzar els seus sistemes d'IA d'alt risc en el mercat de la Unió, els proveïdors establerts en tercers països, per mandat escrit, han de designar un representant autoritzat establert a la Unió.
2. El proveïdor ha de permetre que el seu representant autoritzat faci les funcions que s'especifiquen en el mandat rebut del proveïdor.
3. El representant autoritzat ha de dur a terme les funcions que s'especifiquen en el mandat que ha rebut del proveïdor. Si les autoritats de vigilància del mercat ho sol·liciten, se'ls ha de proporcionar una còpia del mandat, en una de les llengües oficials de les institucions de la Unió, segons les indicacions de l'autoritat competent. A l'efecte del Reglament, el mandat faculta el representant autoritzat per dur a terme les funcions següents:
 - (a) verificar que la declaració UE de conformitat a què l'article 47 es refereix i la documentació tècnica a què l'article 11 es refereix s'han elaborat, i que el proveïdor ha dut a terme un procediment d'avaluació de la conformitat adequat;
 - (b) conservar a disposició de les autoritats competents i de les autoritats o organismes nacionals a què es refereix l'article 74, apartat 10, durant un període de deu anys a comptar des de la introducció en el mercat o la posada en servei del sistema d'IA d'alt risc, les dades de contacte del proveïdor que hagi nomenat el representant autoritzat, una còpia de la declaració UE de conformitat a què l'article 47 es refereix, la documentació tècnica i, si s'escau, el certificat expedit per l'organisme notificat;

(c)prèvia sol·licitud motivada, proporcionar a una autoritat competent tota la informació i documentació, inclosa la referida en la lletra b) d'aquest apartat, necessària per demostrar la conformitat d'un sistema d'IA d'alt risc amb els requisits establerts en la secció 2, incloent-hi l'accés als registres, tal com es refereix a l'article 12, apartat 1, generat automàticament pel sistema d'IA d'alt risc, en la mesura que aquests registres estiguin sota el control del proveïdor;

(d)prèvia sol·licitud motivada, cooperar amb les autoritats competents en qualsevol acció que aquestes emprenguin en relació amb el sistema d'IA d'alt risc, en particular per reduir i mitigar els riscos que el sistema d'IA d'alt risc comporta;

(e)si escau, complir les obligacions de registre esmentades a l'article 49, apartat 1, o, si és el proveïdor mateix qui porta el registre, garantir que la informació a què l'annex VIII, secció A, punt 3, es refereix, sigui correcta.

En virtut del mandat, s'habilita el representant autoritzat perquè les autoritats competents s'hi posin en contacte, a més d'amb ell o en comptes d'amb ell, en relació amb totes les qüestions que tinguin a veure amb la garantia del compliment del Reglament.

4. El representant autoritzat ha de posar fi al mandat si considera o té motius per considerar que el proveïdor actua contravenint les obligacions que li corresponen segons el Reglament. Si és el cas, n'ha d'informar immediatament l'autoritat de vigilància del mercat pertinent i, si escau, també n'ha d'informar l'organisme notificat corresponent. També ha d'informar dels motius de la rescissió.

Article 23

obligacions dels importadors

1. Abans d'introduir en el mercat un sistema d'IA d'alt risc, els importadors s'han d'assegurar que el sistema sigui conforme amb el Reglament comprovant que:

(a)el proveïdor del sistema d'IA d'alt risc hagi dut a terme el procediment d'avaluació de la conformitat pertinent a què l'article 43 es refereix;

(b)el proveïdor hagi elaborat la documentació tècnica d'acord amb l'article 11 i l'annex IV.

(c)el sistema porti el marcatge CE requerit i s'acompanyi amb la declaració UE de conformitat esmentada a l'article 47 i de les instruccions d'ús;

(d)el proveïdor hagi designat un representant autoritzat d'acord amb l'article 22, apartat 1.

2. Si té prou motius per considerar que un sistema d'IA d'alt risc no és conforme amb el Reglament, s'ha falsificat o s'ha acompanyat amb documentació falsificada, l'importador no l'ha d'introduir en el mercat fins que s'hagi assolit la conformitat del sistema. Si el sistema d'IA d'alt risc presenta un risc en el sentit de l'article 79, apartat 1, l'importador n'ha d'informar el proveïdor del sistema, el representant autoritzat i les autoritats de vigilància del mercat.

3. En l'embalatge del sistema d'IA d'alt risc o en la documentació d'acompanyament, els importadors han d'indicar el seu nom, el nom comercial registrat o la marca registrada i la seva adreça de contacte.
4. Mentre siguin responsables d'un sistema d'IA d'alt risc, els importadors han de vetllar perquè les condicions d'emmagatzematge o transport, si és el cas, no comprometin el compliment, per part del sistema mateix, dels requisits que s'estableixen en la secció 2.
5. Durant un període de deu anys després que el sistema d'IA d'alt risc s'hagi introduït en el mercat o posat en servei, els importadors han de conservar una còpia del certificat expedit per l'organisme notificat, si hi és, de les instruccions d'ús i de la declaració UE de conformitat esmentada a l'article 47.
6. Prèvia sol·licitud motivada, els importadors han de facilitar a les autoritats competents pertinents la informació i la documentació, incloses les esmentades a l'apartat 5, que calguin per demostrar que un sistema d'IA d'alt risc és conforme amb els requisits establerts a la secció 2; en una llengua que les autoritats esmentades puguin entendre fàcilment. A aquest efecte, també han de garantir que la documentació tècnica els pugui ser posada a disposició.
7. Els importadors han de cooperar amb les autoritats competents en qualsevol mesura que les autoritats prenguin en relació amb un sistema d'IA d'alt risc introduït en el mercat pels importadors; en particular, per reduir i mitigar els riscos que comporta.

Article 24

obligacions dels distribuïdors

1. Abans d'introduir-lo en el mercat, els distribuïdors han de comprovar que el sistema d'IA d'alt risc porta el marcatge CE exigint, que s'acompanya amb una declaració de la conformitat de la UE esmentada a l'article 47 i amb les instruccions d'ús, i que el proveïdor i l'importador del sistema, segons correspongui, han complert les obligacions respectives que els corresponen segons l'article 16, lletres b) i c) i l'article 23, apartat 3.
2. Si, basant-se en la informació de què disposa, considera o té raons per considerar que un sistema d'IA d'alt risc no és conforme amb els requisits de la secció 2, el distribuïdor no el pot introduir en el mercat fins que n'hagi assolit la conformitat. A més, si el sistema d'IA d'alt risc presenta un risc en el sentit de l'article 79, apartat 1, el distribuïdor n'ha d'informar el proveïdor o l'importador, segons correspongui.
3. Els distribuïdors han de garantir que, mentre un sistema d'IA d'alt risc estigui sota la seva responsabilitat, les condicions d'emmagatzematge o transport, si escau, no posin en perill el compliment del sistema amb els requisits establerts a la secció 2.
4. El distribuïdor que, basant-se en la informació de què disposa, consideri, o tingui motius per considerar, que un sistema d'IA d'alt risc que ha comercialitzat no és conforme amb els requisits establerts a la secció 2 ha d'adoptar les mesures correctores necessàries perquè hi sigui conforme, per retirar-lo del mercat o recuperar-lo, o vetllar perquè el proveïdor, l'importador o un altre operador pertinent, segons escaigui, les adopti. Quan el sistema d'IA d'alt risc presenti un risc en el sentit de l'article 79, apartat 1, el distribuïdor n'ha d'informar immediatament el proveïdor o importador del sistema i les autoritats competents per al sistema d'IA d'alt risc en qüestió, donant detalls, en particular, de l'incompliment i de qualsevol acció correctora presa.

5. A petició motivada d'una autoritat competent pertinent, els distribuïdors d'un sistema d'IA d'alt risc han de proporcionar a aquesta autoritat tota la informació i documentació referent a les seves accions d'acord amb els paràgrafs 1 a 4 necessaris per demostrar la conformitat d'aquest sistema amb els requisits establerts a l'apartat 2.

6. Els distribuïdors han de cooperar amb les autoritats competents en qualsevol mesura que les autoritats adoptin en relació amb un sistema d'IA d'alt risc comercialitzat pels distribuïdors; en particular, per reduir o mitigar el risc que comporta.

Article 25

Responsabilitats al llarg de la cadena de valor de la IA

1. Qualsevol distribuïdor, importador, responsable del desplegament o tercer es considera proveïdor d'un sistema d'IA d'alt risc als efectes del Reglament i està subjecte a les obligacions del proveïdor en virtut de l'article 16, en qualsevol de les circumstàncies següents:

(a) quan faci constar el seu nom o marca en un sistema d'IA d'alt risc ja introduït en el mercat o posat en servei, sense perjudici dels acords contractuals que estableixin que les obligacions s'assignen d'una altra manera;

(b) quan modifiqui de manera significativa un sistema d'IA d'alt risc que ja hagi introduït en el mercat o posat en servei, de manera que continuï sent un sistema d'IA d'alt risc d'acord amb l'article 6;

(c) quan modifiqui la finalitat prevista del sistema d'IA, inclòs un sistema d'IA d'ús general, que no s'hagi considerat d'alt risc i que ja s'hagi introduït en el mercat o posat en servei, de manera que el sistema d'IA en qüestió esdevingui un sistema d'IA d'alt risc d'acord amb l'article 6.

2. En donar-se les circumstàncies esmentades a l'apartat 1 el proveïdor que inicialment hagi introduït el sistema d'IA en el mercat o l'hagi posat en servei ja no es considera proveïdor del sistema d'IA en particular als efectes del Reglament. Ha de cooperar estretament amb els nous proveïdors i facilitar, segons siguin necessaris, la informació, l'accés tècnic o altra assistència que raonablement s'hagin previst i considerat necessaris per al compliment de les obligacions establertes en el present Reglament; en particular, pel que fa al compliment de l'avaluació de la conformitat dels sistemes d'IA d'alt risc. Aquest apartat no s'aplica en els casos en què el proveïdor inicial hagi especificat clarament que el seu sistema d'IA no s'ha de transformar en un sistema d'IA d'alt risc i, per tant, no està obligat a lliurar la documentació.

3. En el cas de sistemes d'IA d'alt risc que siguin components de seguretat dels productes coberts per la legislació d'harmonització de la Unió enumerada a l'annex I, secció A, el fabricant del producte es considera proveïdor del sistema d'IA d'alt risc i està subjecte a les obligacions establertes a l'article 16 en qualsevol de les circumstàncies següents:

(a) quan el sistema d'IA d'alt risc s'hagi introduït en el mercat amb el producte que porta el nom o la marca comercial del fabricant del producte;

(b) quan el sistema d'IA d'alt risc s'hagi posat en servei amb el nom o la marca del fabricant del producte després que el producte s'hagi introduït en el mercat.

4. El proveïdor d'un sistema d'IA d'alt risc i el tercer que subministri un sistema d'IA d'alt risc, eines, serveis, components o processos que s'utilitzin o s'integrin en un sistema d'IA d'alt risc han d'especificar, mitjançant acord escrit, la informació, les capacitats, l'accés tècnic i altra assistència que siguin necessaris, segons l'estat de la tècnica generalment reconegut, perquè el proveïdor del sistema d'IA d'alt risc pugui complir plenament les obligacions que el Reglament preveu. Aquest apartat no és aplicable a tercers que posin a disposició del públic eines, serveis, processos o components que no siguin models d'IA d'ús general, en el marc d'una llicència lliure i de codi obert.

L'Oficina d'IA pot elaborar i recomanar clàusules contractuals tipus, de caràcter voluntari, entre els proveïdors de sistemes d'IA d'alt risc i tercers que subministrin eines, serveis, components o processos que es fan servir per a sistemes d'IA d'alt risc o s'hi integren. En l'elaboració de les clàusules contractuals tipus de caràcter voluntari, l'Oficina d'IA ha de tenir en compte els possibles requisits contractuals aplicables en sectors o models de negoci específics. Les clàusules contractuals tipus voluntàries s'han de publicar i estar disponibles sense càrrec en un format electrònic fàcilment utilitzable.

5. Els apartats 2 i 3 s'han d'entendre sense perjudici de la necessitat d'observar i protegir els drets de propietat intel·lectual i industrial, la informació comercial confidencial i els secrets comercials, de conformitat amb el dret de la unió i el dret nacional.

Article 26

Obligacions dels responsables del desplegament de sistemes d'IA d'alt risc

1. Els responsables del desplegament de sistemes d'IA d'alt risc han de prendre les mesures tècniques i organitzatives apropiades per assegurar-se que utilitzen aquests sistemes d'acord amb les instruccions d'ús amb què s'acompanyen els sistemes, d'acord amb els apartats 3 i 6.

2. Els responsables del desplegament han d'encomanar la supervisió humana a les persones físiques que tinguin la competència, la formació i l'autoritat necessàries.

3. Les obligacions establertes en els apartats 1 i 2, s'han d'entendre sense perjudici d'altres obligacions del responsable del desplegament en virtut del dret de la Unió o del país i de la llibertat del responsable del desplegament d'organitzar els recursos i activitats propis amb la finalitat d'aplicar les mesures de supervisió humana indicades pel proveïdor.

4. Sense perjudici dels apartats 1 i 2, en la mesura que el responsable del desplegament exerceixi el control sobre les dades d'entrada, el responsable del desplegament ha d'assegurar que les dades d'entrada siguin rellevants i prou representatives a la vista de la finalitat prevista del sistema d'IA d'alt risc.

5. Els responsables del desplegament han de supervisar el funcionament del sistema d'IA d'alt risc partint de les instruccions d'ús i, si escau, informar els proveïdors d'acord amb l'article 72. Quan tinguin raons per considerar que l'ús del sistema d'IA d'alt risc d'acord amb les instruccions pot comportar que el sistema d'IA presenti un risc en el sentit de l'article 79, apartat 1, els responsables del desplegament n'han d'informar sense dilació indeguda el proveïdor o distribuïdor i l'autoritat de vigilància del mercat pertinent, i suspendre'n l'ús. Quan hagin identificat un incident greu, els responsables del desplegament també n'han d'informar

immediatament primer el proveïdor i després l'importador o distribuïdor i les autoritats de vigilància del mercat pertinents. Si el responsable del desplegament no pot arribar al proveïdor, l'article 73 s'aplica mutatis mutandis. Aquesta obligació no cobreix les dades operatives sensibles dels responsables del desplegament de sistemes d'IA que són autoritats garants del compliment de la llei.

Per als responsables del desplegament que siguin entitats financeres subjectes a requisits relatius a la governança interna pròpia i als seus sistemes o processos en virtut del dret dels serveis financers de la Unió, s'ha de considerar que l'obligació de seguiment establerta en el primer apartat es compleix si es compleixen les normes sobre els sistemes de governança interna, procediments i mecanismes de conformitat amb la legislació de serveis financers pertinent.

6. Els responsables del desplegament de sistemes d'IA d'alt risc han de mantenir els registres generats automàticament per aquest sistema d'IA d'alt risc en la mesura que aquests registres estiguin sota el seu control, durant un període apropiat al propòsit previst del sistema d'IA d'alt risc, d'almenys sis mesos, llevat que es disposi el contrari en el dret de la Unió o en el dret nacional aplicable, en particular en el dret de la Unió sobre la protecció de dades personals.

Els responsables del desplegament que siguin entitats financeres subjectes a requisits relatius a la seva governança interna, els seus mecanismes o els seus processos en virtut del dret dels serveis financers de la Unió han de mantenir els registres com a part de la documentació que es conserva d'acord amb la legislació pertinent del servei financer de la Unió.

7. Abans de posar en servei o fer servir un sistema d'IA d'alt risc en el lloc de treball, els responsables del desplegament que siguin ocupadors han d'informar els representants dels treballadors i els treballadors afectats que estaran subjectes a l'ús del sistema d'IA d'alt risc. Quan calgui, aquesta informació s'ha de facilitar de conformitat amb les normes i procediments establerts en el dret de la Unió i en la pràctica nacional sobre la informació dels treballadors i els seus representants.

8. Els responsables del desplegament de sistemes d'IA d'alt risc que siguin autoritats públiques o institucions, organismes, oficines o organismes de la Unió han de complir les obligacions de registre a què l'article 49 es refereix. Quan trobin que el sistema d'IA d'alt risc que preveuen fer servir no ha estat registrat a la base de dades de la UE a què es refereix l'article 71, aquests responsables del desplegament no han de fer servir aquest sistema i n'han d'informar el proveïdor o el distribuïdor.

9. Quan escaigui, els responsables del desplegament de sistemes d'IA d'alt risc han de fer servir la informació proporcionada en virtut de l'article 13 del Reglament per complir l'obligació de dur a terme una avaluació d'impacte de protecció de dades segons l'article 35 del Reglament (UE) 2016/679 o l'article 27 de la Directiva (UE) 2016/680.

10. Sense perjudici de la Directiva (UE) 2016/680, en el marc d'una investigació per a la recerca dirigida d'una persona sospitosa o condemnada per haver comès un delictes, el responsable del desplegament d'un sistema d'IA d'alt risc per a la identificació biomètrica remota en diferit ha de demanar una autorització, ex ante, o sense demora indeguda i sense que hagin passat més de 48 hores, per una autoritat judicial o una autoritat administrativa amb decisió vinculant i subjecta a revisió judicial, per a l'ús d'aquest sistema, excepte quan s'utilitzi per a la identificació inicial d'un sospitós potencial basada en fets objectius i verificables directament vinculats a la infracció. Cada ús s'ha de limitar al que sigui estrictament necessari per a la investigació d'un delictes específic.

Si es rebutja l'autorització sol·licitada d'acord amb l'apartat anterior, l'ús del sistema d'identificació biomètrica remota en diferit vinculat a aquesta autorització sol·licitada s'ha d'aturar amb efecte immediat i s'han d'eliminar les dades personals vinculades a l'ús del sistema d'IA d'alt risc per al qual es va sol·licitar l'autorització.

En cap cas s'ha de fer servir un sistema d'IA d'alt risc per a la identificació biomètrica remota en diferit amb finalitats d'aplicació de la llei de manera no específica, sense cap vincle amb un delictes, un procediment penal, una amenaça real, present o real i previsible d'un delictes, o la recerca d'una persona desapareguda específica. S'ha d'assegurar que cap decisió que produeixi un efecte jurídic advers sobre una persona no pugui prendre's per les autoritats garantees del compliment de la llei partint només dels resultats de sortida d'aquests sistemes d'identificació biomètrica remota en diferit.

El present apartat queda sense perjudici de l'article 9 del Reglament (UE) 2016/679 i de l'article 10 de la Directiva (UE) 2016/680 per al tractament de dades biomètriques.

Amb independència de la finalitat o del responsable del desplegament, cada ús dels sistemes d'IA s'ha de documentar en l'expedient policial corresponent i posar-se a disposició de l'autoritat de vigilància del mercat pertinent i de l'autoritat nacional de protecció de dades, si aquestes ho sol·liciten, excepte en el cas que la divulgació sigui de dades operatives sensibles relacionades amb la garantia del compliment de la llei. El present apartat s'ha d'entendre sense perjudici de les competències que confereix la Directiva (UE) 2016/680 sobre les autoritats de control.

Els responsables del desplegament han de presentar informes anuals a les autoritats nacionals de vigilància del mercat i de protecció de dades sobre l'ús de sistemes d'identificació biomètrica remota en diferit, excloent la divulgació de dades operatives sensibles relacionades amb la garantia del compliment de la llei. Els informes poden ser agregats per cobrir més d'un desplegament.

Els estats membres poden introduir, de conformitat amb el dret de la Unió, lleis més restrictives sobre l'ús de sistemes d'identificació biomètrica remota en diferit.

11. Sense perjudici del que disposa l'article 50 del Reglament, els responsables del desplegament de sistemes d'IA d'alt risc a què es refereix l'annex III i que prenen decisions o ajuden en la presa de decisions relacionades amb les persones físiques han d'informar les persones físiques que estan subjectes a l'ús del sistema d'IA d'alt risc. Per als sistemes d'IA d'alt risc utilitzats amb finalitats de garantia del compliment de la llei, s'ha d'aplicar l'article 13 de la Directiva (UE) 2016/680.

12. Els responsables del desplegament han de cooperar amb les autoritats competents pertinents en qualsevol acció que aquestes autoritats prenguin en relació amb el sistema d'IA d'alt risc per aplicar aquest Reglament.

Article 27

Avaluació de l'impacte en els drets fonamentals per als sistemes d'IA d'alt risc

1. Abans de desplegar un sistema d'IA d'alt risc a què es refereix l'article 6, apartat 2, a excepció dels sistemes d'IA d'alt risc destinats a l'ús en l'àrea enumerada en el punt 2 de l'annex III, els responsables del desplegament que són organismes regulats pel dret públic, o bé les entitats privades que presten serveis públics, i els responsables del desplegament de sistemes d'IA d'alt risc als quals es fa referència en el punt 5, lletres b) i c), de l'annex III, han d'avaluar l'impacte en

els drets fonamentals que l'ús d'aquest sistema pugui tenir. A aquest efecte, els responsables del desplegament han de fer una avaluació que consisteixi en:

(a) una descripció dels processos del responsable del desplegament en què el sistema d'IA d'alt risc s'utilitzarà d'acord amb la finalitat que té prevista;

(b) una descripció del període durant el qual s'ha de fer servir cada sistema d'IA d'alt risc i la freqüència amb què es farà servir;

(c) les categories de persones i grups naturals susceptibles de ser afectats per l'ús en el context específic;

(d) els riscos específics de dany susceptibles de tenir un impacte en les categories de persones físiques o grups de persones identificades de conformitat amb el punt c) d'aquest apartat, tenint en compte la informació facilitada pel proveïdor de conformitat amb l'article 13;

(e) una descripció de l'aplicació de mesures de supervisió humana, d'acord amb les instruccions d'ús;

(f) les mesures que s'han d'adoptar en el cas de la materialització d'aquests riscos, incloses les disposicions per a la governança interna i els mecanismes de reclamació.

2. L'obligació establerta en l'apartat 1 s'aplica al primer ús del sistema d'IA d'alt risc. En casos similars, el responsable del desplegament pot confiar en avaluacions d'impacte de drets fonamentals fetes prèviament pel proveïdor o en avaluacions d'impacte existents. Si, durant l'ús del sistema d'IA d'alt risc, considera que algun dels elements enumerats en l'apartat 1 ha canviat o no està actualitzat, el responsable del desplegament ha de prendre les mesures necessàries per actualitzar la informació.

3. Una vegada feta l'avaluació a què l'apartat 1 d'aquest article es refereix, el responsable del desplegament n'ha de notificar els resultats a l'autoritat de vigilància del mercat, presentant el model emplenat a què es refereix l'apartat 5 d'aquest article com a part de la notificació. En el cas a què es refereix l'article 46, apartat 1, els responsables del desplegament poden estar exempts de l'obligació de notificar.

4. Si ja es compleix alguna de les obligacions establertes en aquest article a través de l'avaluació d'impacte de la protecció de dades feta de conformitat amb l'article 35 del Reglament (UE) 2016/679 o l'article 27 de la Directiva (UE) 2016/680, l'avaluació d'impacte dels drets fonamentals a què es refereix l'apartat 1 d'aquest article ha de completar l'avaluació d'impacte de la protecció de dades.

5. L'Oficina d'IA ha d'elaborar un model de qüestionari, fins i tot mitjançant una eina automatitzada, per facilitar que els responsables del desplegament compleixin de manera simplificada les obligacions que els corresponen en virtut d'aquest article.

SECCIÓ 4

Notificar a les autoritats i organismes notificats

Article 28

Notificació a les autoritats

1. Cada estat membre ha de designar o establir, com a mínim, una autoritat notificadora responsable de la creació i execució dels procediments necessaris per a l'avaluació, designació i notificació dels organismes d'avaluació de la conformitat i del seu seguiment. Aquests procediments s'han de desenvolupar en cooperació entre les autoritats notificadores de tots els estats membres.
2. Els estats membres poden decidir que l'avaluació i el seguiment a què es refereix l'apartat 1 l'ha de dur a terme un organisme nacional d'acreditació en el sentit del Reglament (CE) 765/2008 i de conformitat amb aquest.
3. La notificació a les autoritats s'ha d'establir, organitzar i fer funcionar de manera que no sorgeixi cap conflicte d'interessos amb els organismes d'avaluació de la conformitat, i que l'objectivitat i la imparcialitat de les seves activitats se salvaguardin.
4. La notificació a les autoritats s'ha d'organitzar de manera que les decisions relatives a la notificació dels organismes d'avaluació de la conformitat es prenguin per persones competents diferents de les que van avaluar aquests organismes.
5. La notificació a les autoritats no pot oferir ni proporcionar cap activitat que els organismes d'avaluació de la conformitat duguin a terme, ni cap servei de consultoria de caràcter comercial o competitiu.
6. La notificació a les autoritats ha de salvaguardar la confidencialitat de la informació que obtinguin, de conformitat amb l'article 78.
7. Les autoritats notificadores tenen a disposició un nombre adequat de personal competent per al correcte exercici de les seves funcions. El personal competent ha de disposar dels coneixements necessaris, segons calgui, per a la seva funció, en camps com les tecnologies de la informació, la IA i el dret, inclosa la supervisió dels drets fonamentals.

Article 29

Aplicació d'un organisme d'avaluació de la conformitat per a la notificació

1. Els organismes d'avaluació de la conformitat han de presentar una sol·licitud de notificació a l'autoritat notificadora de l'estat membre en què s'estableixin.
2. La sol·licitud de notificació s'ha d'acompanyar amb una descripció de les activitats d'avaluació de la conformitat, del mòdul o mòduls d'avaluació de la conformitat i dels tipus de sistemes d'IA pels quals l'organisme d'avaluació de la conformitat declara ser competent, així com d'un certificat d'acreditació, quan existeixi, emès per un organisme nacional d'acreditació que acredita que l'organisme d'avaluació de la conformitat compleix els requisits establerts a l'article 31.

S'ha d'afegir qualsevol document vàlid relacionat amb les designacions existents de l'organisme notificat per l'interessat en virtut de qualsevol altra legislació d'harmonització de la Unió.

3. Quan no pugui proporcionar un certificat d'acreditació, l'organisme avaluador de la conformitat en qüestió ha de proporcionar a l'autoritat notificadora totes les proves documentals necessàries per a la verificació, el reconeixement i el seguiment regular del seu compliment dels requisits establerts a l'article 31.

4. Per als organismes notificats designats en virtut de qualsevol altra legislació d'harmonització de la Unió, tots els documents i certificats vinculats a les designacions es poden fer servir per donar suport al seu procediment de designació d'acord amb el present Reglament. L'organisme notificat ha d'actualitzar la documentació a què es refereixen els paràgrafs 2 i 3 d'aquest article sempre que es produeixin canvis rellevants, amb la finalitat que l'autoritat responsable dels organismes notificats pugui supervisar i verificar el compliment continu de tots els requisits establerts a l'article 31.

Article 30

Procediment de notificació

1. La notificació a les autoritats només pot notificar als organismes d'avaluació de la conformitat que hagin complert els requisits establerts a l'article 31.

2. Les autoritats notificadores han de notificar a la Comissió i als altres estats membres, utilitzant l'eina de notificació electrònica desenvolupada i gestionada per la Comissió, de cada organisme d'avaluació de la conformitat a què es refereix l'apartat 1.

3. La notificació a què es refereix l'apartat 2 d'aquest article ha d'incloure els detalls complets de les activitats d'avaluació de la conformitat, el mòdul o mòduls d'avaluació de la conformitat, els tipus de sistemes d'IA en qüestió, i l'acreditació pertinent de la competència. Quan una notificació no es basi en un certificat d'acreditació tal com es refereix a l'article 29, apartat 2, l'autoritat notificadora ha de proporcionar a la Comissió i als altres estats membres proves documentals que acreditin la competència de l'organisme d'avaluació de la conformitat i les disposicions vigents per garantir que aquest organisme sigui supervisat regularment i continuï satisfent els requisits establerts a l'article 31.

4. L'organisme d'avaluació de la conformitat en qüestió només pot exercir les activitats d'un organisme notificat quan la Comissió o els altres estats membres no presentin objeccions en el termini de dues setmanes des de la notificació per part d'una autoritat notificadora, quan inclogui un certificat d'acreditació a què es refereix l'article 29, apartat 2, o en el termini de dos mesos des de la notificació per part de l'autoritat notificadora, quan inclogui proves documentals a què es refereix l'article 29, apartat 3.

5. Quan es plantegin objeccions, la Comissió ha d'entrar, sense demora, en consultes amb els estats membres pertinents i amb l'organisme d'avaluació de la conformitat. En aquest sentit, la Comissió ha de decidir si l'autorització està justificada. La Comissió ha d'adreçar la seva decisió a l'estat membre interessat i a l'organisme d'avaluació de la conformitat pertinent.

Article 31

Requisits dels organismes notificats

1. Un organisme notificat s'ha d'establir en virtut del dret nacional d'un estat membre, amb personalitat jurídica.

2. Els organismes notificats han de satisfer els requisits organitzatius, de gestió de la qualitat, de recursos i de procés necessaris per complir les seves funcions, així com els requisits adequats de ciberseguretat.
3. L'estructura organitzativa, l'assignació de responsabilitats, les línies d'informació i el funcionament dels organismes notificats han de garantir la confiança en el seu acompliment i en els resultats de les activitats d'avaluació de la conformitat que els organismes notificats duen a terme.
4. Els organismes notificats han de ser independents del proveïdor d'un sistema d'IA d'alt risc en relació amb el qual facin activitats d'avaluació de la conformitat. Els organismes notificats també han de ser independents de qualsevol altre operador que tingui un interès econòmic en els sistemes d'IA d'alt risc avaluats, i també de qualsevol competidor del proveïdor. Això no exclou l'ús de sistemes d'IA avaluats d'alt risc que siguin necessaris per a les operacions de l'organisme d'avaluació de la conformitat, ni l'ús d'aquests sistemes d'IA d'alt risc per a finalitats personals.
5. L'organisme d'avaluació de la conformitat, la seva alta direcció i el personal responsable de dur-ne a terme les tasques d'avaluació de la conformitat no poden estar directament implicats en el disseny, desenvolupament, comercialització o ús de sistemes d'IA d'alt risc, i tampoc no poden representar les parts implicades en aquestes activitats. No pot participar en cap activitat que pugui contradir la seva independència de judici o integritat en relació amb les activitats d'avaluació de la conformitat per a les quals se'ls notifiqui. Això s'ha d'aplicar, en particular, als serveis de consultoria.
6. Els òrgans notificats s'han d'organitzar i fer funcionar de manera que se'n preservin la independència, l'objectivitat i la imparcialitat de les seves activitats. Els organismes notificats han de documentar i aplicar una estructura i procediments per salvaguardar la imparcialitat i promoure i aplicar els principis d'imparcialitat en el conjunt de la seva organització, personal i activitat d'avaluació.
7. Els òrgans notificats han de disposar de procediments documentats que assegurin que el seu personal, comitès, filials, subcontractistes i qualsevol cos o personal associat d'organismes externs mantinguin, d'acord amb l'article 78, la confidencialitat de la informació que entri en possessió seva durant l'exercici de les activitats d'avaluació de la conformitat excepte quan la divulgació sigui una obligació imposada per la llei. El personal dels òrgans notificats té el deure d'observar el secret professional en relació amb tota la informació que obtingui en l'exercici de les seves funcions en virtut del present Reglament, excepte en relació amb les autoritats notificadores de l'estat membre en què es duguin a terme les seves activitats.
8. Els organismes notificats han de disposar de procediments per a l'exercici de les activitats que tinguin en compte la mida d'un proveïdor, el sector en què aquest opera, la seva estructura i el grau de complexitat del sistema d'IA en qüestió.
9. Els organismes notificats han de contractar una assegurança de responsabilitat civil apropiada per a les seves activitats d'avaluació de la conformitat, llevat que l'estat membre assumeixi la responsabilitat en què s'estableixi d'acord amb el dret nacional o que el mateix estat membre sigui directament responsable de l'avaluació de la conformitat.
10. Els òrgans notificats han de poder dur a terme totes les seves funcions en virtut del present Reglament amb el màxim grau d'integritat professional i la competència requerida en l'àmbit

específic, tant si aquestes funcions són dutes a terme pels organismes notificats mateixos com si es duen en nom seu i sota responsabilitat seva.

11. Els organismes notificats han de tenir les competències internes suficients per poder avaluar eficaçment les funcions fetes per les parts externes en nom seu. L'organisme notificat ha de disposar de personal administratiu, tècnic, jurídic i científic suficient que tingui experiència i coneixement en relació amb els tipus de sistemes d'IA pertinents, dades i informàtica de dades, i en relació amb els requisits establerts a la secció 2.

12. Els organismes notificats han de participar en les activitats de coordinació a què es refereix l'article 38. Així mateix, han de prendre part, directament o per representació, en organitzacions europees de normalització, o s'asseguraran de mantenir-se al corrent de la situació actualitzada de les normes pertinents.

Article 32

Presumpció de conformitat amb els requisits relatius als organismes notificats

Quan un organisme d'avaluació de la conformitat demostrï que compleix els criteris establerts en les normes harmonitzades pertinents, o en parts d'aquestes, les referències de les quals siguin publicades en el Diari Oficial de la Unió Europea, es presumirà que compleix els requisits establerts a l'article 31 en la mesura que les normes harmonitzades aplicables contemplin aquests mateixos requisits.

Article 33

Filials d'organismes notificats i subcontractació

1. Quan subcontracti tasques específiques relacionades amb l'avaluació de la conformitat o recorri a una filial, l'organisme notificat s'ha d'assegurar que el subcontractista o la filial compleixin els requisits establerts en l'article 31, i ha d'informar l'autoritat notificadora en conseqüència.

2. Els organismes notificats són plenament responsables de les tasques fetes per qualsevol subcontractista o filial.

3. Les activitats només poden subcontractar-se o delegar-se en una filial previ consentiment del proveïdor. Els organismes notificats han de posar a disposició del públic una llista de les seves filials.

4. Els documents pertinents relatius a l'avaluació de les qualificacions del subcontractista o de la filial i el treball que duguin a terme en virtut del present Reglament s'han de mantenir a disposició de l'autoritat notificadora durant període de cinc anys a partir de la data de finalització de la subcontractació.

Article 34

Obligacions operatives dels organismes notificats

1. Els organismes notificats han de verificar la conformitat dels sistemes d'IA d'alt risc segons els procediments d'avaluació de la conformitat establerts a l'article 43.

2. Els organismes notificats han d'estalviar càrregues innecessàries als proveïdors en el desenvolupament de les seves activitats, tenint-ne en compte les dimensions, el sector en què opera, l'estructura i el grau de complexitat del sistema d'IA d'alt risc en qüestió, en particular per

minimitzar les càrregues administratives i els costos de compliment per a les empreses micro i petites en el sentit de la recomanació 2003/361/CE. L'organisme notificat ha de respectar, no obstant això, el grau de rigor i el nivell de protecció necessari per al compliment del sistema d'IA d'alt risc amb els requisits del Reglament.

3. Els organismes notificats han de posar a disposició de l'autoritat notificadora esmentada a l'article 28, i presentar-li si ho demana, tota la documentació pertinent, inclosa la documentació dels proveïdors, per tal que aquesta autoritat pugui dur a terme les activitats d'avaluació, designació, notificació i supervisió, i de facilitar l'avaluació descrita en aquesta secció.

Article 35

Números d'identificació i llistes d'organismes notificats

1. La Comissió ha d'assignar un número d'identificació únic a cada organisme notificat, fins i tot quan un organisme sigui notificat en virtut de més d'un acte de la Unió.

2. La Comissió ha de posar a disposició del públic la llista dels organismes notificats en virtut del Reglament, inclosos els seus números d'identificació i les activitats per a les quals han estat notificats. La Comissió ha de vetllar perquè la llista estigui actualitzada.

Article 36

Canvis en les notificacions

1. L'autoritat notificadora ha de notificar a la Comissió i als altres estats membres qualsevol canvi rellevant en la notificació d'un organisme notificat a través de l'eina de notificació electrònica a què es refereix l'article 30, apartat 2.

2. Els procediments establerts als articles 29 i 30 s'han d'aplicar a les ampliacions de l'abast de la notificació.

Per a canvis en la notificació que no siguin ampliacions de l'àmbit d'aplicació, s'han d'aplicar els procediments establerts en els apartats 3 a 9.

3. Quan un organisme notificat decideixi cessar les activitats d'avaluació de la conformitat, n'ha d'informar l'autoritat notificadora i els proveïdors interessats al més aviat possible i, en cas de cessament previst, almenys un any abans de cessar. Els certificats de l'organisme notificat poden mantenir-se vàlids durant un període de nou mesos després del cessament de les activitats de l'organisme notificat, sempre que un altre organisme notificat hagi confirmat per escrit que assumeix responsabilitats sobre els sistemes d'IA d'alt risc coberts per aquests certificats. Aquest últim organisme notificat ha de completar una avaluació total dels sistemes d'IA d'alt risc afectats al final d'aquest període de nou mesos abans d'emetre nous certificats per a aquests sistemes. Quan l'organisme notificat hagi cessat l'activitat, l'autoritat notificadora ha de revocar la designació.

4. Quan una autoritat notificadora tingui raons suficients per considerar que un organisme notificat ja no compleix els requisits establerts a l'article 31, o no compleix les seves obligacions, l'autoritat notificadora ha d'investigar al més aviat possible i amb diligència màxima. En aquest context, ha d'informar l'organisme notificat interessat sobre les objeccions plantejades i donar-li la possibilitat de comunicar què n'opina. Si arriba a la conclusió que l'organisme notificat ja no compleix els requisits establerts a l'article 31 o que no compleix les seves obligacions, l'autoritat notificadora ha de restringir, suspendre o retirar la designació segons correspongui, en funció de

la gravetat de la incapacitat per complir aquests requisits o aquestes obligacions. Ha d'informar la Comissió i els altres estats membres en conseqüència immediatament.

5. Quan la designació hagi estat suspesa, restringida o retirada totalment o parcialment, l'organisme notificat ho ha de comunicar als proveïdors interessats en el termini de deu dies.

6. En cas de restricció, suspensió o retirada d'una designació, l'autoritat notificadora ha de prendre les mesures adequades per assegurar que es guarden els expedients de l'organisme notificat interessat i posar-los a disposició de les autoritats notificadores en altres estats membres i de les autoritats de vigilància del mercat si aquestes ho sol·liciten.

7. En cas de restricció, suspensió o retirada d'una designació, l'autoritat notificadora ha de:

(a) avaluar l'impacte en els certificats emesos per l'organisme notificat;

(b) Presentar un informe sobre les seves conclusions a la Comissió i als altres estats membres en el termini de tres mesos des que es va notificar la modificació de la designació.

(c) exigir a l'organisme notificat que, en un termini raonable determinat per l'autoritat, suspengui o retiri els certificats que s'hagin emès indegudament, per garantir la conformitat contínua dels sistemes d'IA d'alt risc en el mercat;

(d) Informar la Comissió i els estats membres sobre els certificats per als quals ha requerit la suspensió o la retirada;

(e) proporcionar a les autoritats nacionals competents de l'estat membre en què el proveïdor tingui el domicili social tota la informació pertinent sobre els certificats dels quals ha requerit la suspensió o retirada; aquesta autoritat ha de prendre les mesures apropiades per evitar un risc potencial per a la salut, la seguretat o els drets fonamentals.

8. A excepció dels certificats emesos indegudament, i quan una designació hagi estat suspesa o restringida, els certificats romandran vàlids si es dona una de les circumstàncies següents:

(a) L'autoritat notificadora ha confirmat, en el termini d'un mes des de la suspensió o restricció, que no hi ha risc per a la salut, la seguretat o els drets fonamentals en relació amb els certificats afectats per la suspensió o restricció, i l'autoritat notificadora ha establert un termini per a les accions per posar remei a la suspensió o restricció.

(b) L'autoritat notificadora ha confirmat que no s'emetraran, modificaran o reemetran certificats rellevants per a la suspensió o restricció, i estableix si l'organisme notificat té la capacitat de continuar supervisant i sent responsable dels certificats existents emesos durant el període de suspensió o restricció. En el cas que l'autoritat notificadora determini que l'organisme notificat no té la capacitat de donar suport als certificats emesos, el proveïdor del sistema cobert pel certificat ha de confirmar per escrit a les autoritats nacionals competents de l'estat membre en què tingui el domicili social, en el termini de tres mesos des de la suspensió o

restricció, que un altre organisme notificat qualificat assumeix temporalment les funcions de l'organisme notificat per supervisar i ser responsable dels certificats durant el període de suspensió o restricció.

9. A excepció dels certificats emesos indegudament, i quan s'hagi retirat una designació, els certificats han de romandre vàlids durant un període de nou mesos en les circumstàncies següents:

(a) L'autoritat nacional competent de l'estat membre en què el proveïdor del sistema d'IA d'alt risc cobert pel certificat té el domicili social de negocis ha confirmat que no hi ha risc per a la salut, la seguretat o els drets fonamentals associats als sistemes d'IA d'alt risc en qüestió.

(b) Un altre organisme notificat ha confirmat per escrit que assumeix immediatament la responsabilitat d'aquests sistemes d'IA i completa l'avaluació en el termini de dotze mesos des de la retirada de la designació.

En les circumstàncies a què es refereix el paràgraf primer, l'autoritat nacional competent de l'estat membre en què el proveïdor del sistema cobert pel certificat tingui el lloc de treball pot prorrogar la validesa provisional dels certificats durant períodes addicionals de tres mesos, sense superar els dotze mesos en total.

L'autoritat nacional competent o l'organisme notificat que assumeixi les funcions de l'organisme notificat afectat pel canvi de denominació, ho ha de comunicar immediatament a la Comissió, als altres estats membres i als altres organismes notificats.

Article 37

Impugnació de la competència dels organismes notificats

1. La Comissió ha d'investigar tots els casos en què hi hagi motius per dubtar de la competència d'un organisme notificat o del compliment continuat per un organisme notificat dels requisits establerts a l'article 31 i de les seves responsabilitats aplicables.

2. L'autoritat notificadora ha de proporcionar a la Comissió, a petició, tota la informació pertinent relativa a la notificació o al manteniment de la competència de l'organisme notificat interessat.

3. La Comissió ha de vetllar perquè tota la informació crítica obtinguda en el curs de les seves investigacions, de conformitat amb aquest article, rebi un tracte de confidencialitat d'acord amb l'article 78.

4. Quan la Comissió determini que un organisme notificat no compleix o ja no compleix els requisits per a la seva notificació, ha d'informar l'estat membre notificador en conseqüència i sol·licitar-li que adopti les mesures correctores necessàries, inclosa la suspensió o retirada de la notificació si és necessari. Quan l'estat membre no adopti les mesures correctores necessàries, la Comissió pot, mitjançant un acte d'execució, suspendre, restringir o retirar la designació. Aquest acte d'execució s'ha d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

Article 38

Coordinació dels organismes notificats

1. La Comissió ha de vetllar perquè, pel que fa als sistemes d'IA d'alt risc, es posin en marxa una coordinació i cooperació adequades entre els organismes notificats actius en els procediments d'avaluació de la conformitat d'acord amb el present Reglament i s'operi adequadament en forma d'un grup sectorial d'organismes notificats.
2. Cada autoritat notificadora ha de vetllar perquè els organismes notificats participin en el treball d'un grup a què es refereix l'apartat 1, directament o a través de representants designats.
3. La Comissió ha de facilitar l'intercanvi de coneixements i bones pràctiques entre les autoritats notificadores.

Article 39

Organismes d'avaluació de la conformitat de tercers països

Els organismes d'avaluació de la conformitat establerts en virtut de la llei d'un tercer país amb el qual la Unió ha conclòs un acord poden estar autoritzats a dur a terme les activitats dels organismes notificats en virtut del present Reglament, sempre que compleixin els requisits establerts en l'article 31 o garanteixin un nivell equivalent de compliment.

SECCIÓ 5

Normes, avaluació de la conformitat, certificats, registre

Article 40

Normes harmonitzades i entregables d'estandardització

1. Els sistemes d'IA d'alt risc o els models d'IA d'ús general que siguin conformes amb les normes harmonitzades o parts d'aquestes, les referències dels quals hagin estat publicades en el Diari oficial de la Unió Europea d'acord amb el Reglament (UE) 1025/2012, es presumeix que són conformes amb els requisits establerts a la secció 2 d'aquest capítol o, si escau, amb les obligacions establertes en el capítol V, seccions 2 i 3 del Reglament, en la mesura que aquestes normes cobreixin aquests requisits o obligacions.

2. D'acord amb l'article 10 del Reglament (UE) 1025/2012, la Comissió ha d'emetre, sense dilació indeguda, sol·licituds d'estandardització que cobreixin tots els requisits establerts en la secció 2 d'aquest capítol i, si escau, sol·licituds d'estandardització que cobreixen les obligacions establertes en el capítol V, seccions 2 i 3, del present Reglament. La sol·licitud d'estandardització també ha de demanar entregables sobre els processos d'informació i documentació per millorar el rendiment dels recursos dels sistemes d'IA, com ara la reducció del consum d'energia i d'altres recursos del sistema d'IA d'alt risc durant el seu cicle de vida, i sobre el desenvolupament eficient de l'energia dels models d'IA d'ús general. Quan es prepari una sol·licitud de normalització, la Comissió ha de consultar el Consell i les parts interessades pertinents, inclòs el fòrum consultiu.

En emetre una sol·licitud de normalització a les organitzacions europees de normalització, la Comissió ha d'especificar que les normes han de ser clares, coherents, fins i tot amb les normes desenvolupades en els diversos sectors per als productes coberts per la legislació d'harmonització de la Unió existent enumerada a l'annex I, i amb l'objectiu d'assegurar que els sistemes d'IA d'alt risc o els models d'IA d'ús general introduïts en el mercat o posats en servei a la Unió compleixin els requisits o les obligacions pertinents que s'estableixen en el present Reglament.

La Comissió ha de sol·licitar a les organitzacions europees de normalització que presentin proves de l'esforç màxim que han fet per complir els objectius a què es refereixen el primer i el segon paràgrafs d'aquest apartat, de conformitat amb l'article 24 del Reglament (UE) 1025/2012.

3. Els participants en el procés de normalització han de tractar de promoure la inversió i la innovació a IA, també incrementant la seguretat jurídica, així com la competitivitat i el creixement del mercat de la Unió, de contribuir al reforç de la cooperació mundial en pro de la normalització, tenint en compte les normes internacionals existents en l'àmbit de la IA que són coherents amb els valors, drets fonamentals i interessos de la Unió, i de millorar la governança multilateral, garantint una representació equilibrada dels interessos i la participació efectiva de totes les parts interessades pertinents de conformitat amb els articles 5, 6 i 7 del Reglament (UE) 1025/2012.

Article 41

Especificacions comunes

1. La Comissió pot adoptar actes d'execució pels quals s'estableixin especificacions comunes per als requisits establerts en la secció 2 del present capítol o, segons correspongui, per a les obligacions establertes en el capítol V, seccions 2 i 3, sempre que s'hagin complert les condicions següents:

(a) De conformitat amb l'article 10, apartat 1, del Reglament (UE) 1025/2012, la Comissió ha sol·licitat, a una o diverses organitzacions europees de normalització que elaborin una norma harmonitzada per als requisits establerts en la secció 2 del present capítol, o segons correspongui, per a les obligacions establertes en el capítol V, seccions 2 i 3, i:

(i) la sol·licitud no ha estat acceptada per cap de les organitzacions europees de normalització; o

(ii) Les normes harmonitzades que aborden aquesta sol·licitud no es lliuren en el termini establert de conformitat amb l'article 10, apartat 1, del Reglament (UE) 1025/2012; o

(iii) les normes harmonitzades pertinents no aborden prou les preocupacions en matèria de drets fonamentals; o

(iv) les normes harmonitzades no s'ajusten a la sol·licitud; i

(b) No s'ha publicat en el Diari oficial de la Unió Europea cap referència a normes harmonitzades que regulin els requisits establerts en la secció 2 del present capítol, o si escau, les obligacions a què es refereix el capítol V, seccions 2 i 3, de conformitat amb el Reglament (UE) 1025/2012 i no es preveu la publicació de tal referència en un termini raonable.

En redactar les especificacions comunes, la Comissió ha de consultar el fòrum consultiu a què es refereix l'article 67.

Els actes d'execució a què es refereix l'apartat primer d'aquest apartat s'han d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

2. Abans de preparar un projecte d'acte d'execució, la Comissió ha d'informar el comitè a què es refereix l'article 22 del Reglament (UE) 1025/2012 que considera que es compleixen les condicions establertes en l'apartat 1 d'aquest article.

3. Es presumeix que els sistemes d'IA d'alt risc o els models d'IA d'ús general que siguin conformes amb les especificacions comunes al fet que es refereix l'apartat 1, o parts d'aquestes especificacions, són conformes amb els requisits establerts en la secció 2 del present capítol o, segons correspongui, per complir les obligacions a què es refereix el capítol V, seccions 2 i 3, en la mesura que aquestes especificacions comunes contemplin aquests requisits o aquestes obligacions.

4. Quan una norma harmonitzada sigui adoptada per una organització europea de normalització i proposada a la Comissió per publicar-ne la referència al Diari oficial de la Unió Europea, la Comissió ha d'avaluar la norma harmonitzada de conformitat amb el Reglament (UE) 1025/2012. Quan la referència a una norma harmonitzada es publiqui al diari oficial de la Unió Europea, la Comissió derogarà els actes d'execució a què es refereix l'apartat 1, o les parts que cobreixen els mateixos requisits establerts en la secció 2 d'aquest capítol o, segons correspongui, les mateixes obligacions establertes en el capítol VI, seccions 2 i 3.

5. Quan no compleixin les especificacions comunes esmentades a l'apartat 1, els proveïdors de sistemes d'IA d'alt risc o els models d'IA d'ús general han de justificar degudament que han adoptat solucions tècniques que compleixen els requisits a què es refereix la secció 2 del present capítol o, segons correspongui, compleixen les obligacions establertes en el capítol V, seccions 2 i 3, en un nivell que, com a mínim, és equivalent.

6. Quan consideri que una especificació comuna no compleix íntegrament els requisits establerts a la secció 2 o, segons sigui el cas, no compleix les obligacions establertes capítol V, seccions 2 i 3, l'estat membre afectat n'ha d'informar la Comissió amb una explicació detallada. Aleshores, la Comissió ha d'avaluar la informació i, si escau, modificar l'acte d'execució pel qual s'estableix l'especificació comuna en qüestió.

Article 42

Presumpció de conformitat amb determinats requisits

1. Es presumeix que els sistemes d'IA d'alt risc que han estat entrenats i provats amb dades que reflecteixen l'entorn geogràfic, conductual, contextual o funcional específic en què se'n preveu l'ús compleixen els requisits pertinents establerts a l'article 10, apartat 4.

2. Es presumeix que els sistemes d'IA d'alt risc que disposen d'un certificat o una declaració de conformitat en virtut d'un esquema de ciberseguretat d'acord amb el Reglament (UE) 2019/881, les referències dels quals s'hagin publicat al Diari oficial de la Unió Europea, compleixen els requisits de ciberseguretat establerts en l'article 15 del present Reglament en la mesura que el certificat de ciberseguretat o la declaració de conformitat, o parts d'aquests, contemplin aquests requisits.

Article 43

Avaluació de conformitat

1. Per als sistemes d'IA d'alt risc enumerats en l'annex III, punt 1, quan, en demostrar el compliment d'un sistema d'IA d'alt risc amb els requisits establerts en la secció 2, ha aplicat normes harmonitzades segons l'article 40, o, si escau, les especificacions comunes a què l'article 41 es refereix, el proveïdor ha d'optar per un dels següents procediments d'avaluació de la conformitat basats en:

(a) El control intern a què es refereix l'annex VI; o

(b) l'avaluació del sistema de gestió de la qualitat i l'avaluació de la documentació tècnica, amb la implicació d'un organisme notificat, a què es refereix l'annex VII.

En demostrar el compliment d'un sistema d'IA d'alt risc amb els requisits establerts a la secció 2, el proveïdor ha de seguir el procediment d'avaluació de la conformitat establert a l'annex VII en les circumstàncies següents:

(a) Les normes harmonitzades a què es refereix l'article 40 no existeixen, i no es disposa de les especificacions comunes a què es refereix l'article 41.

(b) El proveïdor no ha aplicat la norma harmonitzada o només n'ha aplicat una part.

(c) Les especificacions comunes a què la lletra a) es refereix hi són, però el proveïdor no les ha aplicat.

(d) Una o més de les normes harmonitzades a què la lletra a) es refereix s'ha publicat amb una restricció, i només en la part de la norma que estava restringida.

A l'efecte del procediment d'avaluació de la conformitat a què es refereix l'annex VII, el proveïdor pot triar qualsevol dels organismes notificats. No obstant això, quan el sistema d'IA d'alt risc estigui destinat a posar-se en servei per les autoritats garantees del compliment de la llei, d'immigració o d'asil o per les institucions, organismes, oficines o organismes de la Unió, l'autoritat de vigilància del mercat a què es refereix l'article 74, apartat 8, o 9, segons correspongui, actua com a organisme notificat.

2. Per als sistemes d'IA d'alt risc a què els punts 2 a 8 de l'annex III es refereixen, els proveïdors han de seguir el procediment d'avaluació de la conformitat basat en el control intern, tal com es refereix a l'annex VI, que no preveu la participació d'un organisme notificat.

3. En el cas dels sistemes d'IA d'alt risc regulats pels actes legislatius d'harmonització de la Unió enumerada en l'annex I, secció A, el proveïdor s'ha d'atènyer al procediment d'avaluació de la conformitat pertinent exigida per aquests actes legislatius. Els requisits establerts en la secció 2 d'aquest capítol s'han d'aplicar als sistemes d'IA d'alt risc i han de formar part d'aquesta avaluació. Punts 4.3, 4.4, 4.5. També s'ha d'aplicar el punt 4.6 de l'annex VII.

A l'efecte d'aquesta avaluació, els organismes notificats que hagin estat notificats en virtut d'aquests actes legislatius tenen dret a controlar la conformitat dels sistemes d'IA d'alt risc amb els requisits establerts a la secció 2, sempre que s'hagi avaluat el compliment per part d'aquests

organismes notificats dels requisits establerts en l'article 31, apartats 4, 5, 10 i 11, en el context del procediment de notificació d'acord amb aquests actes legislatius.

Quan un acte legislatiu enumerat en l'annex I, secció A, permeti al fabricant del producte prescindir d'una avaluació de la conformitat de tercers, a condició que el fabricant hagi aplicat totes les normes harmonitzades que contemplen tots els requisits pertinents, aquest fabricant només pot recórrer a aquesta opció si també ha aplicat les normes harmonitzades o, si és el cas, les especificacions comunes a què es refereix l'article 41 que contemplen tots els requisits establerts en la secció 2 del present capítol.

4. Els sistemes d'IA d'alt risc que ja han estat subjectes a un procediment d'avaluació de la conformitat han de sotmetre's a un nou procediment d'avaluació de la conformitat en cas d'una modificació substancial, independentment de si el sistema modificat està destinat a ser distribuït o continua sent utilitzat pel responsable del desplegament actual.

En el cas dels sistemes d'IA d'alt risc que continuïn aprenent després de la seva introducció en el mercat o la seva posada en servei, els canvis en el sistema d'IA d'alt risc i el seu funcionament que hagin estat predeterminats pel proveïdor en el moment de l'avaluació inicial de la conformitat i figuren en la informació recollida en la documentació tècnica esmentada en l'annex IV, punt 2, lletra f), no constituïran modificacions substancials.

5. La Comissió està facultada per adoptar actes delegats de conformitat amb l'article 97 per modificar els annexos VI i VII actualitzant-los a la llum del progrés tècnic.

6. La Comissió pot adoptar els actes delegats, d'acord amb l'article 97, per modificar els apartats 1 i 2 d'aquest article, i així sotmetre els sistemes d'IA d'alt risc a què es refereix l'annex II, articles 2 a 8, al procediment d'avaluació de la conformitat que s'esmenta a l'annex VII o en parts d'aquest. La Comissió ha d'adoptar aquests actes delegats tenint en compte l'eficàcia del procediment d'avaluació de la conformitat basat en el control intern a què es refereix l'annex VI per prevenir o minimitzar els riscos per a la salut i la seguretat i la protecció dels drets fonamentals que aquests sistemes plantegen, així com la disponibilitat de capacitats i recursos adequats per part dels organismes notificats.

Article 44

Certificats

1. Els certificats expedits pels organismes notificats de conformitat amb l'annex VII s'han d'elaborar en una llengua que les autoritats competents puguin entendre fàcilment en l'estat membre en què s'estableixi l'organisme notificat.

2. Els certificats romandran vàlids durant el període que ells mateixos indiquin, sense que el període pugui ser superior a cinc anys en el cas dels sistemes d'IA contemplats a l'annex I o de quatre anys en el cas dels sistemes d'IA contemplats a l'annex III. A petició del proveïdor, la validesa d'un certificat es pot ampliar per a períodes posteriors, cadascun no superior a cinc anys per als sistemes d'intel·ligència artificial coberts per l'annex I, i quatre anys per als sistemes d'IA coberts per l'annex III, basant-se en una nova avaluació d'acord amb els procediments d'avaluació de conformitat aplicables. Tot suplement d'un certificat romandrà vàlid si el certificat que complementa és vàlid.

3. Quan consideri que un sistema d'IA ja no compleix els requisits establerts a la secció 2, l'organisme notificat ha de suspendre o retirar el certificat expedit o imposar-li restriccions, llevat

que el compliment dels requisits es garanteixi mitjançant les accions correctores adequades adoptades pel proveïdor del sistema en el termini establert per l'organisme notificat. L'organisme notificat ha de motivar la seva decisió.

Es disposarà d'un procediment d'apel·lació contra les decisions dels organismes notificats, inclosos els certificats de conformitat emesos.

Article 45

Obligacions d'informació dels organismes notificats

1. Els òrgans notificats han d'informar l'autoritat notificadora sobre el següent:

(a) qualsevol certificat d'avaluació tècnica de la documentació de la Unió, qualsevol complement d'aquests certificats i qualsevol aprovació del sistema de gestió de la qualitat expedits d'acord amb els requisits de l'annex VII;

(b) qualsevol denegació, restricció, suspensió o retirada d'un certificat de la Unió d'avaluació de la documentació tècnica o d'una aprovació d'un sistema de gestió de la qualitat expedida d'acord amb els requisits establerts en l'annex VII;

(c) qualsevol circumstància que afecti l'àmbit d'aplicació o a les condicions de notificació;

(d) de qualsevol sol·licitud d'informació sobre les activitats d'avaluació de la conformitat que hagin rebut de les autoritats de vigilància del mercat;

(e) prèvia sol·licitud, les activitats d'avaluació de la conformitat realitzades dins de l'àmbit d'aplicació de la seva notificació i de qualsevol altra activitat feta, incloses les activitats transfrontereres i les subcontractacions.

2. Cada organisme notificat ha d'informar els altres organismes notificats de:

(a) les aprovacions de sistemes de gestió de la qualitat que hagi rebutjat, suspès o retirat i, prèvia sol·licitud, de les aprovacions de sistemes de gestió de la qualitat que hi hagi expedit;

(b) certificats de la Unió d'avaluació de la documentació tècnica o els suplementes a aquests certificats que hagi rebutjat, retirat, suspès o restringit de qualsevol altra manera i, prèvia sol·licitud, dels certificats o els suplementes a aquests que hagi expedit.

3. Cada organisme notificat ha de proporcionar, als altres organismes notificats que duguin a terme activitats similars d'avaluació de la conformitat que cobreixen els mateixos tipus de sistemes d'IA, informació rellevant sobre qüestions relatives a resultats negatius i, a petició, positius d'avaluació de la conformitat.

4. Els organismes notificats han de preservar la confidencialitat de la informació obtinguda, de conformitat amb el que disposa l'article 78.

Article 46

Exempció del procediment d'avaluació de la conformitat

1. Com a excepció al que disposa l'article 43 i prèvia sol·licitud degudament motivada, qualsevol autoritat de vigilància del mercat podrà autoritzar la introducció en el mercat o la posada en servei de sistemes d'IA d'alt risc específics en el territori de l'estat membre que es tracti per motius excepcionals de seguretat pública o per protegir la vida i la salut de les persones, el medi ambient o actius fonamentals de la indústria i de les infraestructures. Aquesta autorització es concedeix per un període limitat mentre es duguin a terme els procediments d'avaluació de la conformitat necessaris, tenint en compte les raons excepcionals que justifiquen l'exempció. La conclusió dels procediments que es tracti s'ha d'aconseguir en el termini més breu possible.

2. En una situació d'urgència degudament justificada per raons excepcionals de seguretat pública o en el cas d'amenaça específica, substancial i imminent per a la vida o la seguretat física de les persones físiques, les autoritats garants del compliment de la llei o les autoritats de protecció civil poden posar en servei un sistema d'IA d'alt risc específic sense l'autorització a què es refereix l'apartat 1, sempre que se sol·liciti aquesta autorització durant o després de l'ús sense demora indeguda. Si es denega l'autorització a què es refereix l'apartat 1, cal suspendre l'ús del sistema d'IA d'alt risc i descartar immediatament tots els resultats i informació de sortida d'aquest ús.

3. L'autorització a què es refereix l'apartat 1 només s'ha d'expedir si l'autoritat de vigilància del mercat arriba a la conclusió que el sistema d'IA d'alt risc compleix els requisits establerts a la secció 2. L'autoritat de vigilància del mercat ha d'informar la Comissió i els altres estats membres de qualsevol autorització emesa d'acord amb els apartats 1 i 2. Aquesta obligació no comprèn les dades operatives sensibles en relació amb les activitats de les autoritats garants del compliment de la llei.

4. Quan, en el termini de quinze dies naturals des de la recepció de la informació a què es refereix l'apartat 3, no s'hagi plantejat cap objecció, ni per part d'un estat membre ni per part de la Comissió, respecte d'una autorització emesa per una autoritat de vigilància de mercat d'un estat membre d'acord amb l'apartat 1, aquesta autorització es considera justificada.

5. Si, en el termini de quinze dies naturals després de la recepció de la notificació a què es refereix l'apartat 3, un estat membre formula objeccions contra una autorització expedida per una autoritat de vigilància del mercat d'un altre estat membre, o si la Comissió considera que l'autorització vulnera el dret de la Unió o que la conclusió dels estats membres relativa al compliment del sistema al fet que es refereix l'apartat 3 és infundada, la Comissió ha de fer consultes amb l'estat membre pertinent sense demora. Es consultarà als operadors que es tracti i se'ls oferirà la possibilitat d'exposar els seus punts de vista. Tenint en compte això, la Comissió ha de decidir si l'autorització està justificada. La Comissió trametrà la decisió a l'estat membre interessat i als operadors pertinents.

6. Si la Comissió considera que l'autorització no està justificada, l'autoritat de vigilància del mercat de l'estat membre que es tracti l'ha de retirar.

7. En el cas dels sistemes d'IA d'alt risc associats a productes regulats pels actes legislatius d'harmonització de la Unió enumerada en l'annex I, secció A, només s'han d'aplicar les exempcions de l'avaluació de la conformitat establertes en aquests actes legislatius d'harmonització de la Unió.

Article 47

Declaració UE de conformitat

1. El proveïdor ha de redactar una declaració UE de conformitat en un format llegible per màquina, amb signatura electrònica o manuscrita, per a cada sistema d'IA d'alt risc, i l'ha de mantenir a disposició de les autoritats nacionals competents durant un període de deu anys a comptar des que el sistema d'IA d'alt risc s'hagi introduït en el mercat o posat en servei. La declaració UE de conformitat ha d'identificar el sistema d'IA d'alt risc per al qual s'ha elaborat. Si ho demanen, cal lliurar a les autoritats nacionals competents pertinents una còpia de la declaració UE de conformitat.
2. La declaració UE de conformitat ha d'indicar que el sistema d'IA d'alt risc en qüestió compleix els requisits establerts a la secció 2. La declaració UE de conformitat ha de contenir la informació recollida a l'annex V i la traducció corresponent a una llengua que pugui ser fàcilment compresa per les autoritats nacionals competents dels estats membres on el sistema d'IA d'alt risc s'introdueixi en el mercat o es posi a disposició.
3. Quan els sistemes d'IA d'alt risc estiguin subjectes a una altra legislació d'harmonització de la Unió que també requereixi una declaració UE de conformitat, s'ha d'elaborar una declaració única de conformitat respecte de tot el dret de la Unió aplicable al sistema d'IA d'alt risc. La declaració ha de contenir tota la informació necessària per identificar la legislació d'harmonització de la Unió a la qual es refereix la declaració.
4. En redactar la declaració UE de conformitat, el proveïdor assumeix la responsabilitat del compliment dels requisits establerts a la secció 2. El proveïdor ha de mantenir actualitzada la declaració UE de conformitat segons correspongui.
5. La Comissió està facultada per adoptar actes delegats de conformitat amb l'article 97 per modificar l'annex V actualitzant el contingut de la declaració UE de conformitat que s'estableix en aquest annex, amb la finalitat d'introduir elements que es facin necessaris a la llum del progrés tècnic.

Article 48

Marcatge CE

1. El marcatge CE està subjecte als principis generals establerts en l'article 30 del Reglament (CE) 765/2008.
2. Per als sistemes d'IA d'alt risc proporcionats digitalment, s'ha d'utilitzar un marcatge CE digital, només si es pot accedir fàcilment a través de la interfície des de la qual s'accedeix a aquest sistema o a través d'un codi fàcilment accessible per màquina o altres mitjans electrònics.
3. El marcatge CE s'ha de fixar de manera que sigui visible, llegible i indeleble per als sistemes d'IA d'alt risc. Quan això no sigui possible o no la naturalesa del sistema d'IA d'alt risc no ho requereixi, s'ha d'adjuntar a l'embalatge o a la documentació amb què s'acompanya, segons correspongui.
4. En el seu cas, el marcatge CE ha d'anar seguit del número d'identificació de l'organisme notificat responsable dels procediments d'avaluació de la conformitat establerts en l'article 43. El número d'identificació de l'organisme notificat s'ha de fixar per l'organisme mateix o, seguint-ne les instruccions, pel proveïdor o pel representant autoritzat del proveïdor. El número

d'identificació també s'ha d'indicar en qualsevol material promocional que esmenti que el sistema d'IA d'alt risc compleix els requisits per al marcatge CE.

5. Quan els sistemes d'IA d'alt risc estiguin subjectes a una altra llei de la Unió que també preveu l'adhesió al marcatge CE, el marcatge CE ha d'indicar que el sistema d'IA d'alt risc també compleix els requisits d'aquesta altra llei.

Article 49

Registre

1. Abans d'introduir en el mercat o posar en servei un sistema d'IA d'alt risc dels inclosos en l'annex III, a excepció dels sistemes d'IA d'alt risc a què l'annex II, punt 2, es refereix, el proveïdor o, si escau, el representant autoritzat s'ha de registrar ell mateix i el seu sistema a la base de dades de la UE esmentada a l'article 71.

2. Abans d'introduir en el mercat o posar en servei un sistema d'IA per al qual el proveïdor hagi determinat que no és d'alt risc segons l'article 6, apartat 3, el proveïdor o, si escau, el representant autoritzat s'ha d'autoregistrar a la base de dades de la UE a què es refereix l'article 71 i registrar-hi el sistema.

3. Abans de posar en servei o fer servir un sistema d'IA d'alt risc que figura a l'annex III, a excepció dels sistemes d'IA d'alt risc que figuren en el punt 2 de l'annex III, els responsables del desplegament que siguin autoritats, institucions de la Unió, organismes, oficines o òrgans o persones que actuïn en nom seu s'han de registrar, seleccionar el sistema i registrar-ne l'ús a la base de dades de la UE a què es refereix l'article 71.

4. Per als sistemes d'IA d'alt risc a què l'annex III, punts 1, 6 i 7, es refereix, en les àrees de garantia del compliment de la llei, migració, asil i control de fronteres, el registre a què aquest article, apartats 1, 2 i 3, es refereix ha d'estar en una secció segura no pública de la base de dades de la UE de l'article 71 i només incloure la següent informació, segons correspongui, a què es refereix:

(a) annex VIII, secció A, punts 1 a 10, a excepció dels punts 6, 8 i 9;

(b) annex VIII, secció B, punts 1 a 5 i 8 i 9;

(c) annex VIII, secció C, punts 1 a 3;

(d) annex IX, punts 1, 2, 3 i 5.

Només la Comissió i les autoritats nacionals a què es refereix l'article 74, apartat 8, han de tenir accés a les seccions restringides respectives de la base de dades de la UE que figuren en el primer paràgraf d'aquest apartat.

5. Els sistemes d'IA d'alt risc a què l'annex III, punt 2, fa referència s'han de registrar en l'àmbit nacional.

CAPÍTOL IV

OBLIGACIONS DE TRANSPARÈNCIA PER ALS PROVEÏDORS I RESPONSABLES DEL DESPLEGAMENT DE DETERMINATS SISTEMES D'IA

Article 50

Obligacions de transparència per als proveïdors i responsables del desplegament de determinats sistemes d'IA

1. Els proveïdors han d'assegurar que els sistemes d'IA destinats a interactuar directament amb les persones físiques estan dissenyats i desenvolupats de manera que les persones físiques afectades estiguin informades que estan interactuant amb un sistema d'IA, llevat que això sigui obvi des del punt de vista d'una persona física raonablement ben informada, observadora i circumspècta, tenint en compte les circumstàncies i el context d'ús. Aquesta obligació no s'ha d'aplicar als sistemes d'IA autoritzats per la llei per detectar, prevenir, investigar o processar delictes, subjectes a les garanties adequades per als drets i llibertats de tercers, llevat que aquests sistemes estiguin disponibles perquè el públic pugui denunciar un delictes.

2. Els proveïdors de sistemes d'IA, inclosos els sistemes d'IA d'ús general, que generin àudio sintètic, imatge, vídeo o text, s'han d'assegurar que els resultats de sortida del sistema d'IA estiguin marcats en un format llegible per màquina i detectables com a generats artificialment o manipulats. Els proveïdors han de garantir que les seves solucions tècniques siguin efectives, interoperables, robustes i fiables en la mesura que això sigui tècnicament factible, tenint en compte les especificitats i limitacions de diversos tipus de continguts, els costos d'aplicació i l'estat general reconegut de la tècnica, com es pot veure en les normes tècniques. Aquesta obligació no s'ha d'aplicar en la mesura que els sistemes d'IA facin una funció assistencial per a l'edició estàndard o no alterin substancialment les dades d'entrada proporcionades pel responsable del desplegament o la seva semàntica, o la llei ho autoritzi per detectar, prevenir, investigar o perseguir delictes penals.

3. Els responsables del desplegament d'un sistema de reconeixement d'emocions o d'un sistema de categorització biomètrica han d'informar les persones físiques exposades al sistema, i han de tractar les dades personals d'acord amb els Reglaments (UE) 2016/679 i (UE) 2018/1725 i la Directiva (UE) 2016/680, segons correspongui. Aquesta obligació no s'ha d'aplicar als sistemes d'IA utilitzats per a la categorització biomètrica i el reconeixement d'emocions, que estan permesos per la llei per detectar, prevenir o investigar delictes, subjectes a les garanties adequades per als drets i llibertats de tercers, i d'acord amb el dret de la Unió.

4. Els responsables del desplegament d'un sistema d'IA que generi o manipuli imatges, àudio o contingut de vídeo que constitueixin un ultrafals, han de comunicar que el contingut ha estat generat o manipulat artificialment. Aquesta obligació no s'ha d'aplicar quan la llei autoritzi l'ús per detectar, prevenir, investigar o perseguir delictes. Quan el contingut formi part d'un treball o programa evidentment artístic, creatiu, satíric, fictici o anàleg, les obligacions de transparència establertes en aquest apartat es limiten a la divulgació de l'existència d'aquest contingut generat o manipulat de manera adequada que no obstaculitzi la visualització o el gaudi de l'obra.

Els responsables del desplegament d'un sistema d'IA que generi o manipuli text que es publiqui amb la finalitat d'informar el públic sobre qüestions d'interès públic han de revelar que el text ha estat generat o manipulat artificialment. Aquesta obligació no s'ha d'aplicar quan la llei autoritzi l'ús per detectar, prevenir, investigar o perseguir delictes penals o quan el contingut generat per IA hagi experimentat un procés de revisió humana o control editorial i quan una persona física o legal tingui la responsabilitat editorial per la publicació del contingut.

5. La informació a què es refereixen els paràgrafs 1 a 4 s'ha de facilitar a les persones físiques afectades de manera clara i distingible, no més tard del moment de la primera interacció o exposició. La informació s'ha d'ajustar als requisits d'accessibilitat aplicables.

6. Els apartats 1 a 4 no han d'afectar els requisits i les obligacions del capítol III, i s'han d'entendre sense perjudici d'altres obligacions de transparència establertes en el dret de la Unió o en el dret nacional per als responsables del desplegament de sistemes d'IA.

7. L'Oficina d'IA ha de fomentar i facilitar l'elaboració de codis de pràctiques en l'àmbit de la Unió per facilitar l'aplicació efectiva de les obligacions en matèria de detecció i etiquetatge de continguts generats o manipulats artificialment. La Comissió pot adoptar actes d'execució per aprovar aquests codis de bones pràctiques d'acord amb el procediment establert a l'article 56 (6). Si considera que el codi no és adequat, la Comissió pot adoptar un acte d'execució especificant normes comunes per a l'aplicació d'aquestes obligacions d'acord amb el procediment d'examen establert en l'article 98, apartat 2).

CAPÍTOL V

MODELS D'ÚS GENERAL

SECCIÓ 1

Normes de classificació

Article 51

Classificació dels models d'IA d'ús general com a models d'IA d'ús general amb risc sistèmic

1. Un model d'IA d'ús general es classifica com a model d'IA d'ús general amb risc sistèmic si compleix alguna de les condicions següents:

(a) Té capacitats d'alt impacte que s'avaluen partint d'eines i metodologies tècniques adequades, inclosos indicadors i paràmetres de referència.

(b) a partir d'una decisió de la Comissió, d'ofici o després d'una alerta qualificada del comitè científic, té capacitats o un impacte equivalent als establerts a la lletra a) tenint en compte els criteris establerts a l'annex XIII.

2. Es presumeix que un model d'IA d'ús general té altes capacitats d'impacte d'acord amb l'apartat 1, lletra a), quan la quantitat acumulada de còmput utilitzada per a la seva formació mesurada en operacions de punt flotant és superior a 1025.

3. La Comissió ha d'adoptar actes delegats de conformitat amb l'article 97 per modificar els límits enumerats en els apartats 1 i 2 d'aquest article, i per complementar els índexs i indicadors a la llum dels desenvolupaments tecnològics en evolució, com ara millores algorítmiques o una eficiència més gran del maquinari, quan sigui necessari, perquè aquests límits reflecteixin l'estat de la tècnica.

Article 52

Procediment

1. Quan un model d'IA d'ús general compleix la condició a què es refereix l'article 51, apartat 1, lletra a), el proveïdor pertinent ho ha de notificar a la Comissió sense demora i, en tot cas, en les

dues setmanes posteriors al fet que el requisit s'hagi complert o se sàpiga que es complirà. Aquesta notificació ha d'incloure la informació necessària per demostrar que s'ha complert el requisit pertinent. Si pren consciència d'un model d'IA d'ús general que presenta riscos sistèmics dels quals no s'ha notificat, la Comissió pot decidir designar-lo model amb risc sistèmic.

2. El proveïdor d'un model d'IA d'ús general que compleixi la condició a què es refereix l'article 51, apartat 1, lletra a), pot presentar, amb la notificació, arguments prou fonamentats per demostrar que, excepcionalment, tot i que compleix el requisit, el model d'IA d'ús general, per les seves característiques específiques, no presenta riscos sistèmics i, per tant, no s'ha de classificar com a model d'IA d'ús general amb risc sistèmic.

3. Quan conclouï que els arguments presentats de conformitat amb l'apartat 2 no estan prou fonamentats i el proveïdor pertinent no va poder demostrar que el model d'IA d'ús general no presenta, per les seves característiques específiques, riscos sistèmics, la Comissió rebutjarà aquests arguments i el model d'IA d'ús general es considerarà un model d'IA d'ús general amb risc sistèmic.

4. La Comissió pot designar un model d'IA d'ús general com a presentació de riscos sistèmics, d'ofici o després d'una alerta qualificada del comitè científic d'acord amb l'article 90, apartat 1, lletra a), basant-se en els criteris establerts a l'annex XIII.

La Comissió està facultada per adoptar actes delegats de conformitat amb l'article 97 per modificar l'annex XIII especificant i actualitzant els criteris que s'hi estableixen.

5. A petició motivada d'un proveïdor el model del qual ha estat designat com a model d'IA d'ús general amb risc sistèmic, de conformitat amb l'apartat 4, la Comissió ha de tenir en compte la sol·licitud i pot decidir fer una nova avaluació si encara es pot considerar que el model d'IA d'ús general, segons els criteris establerts a l'annex XIII, presenta riscos sistèmics. La petició ha de contenir motius objectius, detallats i nous que hagin sorgit des de la decisió de designació. Els proveïdors poden sol·licitar la revaluació dins els sis mesos següents a la decisió de designació. Quan, després de la revaluació, la Comissió decideixi mantenir la designació de model d'IA d'ús general amb risc sistèmic, els proveïdors poden sol·licitar una revaluació en el termini de sis mesos des que la decisió s'hagi pres.

6. La Comissió ha de vetllar perquè es publiqui una llista de models d'IA d'ús general amb risc sistèmic i mantenir-la actualitzada, sense perjudici de la necessitat d'observar i protegir els drets de propietat intel·lectual i la informació empresarial confidencial o els secrets comercials de conformitat amb el dret de la Unió i el dret nacional.

SECCIÓ 2

Obligacions dels proveïdors de models d'IA d'ús general

Article 53

Obligacions dels proveïdors de models d'IA d'ús general

1. Els proveïdors de models d'IA d'ús general han de:

(a)elaborar i mantenir actualitzada la documentació tècnica del model, incloent-hi el procés d'entrenament i proves i els resultats de l'avaluació, que contingui, com a mínim, la informació recollida a l'annex XI amb la finalitat de facilitar-la, prèvia sol·licitud, a l'Oficina d'IA i a les autoritats nacionals competents;

(b)elaborar, mantenir-se al dia i posar a disposició dels proveïdors de sistemes d'IA informació i documentació que tinguin per objectiu integrar el model d'IA d'ús general en els seus sistemes d'IA. Sense perjudici de la necessitat d'observar i protegir els drets de propietat intel·lectual i la informació comercial o secrets comercials confidencials de conformitat amb el dret de la Unió i el dret nacional, la informació i la documentació han de:

(i)permetre als proveïdors de sistemes d'IA tenir un bon coneixement de les capacitats i limitacions del model d'IA d'ús general i complir les seves obligacions d'acord amb el Reglament; i

(ii) contenir, com a mínim, els elements que es recullen a l'annex XII;

(c)establir directrius per complir el dret de la Unió en matèria de drets d'autor i drets afins, i en particular, per detectar i complir, per exemple, a través de tecnologies punta, una reserva de drets expressada de conformitat amb l'article 4, apartat 3, de la Directiva (UE) 2019/790;

(d)elaborar i posar a disposició del públic un resum prou detallat sobre el contingut utilitzat per a l'entrenament del model d'IA d'ús general, segons un model facilitat per l'Oficina d'IA.

2. Les obligacions de l'apartat 1, lletres a) i b), no s'han d'aplicar a proveïdors de models d'IA que es llancen subjectes a una llicència lliure i de codi obert que permet accedir al model, fer-ne ús, modificar-lo i distribuir-lo, i de la qual els paràmetres, inclosos els pesos, la informació sobre l'arquitectura del model i la informació sobre l'ús que se'n va, estan disponibles per al públic. Aquesta excepció no s'ha d'aplicar als models d'IA d'ús general amb risc sistèmic.

3. Els proveïdors de models d'IA d'ús general han de cooperar amb la Comissió i les autoritats nacionals competents, segons sigui necessari, en l'exercici de les seves competències i facultats en virtut del present Reglament.

4. Els proveïdors de models d'IA d'ús general podran recórrer a codis de bones pràctiques en el sentit de les disposicions de l'article 56 per demostrar el compliment de les obligacions establertes en l'apartat 1 del present article, finalitats que es publiqui una norma harmonitzada. El compliment de les normes harmonitzades europees atorga als proveïdors la presumpció de conformitat en la mesura que aquestes normes cobreixin aquestes obligacions. Els proveïdors de models d'IA d'ús general que no compleixin un codi de pràctiques aprovat o que no compleixin una norma harmonitzada europea han de demostrar mitjans alternatius adequats de compliment per a l'avaluació per part de la Comissió.

5. Per facilitar el compliment de l'annex XI, en particular punt 2, lletres d) i e), la Comissió està facultada per adoptar actes delegats de conformitat amb l'article 97 per detallar les metodologies de mesurament i càlcul amb l'objectiu de permetre una documentació comparable i verificable.

6. La Comissió està facultada per adoptar actes delegats de conformitat amb l'article 97, apartat 2, per modificar els annexos XI i XII d'acord amb els avenços tecnològics.

7. Tota la informació o documentació obtinguda en virtut d'aquest article, inclosos els secrets comercials, s'ha de tractar d'acord amb les obligacions de confidencialitat establertes en l'article 78.

Article 54

Representants autoritzats dels proveïdors de models d'IA d'ús general

1. Abans que s'introdueixi en el mercat de la Unió un model d'IA d'ús general, els proveïdors establerts en tercers països, per mandat escrit, han de designar un representant autoritzat establert a la Unió.

2. El proveïdor ha de permetre que el seu representant autoritzat faci les funcions que s'especifiquen en el mandat rebut del proveïdor.

3. El representant autoritzat ha de dur a terme les funcions que s'especifiquen en el mandat que ha rebut del proveïdor. Ha de proporcionar una còpia del mandat a l'Oficina d'IA, si aquesta ho sol·licita, en una de les llengües oficials de les institucions de la Unió. A l'efecte del Reglament, el mandat faculta el representant autoritzat per dur a terme les funcions següents:

(a) Verificar que la documentació tècnica especificada a l'annex XI s'hagi elaborat i que el proveïdor hagi complert totes les obligacions a què es refereix l'article 53 i, si escau, l'article 55.

(b) conservar una còpia de la documentació tècnica especificada a l'annex XI a disposició de l'Oficina d'IA i de les autoritats nacionals competents, durant un període de deu anys des que el model d'IA d'ús general s'hagi introduït en el mercat, i les dades de contacte del proveïdor que ha designat el representant autoritzat;

(c) prèvia petició motivada, proporcionar a l'Oficina d'IA, tota la informació i documentació, inclosa la referida en la lletra b), necessària per demostrar el compliment de les obligacions d'aquest capítol;

(d) prèvia sol·licitud motivada, cooperar amb l'Oficina d'IA i les autoritats competents en qualsevol acció que aquestes adoptin en relació amb el model d'IA d'ús general, fins i tot quan el model s'integri en els sistemes d'intel·ligència artificial introduïts en el mercat o posats en servei a la Unió.

4. En virtut del mandat, el representant autoritzat queda facultat perquè, a més o en comptes del proveïdor, se li adrecin l'Oficina d'IA o les autoritats competents, pel que fa a totes les qüestions relatives a garantir el compliment del Reglament.

5. El representant autoritzat ha de posar fi al mandat si considera o té motius per considerar que el proveïdor actua contravenint les obligacions que li corresponen segons el Reglament. En aquest cas, també ha d'informar immediatament l'Oficina d'IA sobre la rescissió del mandat i els motius pels quals ha tingut lloc.

6. L'obligació establerta en aquest article no s'ha d'aplicar als proveïdors de models d'IA d'ús general que es publiquin sota una llicència lliure i de codi obert que permeti l'accés, l'ús, la

modificació i la distribució del model, i els paràmetres dels quals, inclosos els pesos, la informació sobre l'arquitectura del model, i la informació sobre l'ús de models, es posin a disposició del públic, llevat que els models d'IA d'ús general presentin riscos sistèmics.

SECCIÓ 3

Obligacions dels proveïdors de models d'IA d'ús general amb risc sistèmic

Article 55

Obligacions dels proveïdors de models d'IA d'ús general amb risc sistèmic

1. A més de les obligacions enumerades als articles 53 i 54, els proveïdors de models d'IA d'ús general amb risc sistèmic han de:

(a)avaluar els models d'acord amb protocols i eines estandarditzades que reflecteixin l'estat de la tècnica, incloent-hi la pràctica i documentació de proves adversàries del model amb la finalitat d'identificar i mitigar els riscos sistèmics;

(b)avaluar i mitigar els possibles riscos sistèmics en l'àmbit de la Unió, incloent-ne l'origen, que puguin derivar del desenvolupament, la introducció en el mercat o l'ús de models d'IA d'ús general amb risc sistèmic;

(c)seguir, documentar i, sense dilació indeguda, aportar a l'Oficina d'IA i, si escau, a les autoritats nacionals competents, informació rellevant sobre incidents greus i possibles mesures correctores per resoldre'ls;

(d)garantir un nivell adequat de protecció de la ciberseguretat per al model d'IA d'ús general amb risc sistèmic i la infraestructura física del model.

2. Els proveïdors de models d'IA d'ús general amb risc sistèmic poden recórrer a codis de bones pràctiques en el sentit de les disposicions de l'article 56 per demostrar el compliment de les obligacions establertes en l'apartat 1 del present article, finalitats que es publiqui una norma harmonitzada. El compliment de les normes harmonitzades europees atorga als proveïdors la presumpció de conformitat en la mesura que aquestes normes cobreixin aquestes obligacions. Els proveïdors de models d'IA d'ús general que no s'adhereixin a un codi de bones pràctiques aprovat o no compleixin una norma harmonitzada europea hauran de demostrar que compleixen les seves obligacions per mitjans alternatius adequats per a la seva avaluació per part de la Comissió.

3. Tota la informació o documentació obtinguda en virtut d'aquest article, inclosos els secrets comercials, s'ha de tractar d'acord amb les obligacions de confidencialitat establertes en l'article 78.

SECCIÓ 4

Codis de bones pràctiques

Article 56

Codis de bones pràctiques

1. L'Oficina d'IA ha de fomentar i facilitar l'elaboració de codis de bones pràctiques en l'àmbit de la Unió per contribuir a l'aplicació adequada del present Reglament, tenint en compte els enfocaments internacionals.
2. El Consell i l'Oficina d'Intel·ligència Artificial han de garantir que els codis de bones pràctiques cobreixin almenys les obligacions previstes als articles 53 i 55, incloses les qüestions següents:
 - (a) els mitjans per garantir que la informació a què es refereix l'article 53, apartat 1, lletres a) i b), es mantingui actualitzada en termes d'avenços tecnològics i de mercat;
 - (b) el nivell de detall adequat per al resum sobre el contingut utilitzat per a l'entrenament;
 - (c) la determinació del tipus i la naturalesa dels riscos sistèmics en l'àmbit de la Unió, incloses les seves fonts, si escau;
 - (d) les mesures, procediments i modalitats d'avaluació i gestió dels riscos sistèmics a escala de la Unió, inclosa la seva documentació, que han de ser proporcionals als riscos i tenir-ne en compte la gravetat i probabilitat i les dificultats específiques per fer-los front, considerant la manera en què aquests riscos poden sorgir i materialitzar-se al llarg de la cadena de valor de la IA.
3. L'Oficina d'IA pot convidar tots els proveïdors de models d'IA d'ús general, i també les autoritats nacionals competents pertinents, a participar en l'elaboració de codis de bones pràctiques. Les organitzacions de la societat civil, la indústria, el món acadèmic i altres parts interessades rellevants, com ara proveïdors posteriors i experts independents, poden donar suport al procés.
4. El Consell d'IA i l'Oficina d'IA han de vetllar perquè els codis de bones pràctiques estableixin clarament els seus objectius específics i continguin compromisos o mesures, inclosos els indicadors clau de rendiment, si fa al cas, per garantir l'assoliment dels objectius, i que tinguin degudament en compte les necessitats i interessos de totes les parts interessades, incloses les persones afectades, en l'àmbit de la Unió.
5. L'Oficina d'IA ha de tenir com a objectiu garantir que els participants en els codis de pràctiques informin regularment l'Oficina d'IA sobre l'aplicació dels compromisos i les mesures adoptades i els seus resultats, fins i tot si es mesuren en relació amb els indicadors clau de rendiment segons correspongui. Els indicadors clau de rendiment i els compromisos d'informació han de reflectir diferències en la mida i la capacitat entre els diferents participants.
6. L'Oficina d'IA i el Consell han de seguir i avaluar amb regularitat l'assoliment dels objectius dels codis de bones pràctiques per part dels participants i la contribució d'aquests a l'aplicació adequada del present Reglament. El Consell i l'Oficina d'IA han d'avaluar si els codis de bones pràctiques cobreixen les obligacions previstes en els articles 53 i 55, i han de seguir i avaluar amb regularitat l'assoliment dels objectius propis. Han de publicar la seva avaluació de l'adequació dels codis de bones pràctiques.

La Comissió pot, a través d'un acte d'execució, aprovar un codi de pràctiques i donar-li validesa general dins la Unió. Aquest acte d'execució s'ha d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

7. L'Oficina d'IA pot convidar els proveïdors de models d'IA d'ús general a adherir-se als codis de bones pràctiques. Per als proveïdors de models d'IA d'ús general que no presentin riscos sistèmics, l'adhesió es pot limitar a les obligacions previstes a l'article 53, llevat que manifestin explícitament interès per unir-se al codi complet.

8. A més, si escau, l'Oficina d'IA ha de fomentar i facilitar la revisió i adaptació dels codis de bones pràctiques; en particular, en funció de les normes emergents. L'Oficina d'IA ha d'ajudar en l'avaluació de les normes disponibles.

9. Els codis de bones pràctiques han d'estar llestos a tot tardar el 2 de maig de 2025. L'Oficina d'IA ha d'adoptar les mesures necessàries, inclosa la invitació als proveïdors, de conformitat amb l'apartat 7.

Si, abans del 2 d'agost de 2025, no es pot tenir elaborat un codi de bones pràctiques, o si l'Oficina d' Intel·ligència Artificial considera que aquest no és adequat després d'haver-lo avaluat segons l'apartat 6 d'aquest article, la Comissió, mitjançant actes d'execució, pot proporcionar normes comunes per a l'aplicació de les obligacions previstes en els articles 53 i 55, incloses les qüestions previstes en l'apartat 2 d'aquest article. Els actes d'execució s'han d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

CAPÍTOL VI

MESURES DE SUPORT A LA INNOVACIÓ

Article 57

Espais controlats de proves per a IA reglamentaris

1. Els estats membres han de vetllar perquè les seves autoritats competents estableixin almenys un espai controlat de proves per a la IA a escala nacional, que ha d'estar operatiu el 2 d'agost de 2026 a tot tardar. Aquest espai controlat de proves també es pot establir de manera conjunta amb les autoritats competents d'altres estats membres. La Comissió pot aportar suport tècnic, assessorament i eines per a l'establiment i el funcionament dels espais controlats de proves per a la IA.

L'obligació prevista en el paràgraf primer també pot complir-se mitjançant la participació en un espai controlat de proves existent en la mesura que aquesta participació proporcioni un nivell de cobertura nacional equivalent als estats membres participants.

2. També poden establir-se espais controlats de proves per a la IA addicionals a escala regional o local o conjuntament amb les autoritats competents d'altres estats membres.

3. El Supervisor Europeu de Protecció de Dades també podrà establir un espai controlat de proves per a la IA per a les institucions, òrgans i organismes de la Unió, i podrà exercir les funcions i tasques de les autoritats nacionals competents de conformitat amb el present capítol.

4. Els estats membres han de vetllar perquè les autoritats competents a què es refereixen els apartats 1 i 2 destinin els recursos suficients per complir les disposicions d'aquest article de manera efectiva i oportuna. Si cal, les autoritats nacionals competents han de cooperar amb altres autoritats pertinents i poden permetre la participació d'altres actors dins l'ecosistema de

la IA. El present article no ha d'afectar altres espais controlats de proves establerts en virtut del dret de la Unió o nacional. Els estats membres han de garantir un nivell adequat de cooperació entre les autoritats que supervisen aquests altres espais controlats de proves i les autoritats nacionals competents.

5. Els espais controlats de proves per a la IA establerts de conformitat amb l'apartat 1 han de proporcionar un entorn controlat que fomenti la innovació i faciliti el desenvolupament, l'entrenament, la prova i la validació de sistemes innovadors d'IA durant un període limitat abans que s'introdueixin en el mercat o es posin en servei, d'acord amb un pla de l'espai controlat de proves específic acordat entre els proveïdors o proveïdors potencials i l'autoritat competent. Aquests espais controlats de proves podran incloure proves en condicions reals supervisades dins seu.

6. Les autoritats competents han de proporcionar, si escau, orientació, supervisió i suport dins l'espai controlat de proves per a la IA amb vista a determinar els riscos, en particular per als drets fonamentals, la salut i la seguretat, a les proves i a les mesures de reducció i la seva eficàcia en relació amb les obligacions i els requisits del present Reglament i, quan escaigui, d'altres disposicions de Dret de la Unió i nacional l'observança de les quals se supervisi en l'espai controlat de proves.

7. Les autoritats competents han de proporcionar als proveïdors i proveïdors potencials que participin en l'espai controlat de proves per a la IA orientacions sobre les expectatives en matèria de regulació i la manera de complir els requisits i obligacions establerts en el present Reglament.

A petició del proveïdor o proveïdor potencial del sistema d'IA, l'autoritat competent ha d'aportar una prova escrita de les activitats dutes a terme amb èxit en l'espai controlat de proves. L'autoritat competent també ha de facilitar un informe de sortida en què es detallin les activitats dutes a terme a l'espai controlat de proves i els resultats i resultats de l'aprenentatge corresponents. Els proveïdors poden fer servir aquesta documentació per demostrar el compliment del present Reglament a través del procés d'avaluació de la conformitat o de les activitats de vigilància del mercat pertinents. Referent a això, les autoritats de vigilància del mercat i els organismes notificats tindran en compte positivament els informes de sortida proporcionats i les proves escrites aportades per l'autoritat nacional competent, amb vista a accelerar els procediments d'avaluació de la conformitat en una mesura raonable.

8. Amb subjecció a les disposicions de confidencialitat de l'article 78, i amb l'acord del proveïdor o proveïdor potencial, la Comissió i el Consell d'IA estan autoritzats a accedir als informes de sortida i els han de tenir en compte, si escau, en l'exercici de les seves funcions en virtut del present Reglament. Si tant el proveïdor com el proveïdor potencial i l'autoritat nacional competent hi consenten de manera explícita, l'informe de sortida es pot posar a disposició pública a través de la plataforma única d'informació a què es refereix aquest article.

9. La finalitat de l'establiment d'espais controlats de proves per a la IA és contribuir a l'assoliment dels objectius següents:

(a) millorar la seguretat jurídica per aconseguir el compliment normatiu del Reglament o, si escau, d'altres disposicions del dret de la Unió i nacional aplicables;

(b) donar suport a l'intercanvi de millors pràctiques mitjançant la cooperació amb les autoritats que participen en l'espai controlat de proves per a la IA;

(c) fomentar la innovació i la competitivitat i facilitar el desenvolupament d'un ecosistema d'IA;

(d) contribuir a un aprenentatge normatiu basat en dades contrastades;

(e) facilitar i accelerar l'accés al mercat de la Unió dels sistemes d'IA, en particular quan els proporcionin pimes, incloses les empreses emergents.

10. Les autoritats nacionals competents han de vetllar perquè, en la mesura que els sistemes innovadors d'IA impliquin el tractament de dades personals o estiguin compresos dins l'àmbit de supervisió d'altres autoritats nacionals o autoritats competents que proporcionin o facilitin l'accés a les dades, les autoritats nacionals de protecció de dades i les altres autoritats nacionals o competents estiguin lligades al funcionament de l'espai controlat de proves per a la IA i involucrades en la supervisió d'aquests aspectes en la mesura que ho permetin les funcions i competències respectives.

11. Els espais controlats de proves per a la IA no afectaran les facultats de supervisió o correctores de les autoritats competents que supervisen els espais controlats de proves, tampoc a escala regional o local. Qualsevol risc significatiu per a la salut i la seguretat i els drets fonamentals identificats durant el desenvolupament i les proves d'aquests sistemes d'IA ha de donar lloc a una mitigació adequada. Les autoritats nacionals competents estan facultades per suspendre temporalment o permanentment el procés de prova, o la participació en l'espai controlat de proves si no és possible una reducció efectiva, i han de comunicar a decisió a l'Oficina d'IA. Amb l'objectiu de donar suport a la innovació en matèria d'IA a la Unió, les autoritats nacionals competents han d'exercir les facultats de supervisió dins els límits del dret pertinent i fer ús de la seva potestat discrecional en aplicar disposicions jurídiques en relació amb un projecte específic d'espai controlat de proves per a la IA.

12. Els proveïdors i proveïdors potencials que participin en l'espai controlat de proves per a la IA han de respondre, d'acord amb el Dret de la Unió i nacional en matèria de responsabilitat, de qualsevol dany infligit a tercers com a resultat de l'experimentació feta en l'espai controlat de proves. No obstant això, sempre que els futurs proveïdors observin el pla específic i els termes i condicions per participar-hi i segueixin de bona fe que l'autoritat nacional competent facilita, no s'han d'imposar multes administratives per part de les autoritats per infraccions del Reglament. Si altres autoritats competents responsables d'altres disposicions del dret de la Unió i nacional han participat activament en la supervisió del sistema d'IA en l'espai controlat de proves i han proporcionat orientacions per al compliment, no s'han d'imposar multes administratives en relació amb aquestes disposicions.

13. Els espais controlats de proves per a la IA seran dissenyats i posats en pràctica de tal manera que, quan escaigui, facilitin la cooperació transfronterera entre les autoritats nacionals competents.

14. Les autoritats nacionals competents han de coordinar les seves activitats i cooperaran en el marc del Consell.

15. Les autoritats nacionals competents han d'informar l'Oficina d'IA i el Consell d'IA de l'establiment d'un espai controlat de proves i els poden demanar suport i orientació. L'Oficina d'IA ha de posar a disposició del públic una llista dels espais controlats de proves previstos i existents i mantenir-la actualitzada per fomentar més interacció en els espais controlats de proves per a la IA, així com la cooperació transfronterera.

16. Les autoritats nacionals competents han de presentar informes anuals a l'Oficina d'IA i al Consell d'IA, per primera vegada un any després de l'establiment de l'espai controlat de proves per a la IA i, posteriorment, cada any fins a la finalització, així com un informe final. Aquests informes han de proporcionar informació sobre el progrés i els resultats de la posada en pràctica d'aquests espais controlats de proves, incloent-hi millors pràctiques, incidents, ensenyaments extrets i recomanacions sobre la seva configuració i, si s'escau, sobre l'aplicació i possible revisió del present Reglament, inclosos els seus actes delegats i d'execució, i sobre l'aplicació d'altres disposicions de Dret de la Unió, supervisada per les autoritats competents en el marc de l'espai controlat de proves. Les autoritats nacionals competents han de posar a disposició del públic, en línia, els informes anuals o resums d'aquests informes. La Comissió ha de tenir en compte, si escau, els informes anuals en l'exercici de les seves funcions en virtut del present Reglament.

17. La Comissió ha de desenvolupar una interfície única i específica que contingui tota la informació pertinent relacionada amb els espais controlats de proves per a la IA perquè les parts interessades puguin interactuar amb els espais controlats de proves per a la IA i plantejar consultes a les autoritats competents, i també demanar orientacions no vinculants sobre la conformitat de productes, serveis i models de negoci innovadors que incorporin tecnologies d'IA, de conformitat amb l'article 62, apartat 1, lletra c). La Comissió s'ha de coordinar de manera proactiva amb les autoritats nacionals competents, si escau.

Article 58

Disposicions detallades relatives als espais controlats de proves per a la IA i al funcionament d'aquests espais

1. A fi d'evitar que es produeixi una fragmentació a la Unió, la Comissió ha d'adoptar actes d'execució que especifiquin les disposicions detallades per a l'establiment, el desenvolupament, la posada en pràctica, el funcionament i la supervisió dels espais controlats de proves per a la IA. Els actes d'execució han d'incloure principis comuns en els següents temes:

(a) els criteris d'admissibilitat i selecció per participar en l'espai controlat de proves per a la IA;

(b) els procediments per a la sol·licitud, la participació, la supervisió, la sortida i la terminació de l'espai controlat de proves per a la IA, inclosos el pla de l'espai controlat de proves i l'informe de sortida;

(c) els termes i condicions aplicables als participants.

Els actes d'execució s'han d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

2. Els actes d'execució a què es refereix l'apartat 1 han de garantir:

- (a) que els espais controlats de proves per a la IA estiguin oberts a qualsevol proveïdor o proveïdor potencial d'un sistema d'IA que presenti una sol·licitud i compleixi els criteris d'admissibilitat i selecció, que seran transparents i equitatius, i també que les autoritats nacionals competents informin els sol·licitants de la seva decisió en un termini de tres mesos a partir de la presentació de la sol·licitud;
- (b) que els espais controlats de proves per a la IA permetin un accés ampli i igualitari i s'adaptin a la demanda de participació; els proveïdors i proveïdors potencials també poden presentar sol·licituds en associació amb responsables del desplegament i amb altres tercers pertinents;
- (c) que les disposicions detallades i les condicions relatives als espais controlats de proves per a la IA propiciïn, en la mesura del possible, que les autoritats nacionals competents disposin de flexibilitat per establir i gestionar els seus espais controlats de proves per a la IA;
- (d) que l'accés als espais controlats de proves per a la IA sigui gratuït per a les pimes, incloses les empreses emergents, sens perjudici dels costos excepcionals que les autoritats nacionals competents puguin recuperar d'una forma justa i proporcionada;
- (e) que es faciliti als proveïdors i proveïdors potencials, mitjançant els resultats de l'aprenentatge dels espais controlats de proves per a la IA, el compliment de les obligacions d'avaluació de la conformitat en virtut del present Reglament i l'aplicació voluntària dels codis de conducta a què es refereix l'article 95;
- (f) que els espais controlats de proves per a la IA facilitin la participació d'altres agents pertinents de l'ecosistema de la IA, com ara els organismes notificats i els organismes de normalització, les pimes, incloses les empreses emergents, les empreses, els agents innovadors, les instal·lacions d'assaig i experimentació, els laboratoris de recerca i experimentació i els centres europeus d'innovació digital, els centres d'excel·lència i els investigadors, per permetre i facilitar la cooperació amb els sectors públic i privat;
- (g) que els procediments, processos i requisits administratius per a la sol·licitud, la selecció, la participació i la sortida de l'espai controlat de proves per a la IA siguin senzills i fàcilment intel·ligibles i es comuniquin clarament, a fi de facilitar la participació de les pimes, incloses les empreses emergents, amb capacitats jurídiques i administratives limitades, i es racionalitzin a tota la Unió, a fi d'evitar la fragmentació i fer que la participació en un espai controlat de proves per a la IA establert per un estat membre o pel Supervisor Europeu de Protecció de Dades estigui reconeguda mútuament i uniformement i tingui els mateixos efectes jurídics a tota la Unió;

(h) que la participació en l'espai controlat de proves per a la IA es limiti a un període que s'ajusti a la complexitat i l'escala del projecte, prorrogable per l'autoritat nacional competent;

(i) que els espais controlats de proves per a la IA facilitin el desenvolupament d'eines i infraestructures per a la prova, l'avaluació comparativa, l'avaluació i l'explicació de les dimensions dels sistemes d'IA pertinents per a l'aprenentatge normatiu, com la precisió, la solidesa i la ciberseguretat, així com de mesures per mitigar els riscos per als drets fonamentals i la societat en conjunt.

3. als proveïdors potencials que participin en els espais controlats de proves per a la IA, en particular a les pimes i les empreses emergents, quan escaigui, se'ls ha d'oferir serveis previs al desplegament, com ara orientacions sobre l'aplicació del present Reglament, altres serveis que aporten valor afegit, com ara ajut amb els documents de normalització i la certificació, i accés a les instal·lacions d'assaig i experimentació, els centres europeus d'innovació digital i els centres d'excel·lència.

4. Quan estudiïn autoritzar la pràctica de proves en condicions reals supervisades en el marc d'un espai controlat de proves per a la IA que s'estableixi en virtut del present article, les autoritats nacionals competents han d'acordar específicament les condicions d'aquestes proves i, en particular, les garanties adequades amb els participants, amb vista a protegir els drets fonamentals, la salut i la seguretat. Si és el cas, han de cooperar amb altres autoritats nacionals competents a fi de garantir pràctiques coherents a tota la Unió.

Article 59

Tractament ulterior de dades personals per al desenvolupament de determinats sistemes d'IA en favor de l'interès públic en l'espai controlat de proves per a la IA

1. En l'espai controlat de proves, les dades personals recaptades lícitament amb altres finalitats només es poden tractar amb l'objectiu de desenvolupar, entrenar i provar determinats sistemes d'IA en l'espai controlat de proves quan es compleixin totes les condicions següents:

(a) Els sistemes d'IA s'han de desenvolupar per salvaguardar l'interès públic substancial d'una autoritat o d'una altra persona física o jurídica i en una o més de les àrees següents:

(i) la seguretat pública i la salut pública, inclosa la detecció de malalties, la prevenció del diagnòstic, el control i el tractament i la millora dels sistemes d'atenció sanitària;

(ii) un alt nivell de protecció i millora de la qualitat del medi ambient, protecció de la biodiversitat, protecció contra la contaminació, mesures de transició verda, mesures de mitigació del canvi climàtic i mesures d'adaptació;

(iii) sostenibilitat energètica;

(iv) seguretat i resiliència dels sistemes de transport i mobilitat, infraestructures i xarxes crítiques;

- (v) eficiència i qualitat de les administracions públiques i dels serveis públics;

- (b) Les dades tractades són necessàries per complir un o més dels requisits esmentats en el capítol III, secció 2, quan aquests requisits no es puguin complir efectivament mitjançant el tractament de dades anònimes, sintètiques o altres no personals;

- (c) hi ha mecanismes de supervisió eficaços per detectar si, durant l'experimentació en l'espai controlat de proves, poden produir-se riscos elevats per als drets i llibertats dels interessats, esmentats a l'article 35 del Reglament (UE) 2016/679 i a l'article 39 del Reglament (UE) 2018/1725, així com mecanismes de resposta per mitigar sense demora aquests riscos i, si s'escau, aturar el tractament;

- (d) Els proveïdors només poden compartir les dades recaptades originalment de conformitat amb el dret de la Unió en matèria de protecció de dades; les dades personals creades en l'espai controlat de proves no poden sortir de l'espai controlat de proves;

- (e) Els proveïdors poden compartir les dades recopilades originalment només d'acord amb la legislació de protecció de dades de la Unió; cap dada personal creada en l'espai controlat de proves no es pot compartir fora de l'espai controlat de proves.

- (f) El tractament de dades personals en el context de l'espai controlat de proves no condueix a mesures o decisions que afecten els interessats ni afecta l'aplicació dels seus drets establerts en la legislació de la Unió sobre protecció de dades personals;

- (g) les dades personals tractades en el context de l'espai controlat de proves estan protegides per mesures tècniques i organitzatives apropiades i s'eliminen una vegada acabada la participació en l'espai controlat de proves o quan les dades personals han arribat al final del període de conservació;

- (h) els arxius de registre del tractament de dades personals en el context de l'espai controlat de proves es conserven mentre dura la participació en l'espai controlat de proves, llevat que es disposi una altra cosa en el dret de la Unió o el dret nacional;

- (i) una descripció completa i detallada del procés i la justificació de l'entrenament, les proves i la validació del sistema d'IA es manté juntament amb els resultats de les proves com a part de la documentació tècnica a què es refereix l'annex IV;

(j) Es publica una breu síntesi del projecte d'IA desenvolupat en l'espai controlat de proves, juntament amb els seus objectius i resultats previstos, en el lloc web de les autoritats competents; aquesta obligació no comprèn les dades operatives sensibles relatives a les activitats de les autoritats garants del compliment de la llei, del control fronterer, de la immigració o de l'asil.

2. Quan es dugui a terme amb finalitats de prevenció, investigació, detecció o enjudiciament de delictes o d'execució de sancions penals, incloses la protecció davant amenaces per a la seguretat pública i la prevenció d'aquestes amenaces, i sota el control i la responsabilitat de les autoritats garants del compliment de la llei, el tractament de dades personals en els espais controlats de proves per a la IA s'ha de basar en un dret específic, de la Unió o nacional, i complir les condicions acumulatives que s'indiquen a l'apartat 1.

3. L'apartat 1 s'entén sense perjudici del dret de la Unió o del dret nacional que exclou el tractament de dades personals per a finalitats que no siguin les explícitament esmentades en aquesta llei així com sense perjudici del dret de la Unió o del dret nacional que estableix les bases per al tractament de dades personals necessàries amb la finalitat de desenvolupar, provar o formar sistemes d'IA innovadors o qualsevol altra base legal, de conformitat amb el dret de la Unió sobre la protecció de dades personals.

Article 60

Proves de sistemes d'IA d'alt risc en condicions reals fora dels espais controlats de proves per a la IA

1. Els proveïdors o proveïdors potencials de sistemes d'IA d'alt risc enumerats a l'annex III poden fer proves de sistemes d'IA d'alt risc en condicions reals fora dels espais controlats de proves per a la IA de conformitat amb el present article i amb el pla de la prova en condicions reals a què es refereix el present article, sens perjudici de les prohibicions establertes a l'article 5.

La Comissió, mitjançant actes d'execució, ha d'especificar els elements detallats del pla de proves del món real. Els actes d'execució s'han d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

Aquest apartat s'entén sense perjudici de la legislació de la Unió o del dret nacional sobre les proves en condicions reals de sistemes d'IA d'alt risc relacionats amb els productes coberts per la legislació d'harmonització de la Unió enumerada a l'annex I.

2. Els proveïdors o proveïdors potencials poden fer les proves de sistemes d'IA d'alt risc a què es refereix l'annex III en condicions reals en qualsevol moment abans d'introduir en el mercat o posar en servei el sistema d'IA per si mateixos o en associació amb un o més responsables del desplegament o responsables del desplegament potencials.

3. La prova dels sistemes d'IA d'alt risc en condicions reals en virtut d'aquest article s'ha de fer sense perjudici de qualsevol revisió ètica que el dret de la Unió o el dret nacional exigeixin.

4. Els proveïdors o proveïdors potencials poden fer les proves en condicions reals només quan es compleixen totes les condicions següents:

(a) El proveïdor o proveïdor potencial ha elaborat un pla de proves del món real i l'ha presentat a l'autoritat de vigilància del mercat de l'estat membre on es faran les proves en condicions reals.

- (b) L'autoritat de vigilància del mercat de l'estat membre en què es faran les proves en condicions reals ha aprovat les proves en condicions reals i el pla de proves del món real; quan l'autoritat de vigilància del mercat no hagi proporcionat una resposta en un termini de trenta dies, s'entendrà que s'han aprovat les proves en condicions reals del món i el pla de proves del món real; quan la legislació nacional no concedeix una aprovació tàcita, les proves en condicions reals romanen subjectes a una autorització.
- (c) El proveïdor o proveïdor potencial, a excepció de proveïdors o proveïdors potencials de sistemes d'IA d'alt risc a què es fa referència a l'annex III, punts 1, 6 i 7, en les àrees de garantia del compliment de la llei, migració, asil i gestió de control de fronteres, i els sistemes d'IA d'alt risc a què es refereix l'annex III punt 2, han registrat les proves en condicions reals d'acord amb l'article 71, apartat 4, amb un número d'identificació únic a escala de la Unió i amb la informació especificada a l'annex IX; el proveïdor o proveïdor potencial de sistemes d'IA d'alt risc a què es refereix l'annex III, punt 1, 6 i 7, en els àmbits de garantia del compliment de la llei i gestió de migració, asil i control de fronteres, ha registrat les proves en condicions reals en la secció segura no pública de la base de dades de la UE d'acord amb l'article 49, lletra d), amb un únic número d'identificació únic a tota la Unió i amb la informació que s'hi especifica; el proveïdor o proveïdor potencial de sistemes d'IA d'alt risc a què es refereix l'annex III, punt 2, ha registrat les proves en condicions reals d'acord amb l'article 49, apartat 5.
- (d) El proveïdor o proveïdor que faci les proves en condicions reals està establert a la Unió o ha designat un representant legal establert a la Unió.
- (e) Les dades recopilades i tractades amb la finalitat de les proves en condicions reals es transfereixen a tercers països només sempre que s'apliquin les salvaguardes apropiades i aplicables segons el dret de la Unió.
- (f) Les proves en condicions reals no duren més del necessari per assolir els seus objectius i en tot cas no més de sis mesos, termini que es pot prorrogar fins a sis mesos més, subjecte a notificació prèvia del proveïdor o proveïdor potencial a l'autoritat de vigilància del mercat, acompanyat d'una explicació de la necessitat d'aquesta ampliació.
- (g) Els subjectes de les proves en condicions reals que siguin persones pertanyents a col·lectius vulnerables per la seva edat o discapacitat, estan degudament protegits.
- (h) Quan un proveïdor o un proveïdor potencial organitza les proves en condicions reals en cooperació amb un o més responsables del desplegament o responsables del desplegament potencials, aquests últims han estat informats de tots els aspectes de les proves que són rellevants per a la seva decisió de participar, i s'han donat les instruccions pertinents per a l'ús del sistema d'IA a què es refereix l'article 13; el proveïdor o el proveïdor potencial i el

responsable del desplegament o el responsable del desplegament potencial han de concloure un acord que especifiqui les seves funcions i responsabilitats amb la finalitat de garantir el compliment de les disposicions per a les proves en condicions reals en virtut del present Reglament i en virtut d'una altra legislació nacional i de la Unió aplicable.

(i) Els subjectes de les proves en condicions reals han donat el consentiment informat de conformitat amb l'article 61 o, en el cas de la garantia del compliment de la llei, quan la recerca del consentiment informat impedeixi que el sistema d'IA es provi, les proves en si i el resultat de les proves en les condicions reals no han de tenir cap efecte negatiu en els subjectes, dels quals se n'han d'eliminar les dades personals després que la prova s'hagi fet.

(j) Les proves en condicions reals se supervisen efectivament pel proveïdor o proveïdor potencial, i també pels responsables del desplegament o els responsables del desplegament potencials a través de persones que estan degudament qualificades en el camp corresponent i tenen la capacitat, la formació i l'autoritat necessàries per dur a terme les seves funcions.

(k) Les prediccions, recomanacions o decisions del sistema d'IA es poden revertir i ignorar de manera efectiva.

5. Qualsevol subjecte de les proves en condicions reals del món, o el seu representant legalment designat, si escau, pot, sense perjudici resultant i sense haver de proporcionar cap justificació, retirar-se de la prova en qualsevol moment revocant el consentiment informat, i pot sol·licitar la supressió immediata i permanent de les seves dades personals. La retirada del consentiment informat no ha d'afectar les activitats ja fetes.

6. D'acord amb l'article 75, els Estats membres confereixen a les seves autoritats de vigilància del mercat la potestat d'exigir als proveïdors i als proveïdors potencials que proporcionin informació, de dur a terme inspeccions remotes o in situ no anunciades i de fer controls sobre la pràctica de les proves en condicions reals i els sistemes d'IA d'alt risc relacionats. Les autoritats de vigilància del mercat han d'utilitzar aquestes competències per garantir el desenvolupament segur de les proves en condicions reals.

7. Qualsevol incident greu identificat en el transcurs de les proves en condicions reals s'ha de comunicar a l'autoritat nacional de vigilància del mercat de conformitat amb l'article 73. El proveïdor o el proveïdor potencial ha d'adoptar mesures de mitigació immediates o, si no pot ser, suspendre les proves en condicions reals del món fins que aquesta mitigació es produeixi o, en cas contrari, cancel·lar-les. El proveïdor o proveïdor potencial ha d'establir un procediment per a la ràpida recuperació del sistema d'IA quan es posi fi a les proves en condicions reals.

8. Els proveïdors o proveïdors potencials han de notificar a l'autoritat nacional de vigilància del mercat en l'Estat membre, quan la prova es faci en condicions reals, de la suspensió o l'acabament de les proves en condicions reals i dels resultats finals.

9. El proveïdor o proveïdor és responsable en virtut de la legislació de la Unió i de la legislació nacional de responsabilitat dels danys causats en el transcurs de les seves proves en condicions reals.

Article 61

Consentiment informat per participar en proves en condicions reals fora dels espais controlats de proves per a la IA

1. A l'efecte de provar en condicions reals d'acord amb l'article 60, s'ha d'obtenir el consentiment dels subjectes de les proves abans que hi participin i després que se'ls hagi informat degudament amb informació concisa, clara, rellevant i comprensible en relació amb:

(a) la naturalesa i els objectius de les proves en condicions reals i les possibles molèsties que puguin estar vinculades a la seva participació;

(b) les condicions en què es faran les proves en condicions reals, inclosa la durada prevista de la participació del subjecte o dels subjectes;

(c) els drets i les garanties en relació amb el fet de participar; en particular, el dret que tenen a negar-se a participar en les proves en condicions reals i el dret a retirar-se'n en qualsevol moment sense que això els perjudiqui ni tinguin l'obligació de justificar-ho;

(d) els procediments per demanar que es reverteixin o no es tinguin en compte les prediccions, recomanacions o decisions del sistema d'IA;

(e) el número d'identificació únic per a tota la Unió Europea de les proves en condicions reals d'acord amb l'article 60, apartat 4, lletra c), i les dades de contacte del proveïdor o del seu representant legal de qui es pot obtenir més informació.

2. El consentiment informat s'ha de datar i documentar i se n'ha de lliurar una còpia als subjectes de prova o al seu representant legal.

Article 62

Mesures dirigides a proveïdors i responsables del desplegament, en particular pimes, incloses les empreses emergents

1. Els Estats membres han d'emprendre les mesures següents:

(a) proporcionar a les pimes, incloses les empreses emergents, que tinguin un domicili social o una sucursal a la Unió un accés prioritari als espais controlats de proves per a la IA, sempre que compleixin les condicions d'admissibilitat i els criteris de selecció; l'accés prioritari no ha d'impedir que altres pimes, incloses les empreses emergents, diferents de les esmentades en el present apartat accedeixin a l'espai controlat de proves per a la IA, sempre que també compleixin les condicions d'admissibilitat i els criteris de selecció;

(b) Organitzar activitats específiques de sensibilització i formació sobre l'aplicació del Reglament adaptades a les necessitats de les pimes, incloses les empreses emergents, els responsables del desplegament i, si escau, les autoritats públiques locals;

(c) han de fer servir canals específics existents i establir, si escau, nous canals per a la comunicació amb les pimes, incloses les empreses emergents, els responsables del desplegament i altres agents innovadors, i també, si escau, les autoritats públiques locals, a fi de proporcionar assessorament i respondre als dubtes plantejats sobre l'aplicació del present Reglament, també en relació amb la participació en els espais controlats de proves per a la IA;

(d) facilitar la participació de les pimes i altres parts interessades rellevants en el procés de desenvolupament de la normalització.

2. Els interessos i necessitats específiques dels proveïdors de pimes, incloses les empreses emergents, s'han de tenir en compte a l'hora d'establir les taxes per a l'avaluació de la conformitat en virtut de l'article 43, reduint-les taxes proporcionalment a les dimensions de les empreses mateixes i del mercat i altres indicadors rellevants.

3. L'Oficina d'IA ha de dur a terme les accions següents:

(a) proporcionar models normalitzats per a les àrees cobertes pel present Reglament, segons especifiqui el Consell en la seva sol·licitud;

(b) desenvolupar i mantenir una única plataforma d'informació que faciliti un ús fàcil de la informació en relació amb el present Reglament per a tots els operadors del conjunt de la Unió;

(c) organitzar campanyes de comunicació adequades per conscienciar sobre les obligacions derivades del Reglament;

(d) avaluar i promoure la convergència de les millors pràctiques en els procediments de contractació pública en relació amb els sistemes d'IA;

Article 63

Exempcions per a operadors específics

1. Les microempreses, en el marc de la Recomanació 2003/361/CE, poden complir certs elements del sistema de gestió de la qualitat exigits per l'article 17 del present Reglament de manera simplificada, sempre que no tinguin empreses associades o empreses vinculades en el sentit d'aquesta recomanació. A aquest efecte, la Comissió ha d'elaborar directrius sobre els elements del sistema de gestió de la qualitat que es puguin complir de manera simplificada tenint en compte les necessitats de les microempreses, sense afectar el nivell de protecció ni la necessitat de complir els requisits respecte dels sistemes d'IA d'alt risc.

2. L'apartat 1 d'aquest article no s'ha d'interpretar com a exempció per als operadors del deure de complir qualsevol altre requisit o obligació del present Reglament, inclosos els establerts en els articles 9, 13, 11, 12, 10, 14, 15, 72 i 73.

CAPÍTOL VII

GOVERNANÇA

SECCIÓ 1

Governança en l'àmbit de la Unió Europea

Article 64

Oficina d'IA

1. A través de l'Oficina d'IA la Comissió acumula experiència i capacitats de la Unió en l'àmbit de la IA.
2. Els estats membres han de facilitar les funcions encomanades a l'Oficina d'IA, tal com es reflecteix en el present Reglament.

Article 65

Creació i estructura del Consell Europeu d'Intel·ligència Artificial

1. Es crea un Consell Europeu d'Intel·ligència Artificial ("Consell").
2. El Consell ha d'estar compost per un representant per cada estat membre. El Supervisor Europeu de Protecció de dades hi ha de participar com a observador. L'Oficina d'IA també assisteix a les reunions del Consell, sense participar en la votació. Segons cada cas, quan les qüestions que es debatin els siguin rellevants, el Consell pot convidar altres autoritats, organismes o experts nacionals i de la Unió a assistir a les reunions.
3. Cada representant ha de ser designat pel seu Estat membre per a un període de tres anys, renovable una vegada.
4. Els Estats membres han de garantir que els seus representants en el Consell compleixin els requisits següents:
 - (a)tenir les competències i competències pertinents en el seu estat membre per contribuir activament a l'assoliment de les funcions del Consell a què es refereix l'article 66;
 - (b)estar designats com a punt de contacte únic amb el Consell i, si escau, tenint en compte les necessitats dels estats membres, com a punt de contacte únic per a les parts interessades;
 - (c)estar facultats per facilitar la coherència i la coordinació entre les autoritats nacionals competents en el seu estat membre pel que fa a l'aplicació del Reglament, fins i tot mitjançant la recollida de dades i informació pertinents amb la finalitat de complir les seves funcions en el Consell.
5. Els representants designats dels estats membres adoptaran el reglament del Consell per majoria de dos terços. El Reglament de procediment ha d'establir, en particular, els

procediments per al procés de selecció, la durada del mandat i les especificacions de les funcions de la presidència, les disposicions detallades per al vot i l'organització de les activitats del Consell i les dels seus subgrups.

6. El Consell ha de crear dos subgrups permanents per proporcionar una plataforma de cooperació i intercanvi entre les autoritats de vigilància del mercat i per notificar a les autoritats qüestions relacionades amb la vigilància del mercat i els organismes notificats respectivament.

El subgrup permanent de vigilància del mercat ha d'actuar com a grup de cooperació administrativa (ADCO) per al present Reglament en el sentit de l'article 30 del Reglament (UE) 2019/1020.

El Consell d'IA pot establir altres subgrups permanents o temporals, segons correspongui, amb la finalitat d'examinar qüestions específiques. Si és el cas, els representants del fòrum consultiu a què es refereix l'article 67 poden ser convidats a aquests subgrups o a reunions específiques d'aquests subgrups com a observadors.

7. La Junta Directiva s'ha d'organitzar i funcionar per salvaguardar l'objectivitat i la imparcialitat de les seves activitats.

8. Ha de presidir el Consell un dels representants dels Estats membres. L'Oficina d'IA facilita la secretaria del Consell, convoca les reunions a petició del president i prepara l'ordre del dia segons les tasques del Consell d'acord amb el present Reglament i la normativa interna pròpia.

Article 66

Funcions del Consell

El Consell ha d'assessorar i assistir la Comissió i els estats membres per facilitar l'aplicació coherent i efectiva del present Reglament. En aquest sentit, i en particular, el Consell pot:

- (a) contribuir a la coordinació entre les autoritats nacionals competents responsables de l'aplicació del present Reglament i, en cooperació amb les autoritats de vigilància del mercat de què es tracti i previ acord d'aquestes, donar suport a les activitats conjuntes de les autoritats de vigilància del mercat a què es refereix l'article 74, apartat 11;
- (b) recollir i compartir els coneixements tècnics i reglamentaris i les millors pràctiques entre els estats membres;
- (c) assessorar sobre l'aplicació del Reglament, en particular pel que fa a l'aplicació de normes sobre models d'IA d'ús general;
- (d) contribuir a l'harmonització de les pràctiques administratives als estats membres, fins i tot en relació amb la derogació dels procediments d'avaluació de la conformitat a què es refereix l'article 46, el funcionament dels espais controlats de proves per a IA i les proves en condicions reals a què es refereixen els articles 57, 59 i 60;

(e) a petició de la Comissió o per iniciativa pròpia, emetre recomanacions i dictàmens escrits sobre qualsevol assumpte rellevant relacionat amb la implantació del present Reglament i la seva aplicació coherent i efectiva, incloent-hi:

(i) sobre el desenvolupament i aplicació de codis de conducta i codis de bones pràctiques de conformitat amb el present Reglament, així com de les directrius de la Comissió;

(ii) sobre l'avaluació i revisió del present Reglament de conformitat amb l'article 112, inclosos els informes d'incidents greus a què es refereix l'article 73, i el funcionament de la base de dades de la UE a què es refereix l'article 71, la preparació dels actes delegats o d'execució, i pel que fa a les possibles alineacions del Reglament amb la legislació d'harmonització de la Unió enumerada a l'annex I;

(iii) Sobre especificacions tècniques o normes existents en relació amb els requisits establerts en el capítol III, secció 2;

(iv) sobre l'ús de normes harmonitzades o especificacions comunes a què es refereixen els articles 40 i 41;

(v) sobre tendències, com la competitivitat global europea en IA, l'adopció de la IA a la Unió Europea i el desenvolupament de capacitats digitals;

(vi) sobre tendències en l'evolució de la tipologia de les cadenes de valor de la IA, en particular sobre les implicacions resultants en termes de rendició de comptes;

(vii) sobre la possible necessitat de modificació de l'annex III, de conformitat amb l'article 7, i sobre la possible necessitat de revisió de l'article 5 de conformitat amb l'article 112, tenint en compte les proves disponibles pertinents i els últims avenços tecnològics;

(f) donar suport a la Comissió en la promoció de l'alfabetització en matèria d'intel·ligència artificial, sensibilització pública i comprensió dels beneficis, riscos, salvaguardes i drets i obligacions en relació amb l'ús dels sistemes d'IA.

(g) facilitar el desenvolupament de criteris comuns i el coneixement compartit entre els operadors del mercat i les autoritats competents dels conceptes pertinents previstos en el present Reglament, fins i tot contribuint al desenvolupament de punts de referència;

- (h) cooperar, si s'escau, amb altres institucions, òrgans i organismes de la Unió, així com amb grups d'experts i xarxes pertinents de la Unió, en particular en els àmbits de la seguretat dels productes, la ciberseguretat, la competència, els serveis digitals i de mitjans de comunicació, els serveis financers, la protecció dels consumidors, i la protecció de dades i dels drets fonamentals;
- (i) contribuir a la cooperació efectiva amb les autoritats competents de tercers països i amb les organitzacions internacionals;
- (j) assistir les autoritats nacionals competents i la Comissió en el desenvolupament de l'experiència organitzativa i tècnica requerida per a l'aplicació del present Reglament, incloent-hi contribuir a l'avaluació de les necessitats de formació del personal dels estats membres implicats en aplicar-lo;
- (k) assistir a l'Oficina d'IA en el suport a les autoritats nacionals competents per a l'establiment i el desenvolupament d'espais controlats de proves per a la IA, i facilitar la cooperació i l'intercanvi d'informació entre espais controlats de proves per a la IA;
- (l) contribuir al desenvolupament de documents d'orientació i aportar-hi assessorament pertinent;
- (m) assessorar la Comissió en relació amb els assumptes internacionals sobre IA;
- (n) emetre dictàmens per a la Comissió sobre les alertes qualificades relatives als models d'IA d'ús general;
- (o) rebre dictàmens dels estats membres sobre alertes qualificades relatives als models d'IA d'ús general i les experiències i pràctiques nacionals sobre el seguiment i l'aplicació dels sistemes d'IA, en particular els sistemes que integren els models d'IA d'ús general.

Article 67

Fòrum consultiu

1. S'ha d'establir un fòrum d'assessorament per proporcionar coneixements tècnics i assessorar el Consell i la Comissió, i per contribuir a les tasques que tenen previstes segons el present Reglament.
2. La pertinença al fòrum consultiu ha de representar una selecció equilibrada de les parts interessades, incloent-hi la indústria, les empreses emergents, les pimes, la societat civil i el món acadèmic. La pertinença al fòrum consultiu ha de ser equilibrada pel que fa als interessos

comercials i no comercials i, en la categoria d'interessos comercials, pel que fa a les pimes i altres empreses.

3. La Comissió ha de nomenar els membres del fòrum consultiu, d'acord amb els criteris establerts en l'apartat 2, d'entre les parts interessades amb reconeguda experiència en l'àmbit de la IA.
4. El termini de mandat dels membres del fòrum consultiu és de dos anys, prorrogable fins a un màxim de quatre anys.
5. L'Agència de Drets fonamentals, ENISA, el Comitè Europeu de Normalització (CEN), el Comitè Europeu de Normalització Electrotècnica (CENELEC) i l'Institut Europeu de normes de Telecomunicacions (ETSI) seran membres permanents del fòrum consultiu.
6. El fòrum consultiu ha d'elaborar un reglament intern propi. Ha d'elegir dos copresidents entre els seus membres, d'acord amb els criteris establerts en l'apartat 2. El termini de mandat dels copresidents és de dos anys, renovables una vegada.
7. El fòrum consultiu ha de convocar reunions com a mínim dues vegades a l'any. El fòrum consultiu pot convidar experts i altres parts interessades a les seves reunions.
8. El fòrum consultiu pot elaborar opinions, recomanacions i contribucions escrites a petició del Consell o de la Comissió.
9. El fòrum consultiu pot establir subgrups permanents o temporals, segons correspongui, amb la finalitat d'examinar qüestions específiques relacionades amb els objectius del present Reglament.
10. El fòrum consultiu ha d'elaborar un informe anual sobre les seves activitats. Aquest informe s'ha de fer públic.

Article 68

Comitè científic d'experts independents

1. La Comissió, mitjançant un acte d'execució, ha d'establir un comitè científic d'experts independents (el "comitè científic") destinat a donar suport a les activitats d'aplicació del Reglament. Aquest acte d'execució s'ha d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.
2. El comitè científic ha d'estar format per experts seleccionats per la Comissió segons l'experiència científica o tècnica actualitzada en l'àmbit de la IA necessària per a les tasques establertes en el paràgraf 3, i ha de poder demostrar que compleix totes les condicions següents:
 - (a) tenir una experiència i competència particulars i experiència científica o tècnica en el camp de la IA;
 - (b) ser independent de qualsevol proveïdor de sistemes d'IA o models d'IA d'ús general;
 - (c) tenir capacitat per dur a terme activitats de manera diligent, precisa i objectiva.

La Comissió, en consulta amb el Consell, ha de determinar el nombre d'experts del comitè d'acord amb les necessitats requerides i garantirà una representació equitativa per gèneres i àmbit geogràfic.

3. El comitè científic assessora i assisteix l'Oficina d'IA, en particular pel que fa a les funcions següents:

(a) donar suport a l'aplicació i el compliment efectiu del present Reglament pel que fa als models i sistemes d'IA d'ús general, en particular, mitjançant:

(i) alertar l'Oficina d'IA de possibles riscos sistèmics en l'àmbit de la Unió de models d'IA d'ús general, de conformitat amb l'article 90;

(ii) contribuir al desenvolupament d'eines i metodologies per avaluar capacitats de models i sistemes d'IA d'ús general, fins i tot a través de paràmetres de referència;

(iii) assessorar sobre la classificació dels models d'IA d'ús general amb risc sistèmic;

(iv) assessorar sobre la classificació de diversos models i sistemes d'IA d'ús general;

(v) contribuir al desenvolupament d'eines i models;

(b) donar suport al treball de les autoritats de vigilància del mercat, a petició seva;

(c) donar suport a les activitats de vigilància transfronterera del mercat, tal com s'esmenta a l'article 74, apartat 11, sense perjudici de les competències de les autoritats de vigilància del mercat.

(d) assistir l'Oficina d'IA perquè exerceixi les funcions pròpies en el context del procediment de salvaguarda de la Unió de conformitat amb l'article 81.

4. Els experts del comitè científic han de fer les seves tasques amb imparcialitat i objectivitat, i han de garantir la confidencialitat de la informació i les dades obtingudes en l'execució de les seves tasques i activitats. No han de buscar ni acceptar instruccions de ningú en l'exercici de les funcions pròpies en virtut de l'apartat 3. Cada expert ha d'elaborar una declaració d'interessos i posar-la a disposició del públic. L'Oficina d'IA ha d'establir sistemes i procediments per gestionar i prevenir de manera activa els possibles conflictes d'interès.

5. L'acte d'execució a què es refereix l'apartat 1 ha d'incloure disposicions sobre condicions, procediments i disposicions detallades per al comitè científic i els seus membres per emetre alertes, i sol·licitar l'assistència de l'Oficina d'IA per a l'acompliment de les funcions del comitè científic.

Article 69

Accés al grup d'experts per part dels estats membres

1. Els estats membres poden demanar als experts del comitè científic que donin suport a les seves activitats de garantia del compliment de la llei en virtut del present Reglament.
2. Es pot exigir als Estats membres que paguin taxes per l'assessorament i el suport prestat pels experts. L'estructura i l'import de les taxes, així com l'escala i l'estructura dels costos recuperables, s'establiran en l'acte d'execució a què es refereix l'article 68, apartat 1, tenint en compte els objectius de la correcta aplicació del present Reglament, la rendibilitat i la necessitat de garantir que tots els Estats membres tinguin un accés efectiu als experts.
3. La Comissió ha de facilitar l'accés oportú dels Estats membres als experts, segons sigui necessari, i garantirà que la combinació de les activitats de suport dutes a terme per les estructures de suport als assaigs d'IA de la Unió d'acord amb l'article 84 i per experts d'acord amb el present article s'organitzi de manera eficient i ofereixi el valor afegit màxim possible.

SECCIÓ 2

Autoritats nacionals competents

Article 70

Designació d'autoritats competents nacionals i punts de contacte únics

1. Cada Estat membre ha d'establir o designar com a autoritats nacionals competents almenys una autoritat notificadora i almenys una autoritat de vigilància del mercat a l'efecte del present Reglament. Les autoritats nacionals competents han d'exercir les seves competències de manera independent, imparcial i sense prejudicis per salvaguardar l'objectivitat de les seves activitats i funcions, i per assegurar l'aplicació i l'aplicació del Reglament. Els membres d'aquestes autoritats s'han d'abstenir de qualsevol acció incompatible amb les seves funcions. Sempre que s'observin aquests principis, aquestes activitats i funcions es poden dur a terme per una o més autoritats designades, d'acord amb les necessitats organitzatives de l'estat membre.
2. Els Estats membres han de comunicar a la Comissió la identitat de les autoritats notificadores i de les autoritats de vigilància del mercat i les funcions d'aquestes autoritats, així com qualsevol canvi posterior que es produeixi. Els estats membres han de posar a disposició del públic informació sobre com es pot contactar amb les autoritats competents i amb els punts de contacte únics, a través de mitjans de comunicació electrònics abans del 2 d'agost de 2025. Els estats membres han de designar una autoritat de vigilància del mercat que actuï com a punt de contacte únic per al present Reglament i notificar-ne la identitat a la Comissió. La Comissió ha de posar a disposició del públic una llista dels punts de contacte únics.
3. Els Estats membres han de vetllar perquè les seves autoritats nacionals competents disposin de recursos tècnics, financers i humans adequats, així com d'infraestructures per al compliment efectiu de les seves funcions en virtut del present Reglament. En particular, les autoritats nacionals competents han de tenir un nombre suficient de personal permanentment disponible, amb competències i coneixements que incloguin una comprensió profunda de tecnologies de la intel·ligència artificial, dades i computació de dades, protecció de dades personals, ciberseguretat, drets fonamentals, riscos per a la salut i la seguretat i coneixement de les normes i requisits legals existents. Els estats membres han d'avaluar i, si escau, actualitzar anualment els requisits de competència i recursos a què es refereix aquest apartat.

4. Les autoritats nacionals competents han de prendre les mesures adequades per garantir un nivell adequat de ciberseguretat.
5. En exercir les seves funcions, les autoritats nacionals competents han d'actuar d'acord amb les obligacions de confidencialitat establertes en l'article 78.
6. Abans del 2 d'agost de 2025, i una vegada cada dos anys a partir d'aleshores, els estats membres han d'informar la Comissió sobre l'estat dels recursos financers i humans de les autoritats nacionals competents, avaluant-ne la idoneïtat. La Comissió ha de transmetre la informació al Consell perquè la debati i emeti les possibles recomanacions.
7. La Comissió ha de facilitar l'intercanvi d'experiències entre les autoritats nacionals competents.
8. Les autoritats nacionals competents poden assessorar i orientar sobre l'aplicació del Reglament, en particular a les pimes, incloses les empreses emergents, tenint en compte les orientacions i l'assessorament del Consell i de la Comissió, segons correspongui. Sempre que vulguin proporcionar orientació i assessorament sobre un sistema d'IA en les àrees cobertes pel dret d'una altra Unió, les autoritats nacionals competents d'acord amb aquest dret de la Unió s'han de consultar, segons correspongui.
9. Quan les institucions, organismes, oficines o òrgans de la Unió es troben en l'àmbit d'aplicació del Reglament, el Supervisor Europeu de Protecció de dades ha d'actuar com a autoritat competent per supervisar-los.

CAPÍTOL VIII

BASE DE DADES DE LA UE PER A SISTEMES D'IA D'ALT RISC

Article 71

Base de dades de la UE per a sistemes d'IA d'alt risc que figuren a l'annex III

1. La Comissió, en col·laboració amb els Estats membres, ha de crear i mantenir una base de dades de la UE que contingui la informació esmentada en els apartats 2 i 3 del present article en relació amb els sistemes d'IA d'alt risc a què es refereix l'article 6, apartat 2, que estiguin registrats d'acord amb els articles 49 i 60, i els sistemes d'IA que no es considerin d'alt risc en virtut de l'article 6, apartat 3, i que estiguin registrats d'acord amb l'article 6, apartat 4, i l'article 49. En establir les especificacions funcionals d'aquesta base de dades, la Comissió ha de consultar els experts pertinents i, en actualitzar les especificacions funcionals d'aquesta base de dades, la Comissió ha de consultar el Consell.
2. Les dades que figuren a l'annex VIII, seccions A i B, s'han d'incorporar a la base de dades de la UE pel proveïdor o, si escau, pel representant autoritzat.
3. Les dades que figuren a l'annex VIII, secció C, s'han d'incorporar a la base de dades de la UE pel responsable del desplegament que sigui autoritat, organisme o òrgan, o que actuï en nom seu, d'acord amb l'article 49, apartats 3 i 4.
4. A excepció de la secció a què es refereixen l'article 49, apartat 4, i l'article 60, apartat 4, lletra c), la informació continguda en la base de dades de la UE registrada de conformitat amb l'article 49 ha de ser accessible, estar disponible per al públic i ser d'ús fàcil. La informació ha de ser fàcilment navegable i llegible per màquina. La informació registrada de conformitat amb

l'article 60 només serà ha de ser accessible a les autoritats de vigilància del mercat i la Comissió, llevat que el proveïdor o proveïdor potencial hagi consentit que es faci accessible al públic.

5. La base de dades de la UE només ha de contenir dades personals en la mesura que aquestes siguin necessàries per a la recollida i el tractament de la informació de conformitat amb el present Reglament. Aquesta informació ha d'incloure els noms i les dades de contacte de les persones físiques que siguin responsables de registrar el sistema i que tinguin l'autoritat legal per representar el proveïdor o el responsable del desplegament, segons correspongui.

6. La Comissió és la responsable de la base de dades de la UE. Ha de posar a disposició dels proveïdors, proveïdors potencials i responsables del desplegament una assistència tècnica i administrativa adequada. La base de dades de la UE ha de complir els requisits d'accessibilitat aplicables.

CAPÍTOL IX

SEGUIMENT POSTCOMERCIALIZACIÓ, INTERCANVI D'INFORMACIÓ I VIGILÀNCIA DEL MERCAT

SECCIÓ 1

Seguiment postcomercialització

Article 72

Seguiment postcomercialització per part de proveïdors i pla de seguiment postcomercialització per a sistemes d'IA d'alt risc

1. Els proveïdors han d'establir i documentar un sistema de seguiment postcomercialització de manera proporcional a la naturalesa de les tecnologies d'IA i als riscos del sistema d'IA d'alt risc.

2. El sistema de seguiment postcomercialització ha de recopilar, documentar i analitzar de manera activa i sistemàtica les dades rellevants que puguin proporcionar els responsables del desplegament o que es puguin recollir per altres fonts sobre el rendiment dels sistemes d'IA d'alt risc al llarg de la seva vida i que permetin al proveïdor avaluar el compliment continu pels sistemes d'IA dels requisits establerts al capítol III, secció 2. Quan sigui rellevant, el seguiment de postcomercialització ha d'incloure una anàlisi de la interacció amb altres sistemes d'IA. L'obligació no cobreix les dades operatives sensibles dels responsables del desplegament que són autoritats garants del compliment de la llei.

3. El sistema de seguiment postcomercialització s'ha de basar en un pla de seguiment postcomercialització. El pla de seguiment postcomercialització ha de formar part de la documentació tècnica a què es refereix l'annex IV. La Comissió ha d'adoptar una llei d'execució que estableixi les disposicions detallades que constitueixen un model per al pla de seguiment postcomercialització i la llista d'elements que s'han d'incloure en el pla abans del 2 de febrer de 2026. Aquest acte d'execució s'ha d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

4. Per a sistemes d'IA d'alt risc previstos en la legislació d'harmonització de la Unió enumerada a l'annex I, secció A, quan ja hi hagi establerts en la legislació esmentada un sistema i un pla de seguiment postcomercialització, per assegurar la coherència, evitar duplicacions i minimitzar les càrregues addicionals, els proveïdors han de tenir l'oportunitat d'integrar, segons correspongui, els elements necessaris que es descriuen als apartats 1, 2 i 3, fent servir el model que s'esmenta

a l'apartat 3, en els sistemes i plans que ja hi ha segons la legislació esmentada, sempre que el nivell de protecció que s'assoleixi sigui equivalent.

El primer apartat d'aquest apartat també s'aplica als sistemes d'IA d'alt risc a què es refereix l'annex III, punt 5, introduïts en el mercat o posats en servei per les entitats financeres que estiguin subjectes als requisits exigits per la legislació de serveis financers de la Unió en relació amb la governança interna, els sistemes o els processos.

SECCIÓ 2

Compartir informació sobre incidents greus

Article 73

Informar d'incidències greus

1. Els proveïdors de sistemes d'IA d'alt risc introduïts en el mercat de la Unió han d'informar de qualsevol incident greu a les autoritats de vigilància del mercat dels estats membres on s'hagi produït aquest incident.

2. L'informe a què es refereix l'apartat 1 s'ha de fer immediatament després que el proveïdor hagi establert un vincle causal entre el sistema d'IA i l'incident greu o la probabilitat raonable d'aquest vincle i, en tot cas, sense que hagin passat més de quinze dies després que el proveïdor o, si escau, el responsable del desplegament, tingui coneixement de la incidència greu.

El termini per a la presentació de la denúncia a què es refereix el subapartat primer ha de tenir en compte la gravetat de la incidència greu.

3. No obstant l'apartat 2 d'aquest article, en cas d'infracció generalitzada o incident greu tal com es defineix en l'article 3, apartat 49, lletra b), l'informe a què es refereix l'apartat 1 d'aquest article s'ha de proporcionar immediatament o, a tot tardar, dos dies després que el proveïdor o, si escau, el responsable del desplegament en tingui coneixement.

4. Sense perjudici de l'apartat 2, en el cas que una persona mori, l'informe s'ha de proporcionar així que el proveïdor o el responsable del desplegament determini o sospiti que hi ha una relació causal entre el sistema d'IA d'alt risc i la incidència greu, sense que en cap cas puguin passar més de deu dies a partir de la data en què el proveïdor o, si és el cas, el responsable del desplegament en tingui coneixement.

5. Quan sigui necessari per garantir la informació oportuna, el proveïdor o, si escau, el responsable del desplegament, pot presentar un informe inicial que sigui incomplet, seguit d'un informe complet.

6. Després de la notificació d'un incident greu, de conformitat amb l'apartat 1, el proveïdor ha de fer, immediatament, les investigacions necessàries en relació amb el greu incident i el sistema d'IA en qüestió. Això inclou una avaluació del risc de la incidència i una acció correctora.

El proveïdor ha de cooperar amb les autoritats competents, i si escau amb l'organisme notificat interessat, durant les investigacions a què es refereix el subapartat primer, sense fer cap investigació que impliqui alterar el sistema d'IA en qüestió de manera que pugui afectar qualsevol avaluació posterior de les causes de l'incident, abans d'informar-ne les autoritats competents.

7. En rebre una notificació relacionada amb un incident greu a què es refereix l'article 3, apartat 49, lletra c), l'autoritat de vigilància del mercat pertinent ha d'informar les autoritats públiques nacionals o els organismes a què es refereix l'article 77, apartat 1). La Comissió ha de desenvolupar orientacions dedicades a facilitar el compliment de les obligacions establertes en l'apartat 1 d'aquest article. Aquesta orientació s'ha d'haver emès el 2 d'agost de 2025 i requereix avaluació amb regularitat.

8. L'autoritat de vigilància del mercat ha de prendre les mesures apropiades, segons el que disposa l'article 19 del Reglament (UE) 2019/1020, en el termini de set dies des de la data en què va rebre la notificació a què es refereix l'apartat 1 d'aquest article, i seguir els procediments de notificació previstos en el present Reglament.

9. Per als sistemes d'IA d'alt risc a què es refereix l'annex III que s'introdueixen en el mercat o es posen en servei per proveïdors subjectes a instruments legislatius de la Unió que estableixen obligacions d'informació equivalents a les establertes en el present Reglament, la notificació d'incidents greus s'ha de limitar a les que s'esmenten a l'article 3, apartat 49, lletra c).

10. Per als sistemes d'IA d'alt risc que són components de seguretat dels dispositius, o són ells mateixos dispositius, coberts pels Reglaments (UE) 2017/745 i (UE) 2017/746, la notificació d'incidents greus s'ha de limitar als esmentats en l'article 3, apartat 49, lletra c), del Reglament, i s'ha de fer a l'autoritat nacional competent escollida a aquest efecte pels estats membres quan s'hagi produït l'incident.

11. Les autoritats nacionals competents han de notificar immediatament a la Comissió qualsevol incident greu, amb independència de si hi ha pres mesures o no n'ha pres, de conformitat amb l'article 20 del Reglament (UE) 2019/1020.

SECCIÓ 3

Garantia del compliment

Article 74

Vigilància del mercat i control dels sistemes d'IA en el mercat de la Unió

1. El Reglament (UE) 2019/1020 s'ha d'aplicar als sistemes d'IA que aquest Reglament contempla. A efectes de l'aplicació efectiva del Reglament s'ha d'entendre el següent:

(a) Tota referència a un operador econòmic d'acord amb el Reglament (UE) 2019/1020 inclou tots els operadors esmentats a l'article 2, apartat 1, del present Reglament.

(b) Tota referència a un producte d'acord amb el Reglament (UE) 2019/1020 inclou tots els sistemes d'IA que estiguin compresos en l'àmbit d'aplicació del present Reglament.

2. Com a part de les seves obligacions d'informació en virtut de l'article 34, apartat 4, del Reglament (UE) 2019/1020, les autoritats de vigilància del mercat han d'informar anualment la Comissió i les autoritats nacionals competents de qualsevol informació identificada en el curs de les activitats de vigilància del mercat que puguin ser d'interès potencial per a la garantia del compliment de la legislació de la Unió en matèria de competència. També han d'informar anualment la Comissió sobre l'ús de les pràctiques prohibides esdevingudes durant l'any i sobre les mesures adoptades.

3. Per als sistemes d'IA d'alt risc relacionats amb els productes coberts per la legislació d'harmonització de la Unió enumerada a l'annex I, secció A, l'autoritat de vigilància del mercat a l'efecte del present Reglament és l'autoritat responsable de les activitats de vigilància del mercat designades en virtut d'aquests actes legislatius.

Per excepció del subapartat primer, i en les circumstàncies apropiades, els estats membres poden designar una altra autoritat pertinent perquè actuï com a autoritat de vigilància del mercat, sempre que garanteixin la coordinació amb les autoritats de vigilància del mercat sectorial pertinents responsables de l'aplicació de la legislació d'harmonització de la Unió enumerada a l'annex I.

4. Els procediments a què es refereixen els articles 79 a 83 del Reglament no s'apliquen als sistemes d'IA relacionats amb els productes coberts per la legislació d'harmonització de la Unió enumerada a l'annex I, secció A, quan aquests actes legislatius ja preveuen procediments que garanteixin un nivell de protecció equivalent i amb el mateix objectiu. En aquests casos, s'han d'aplicar els procediments sectorials pertinents.

5. Sense perjudici de les competències de les autoritats de vigilància del mercat en virtut de l'article 14 del Reglament (UE) 2019 4/1020, amb la finalitat de garantir l'aplicació efectiva del Reglament, les autoritats de vigilància del mercat poden exercir les competències a què es refereix l'article 14, lletres d) i j), del Reglament de forma remota, segons correspongui.

6. Per als sistemes d'IA d'alt risc introduïts en el mercat, posats en servei o emprats per les entitats financeres regulades per la legislació de serveis financers de la Unió, a l'efecte del Reglament, l'autoritat de vigilància del mercat és l'autoritat nacional competent per a la supervisió financera de les entitats subjectes a aquesta legislació en la mesura que la introducció en el mercat, la posada en servei, o l'ús del sistema d'IA estiguin directament relacionats amb la prestació dels serveis financers esmentats.

7. Per exempció de l'apartat 6, en circumstàncies apropiades, i sempre que es garanteixi la coordinació, l'Estat membre pot identificar una altra autoritat pertinent com a autoritat de vigilància del mercat a l'efecte del Reglament.

Les autoritats nacionals de vigilància del mercat que supervisen les entitats de crèdit regulades en virtut de la Directiva 2013/36/UE, que participen en el mecanisme únic de supervisió establert pel Reglament (UE) 1024/2013, han de traslladar, sense demora, al Banc Central Europeu tota la informació identificada en el curs de les seves activitats de vigilància del mercat que pugui ser d'interès potencial per a les funcions de supervisió prudencial del Banc Central Europeu especificades en el Reglament.

8. Per als sistemes d'IA d'alt risc que figuren en l'annex III, punt 1, del present Reglament, en la mesura que els sistemes s'utilitzen per a garantia del compliment de la llei, gestió de fronteres i justícia i democràcia, i per als sistemes d'IA d'alt risc que figuren en l'annex III, punts 6, 7 i 8, del present Reglament, els estats membres han de designar com a autoritats de vigilància del mercat a l'efecte del Reglament mateix, les autoritats competents de control de protecció de dades en virtut del Reglament (UE) 2016/679 o la Directiva (UE) 2016/680, o qualsevol altra autoritat designada de conformitat amb les mateixes condicions establertes en els articles 41 a 44 de la Directiva (UE) 2016/680. Les activitats de vigilància del mercat no han d'afectar de cap manera la independència de les autoritats judicials, ni interferir de cap altra manera en les seves activitats quan actuïn en la capacitat judicial.

9. Quan les institucions, organismes, oficines o òrgans de la Unió són en l'àmbit d'aplicació del Reglament, el Supervisor Europeu de Protecció de dades ha d'actuar com a autoritat de vigilància del mercat, excepte en relació amb el Tribunal de Justícia de la Unió Europea que actuï en la capacitat judicial.

10. Els Estats membres han de facilitar la coordinació entre les autoritats de vigilància del mercat designades en virtut del present Reglament i altres autoritats o organismes nacionals pertinents que supervisen l'aplicació de la legislació d'harmonització de la Unió enumerada a l'annex I, o en altres lleis de la Unió, que puguin ser rellevants per als sistemes d'IA d'alt risc esmentats a l'annex III.

11. Les autoritats de vigilància del mercat i la Comissió han de poder proposar activitats conjuntes, entre les quals les investigacions, que s'han de dur a terme per les autoritats de vigilància del mercat o per aquestes juntament amb la Comissió, que tinguin per objectiu promoure el compliment, identificar l'incompliment, conscienciar o proporcionar orientació en relació amb aquest Reglament pel que fa a categories específiques de sistemes d'IA d'alt risc de les quals es considera que representen un risc greu en dos o més estats membres segons l'article 9 del Reglament (UE) 2019/1020. L'Oficina d'IA ha de contribuir amb coordinació en les investigacions conjuntes.

12. Sense perjudici dels poders previstos en el Reglament (UE) 2019/1020, i quan procedeixi i es limiti al necessari per a l'acompliment de les seves funcions, els proveïdors han de concedir a les autoritats de vigilància del mercat ple accés a la documentació, així com als conjunts de dades d'entrenament, validació i prova utilitzats per al desenvolupament dels sistemes d'IA d'alt risc; també, quan escaigui i amb subjecció a garanties de seguretat, a través d'interfícies de programació d'aplicacions (API) o d'altres eines i mitjans tècnics pertinents que permetin l'accés a distància.

13. Les autoritats de vigilància del mercat han de tenir accés al codi font del sistema d'IA d'alt risc a petició motivada i només quan es compleixin les dues condicions següents:

(a) l'accés al codi font és necessari per avaluar la conformitat d'un sistema d'IA d'alt risc amb els requisits establerts en el capítol III, Secció 2; i

(b) Els procediments i verificacions de prova o auditoria basats en les dades i la documentació aportada pel proveïdor s'han esgotat o s'han demostrat insuficients.

14. Tota la informació o documentació obtinguda per les autoritats de vigilància del mercat es tracta d'acord amb les obligacions de confidencialitat establertes a l'article 78.

Article 75

Assistència mútua, vigilància del mercat i control de sistemes d'IA d'ús general

1. Quan un sistema d'IA es basa en un model d'IA d'ús general, i el model i el sistema s'han desenvolupat pel mateix proveïdor, l'Oficina d'IA té facultats per vigilar i supervisar que el sistema d'IA compleixi les obligacions que li corresponen en virtut del Reglament. Per dur a terme les funcions de seguiment i supervisió, l'Oficina d'IA ha de tenir totes les competències d'una autoritat de vigilància del mercat prevista en aquesta secció i el Reglament (UE) 2019/1020.

2. Quan tinguin raons suficients per considerar sistemes d'IA d'ús general que els responsables del desplegament puguin fer servir directament amb almenys una finalitat que es consideri d'alt risc d'acord amb el Reglament per no complir els requisits que s'hi estableixen, les autoritats pertinents de vigilància del mercat han de cooperar amb l'Oficina d'IA per dur a terme avaluacions de compliment, i n'han d'informar el Consell i altres autoritats de vigilància del mercat en consonància.

3. Quan no pugui concloure la investigació sobre el sistema d'IA d'alt risc per la incapacitat d'accedir a certa informació relacionada amb el model d'IA d'ús general tot i haver fet tots els esforços adequats per obtenir-la, l'autoritat de vigilància del mercat pot presentar una sol·licitud raonada a l'Oficina d'IA i, per mitjà de la sol·licitud, obtindrà accés a la informació. En aquest cas, en un termini de trenta dies, l'Oficina d'IA ha de facilitar sense demora a l'autoritat sol·licitant tota la informació que l'Oficina d'IA consideri pertinent per determinar si un sistema d'IA d'alt risc no compleix. Les autoritats de vigilància del mercat vetllen per la confidencialitat de la informació que obtenen de conformitat amb l'article 78 del Reglament. El procediment previst en el capítol VI del Reglament (UE) 2019/1020 s'ha d'aplicar mutatis mutandis.

Article 76

Supervisió de proves en condicions reals per part de les autoritats de vigilància del mercat

1. Les autoritats de vigilància del mercat han de tenir competències i poders per garantir que les proves en condicions reals siguin conformes amb el Reglament.

2. Quan es facin proves en condicions reals de sistemes d'IA supervisades dins d'un espai controlat de proves per a la IA d'acord amb l'article 58, les autoritats de vigilància del mercat han de verificar el compliment de l'article 60 com a part de la seva funció supervisora en l'espai controlat de proves per a la IA. Si correspon, aquestes autoritats poden permetre que les proves en condicions reals es facin pel proveïdor o proveïdor potencial, com a excepció a les condicions establertes a l'article 60, apartat 4, lletres f) i g).

3. Quan el proveïdor potencial, el proveïdor o un tercer l'hagin informada d'un incident greu o tingui altres motius per considerar que no es compleixen les condicions previstes als articles 60 i 61, l'autoritat de vigilància del mercat pot adoptar al seu territori, segons correspongui, alguna de les decisions següents:

(a) Interrompre o posar fi a les proves en condicions reals.

(b) Exigir al proveïdor o al proveïdor potencial i al responsable del desplegament o al responsable del desplegament potencial que modifiquin qualsevol aspecte de les proves en condicions reals.

4. Quan una autoritat de vigilància del mercat hagi pres una decisió a què es refereix aquest article, apartat 3, o hagi emès una objecció en el sentit de l'article 60, apartat 4, lletra b), en la decisió o l'objecció cal indicar els motius i la forma en què el proveïdor o proveïdor potencial pot impugnar la decisió o l'objecció.

5. Quan hagi pres una decisió a què es refereix l'apartat 3, l'autoritat de vigilància del mercat ha de comunicar les raons que la justifiquen a les autoritats de vigilància del mercat d'altres estats membres on el sistema d'IA ha estat provat d'acord amb el pla de proves.

Article 77

Poders de les autoritats que protegeixen els drets fonamentals

1. Les autoritats o organismes públics nacionals encarregats de supervisar o fer respectar les obligacions contemplades en el dret de la Unió en matèria de protecció dels drets fonamentals, inclòs el dret a la no discriminació, pel que fa a l'ús de sistemes d'IA d'alt risc esmentats a l'annex III han de tenir la facultat de demanar qualsevol documentació creada o conservada d'acord amb el present Reglament i d'accedir-hi, en un llenguatge i format accessibles, quan l'accés a aquesta documentació sigui necessari per al compliment efectiu dels seus mandats, dins els límits de la seva jurisdicció. L'autoritat o organisme públic competent ha d'informar l'autoritat de vigilància del mercat de l'estat membre interessat de qualsevol sol·licitud.
2. A partir del 2 de novembre de 2024, cada estat membre ha d'identificar les autoritats o organismes públics a què es refereix l'apartat 1 i publicar-ne una llista. Els estats membres han de notificar la llista a la Comissió i als altres estats membres i mantenir la llista actualitzada.
3. Quan la documentació a què es refereix l'apartat 1 sigui insuficient per determinar si s'ha produït una infracció de les obligacions derivades del dret de la Unió en matèria de protecció dels drets fonamentals, l'autoritat pública o l'organisme a què es refereix l'apartat 1 pot sol·licitar raonadament a l'autoritat de vigilància del mercat, per a l'organització de les proves del sistema d'IA d'alt risc a través de mitjans tècnics. L'autoritat de vigilància del mercat ha d'organitzar les proves amb la participació estreta de l'autoritat o organisme públic sol·licitant en un termini raonable després de la sol·licitud.
4. Qualsevol informació o documentació obtinguda per les autoritats o organismes públics nacionals a què es refereix l'apartat 1 del present article, d'acord amb aquest mateix, s'ha de tractar de conformitat amb les obligacions de confidencialitat de l'article 78.

Article 78

Confidencialitat

1. La Comissió, les autoritats de vigilància del mercat, els organismes notificats i qualsevol altra persona física o jurídica que participi en l'aplicació del present Reglament, de conformitat amb el Dret de la Unió o nacional, han de respectar la confidencialitat de la informació i les dades obtingudes en l'exercici de les seves funcions i activitats de manera que es protegeixin, en particular:
 - (a) els drets de propietat intel·lectual i la informació comercial confidencial o secrets comercials d'una persona física o jurídica, inclòs el codi font, excepte en els casos a què es refereix l'article 5 de la Directiva (UE) 2016/943 del Parlament Europeu i del Consell [\(57\)](#);
 - (b) l'aplicació efectiva del present Reglament, en particular a efectes d'inspeccions, investigacions o auditories;
 - (c) interessos de seguretat pública i nacional;

(d) el desenvolupament de les causes penals o els procediments administratius;

(e) la informació classificada d'acord amb el Dret de la Unió o nacional.

2. Les autoritats involucrades en l'aplicació del present Reglament de conformitat amb l'apartat 1 només han de sol·licitar les dades que siguin estrictament necessàries per a l'avaluació del risc que presenten els sistemes d'IA i per a l'exercici de les seves competències de conformitat amb el present Reglament i amb el Reglament (UE) 2019/1020. Han d'establir mesures adequades i eficaces en matèria de ciberseguretat a fi de protegir la seguretat i la confidencialitat de la informació i les dades obtingudes, i suprimir les dades recopilades tan aviat com deixin de ser necessàries per a les finalitats per a les quals es van obtenir, de conformitat amb el dret de la Unió i nacional aplicable.

3. Sense perjudici dels apartats 1 i 2, la informació intercanviada de manera confidencial entre les autoritats nacionals competents o entre les autoritats nacionals competents i la Comissió no s'ha de revelar sense consulta prèvia de l'autoritat nacional competent originària i del responsable del desplegament quan els sistemes d'IA d'alt risc a què es refereix l'annex III; punts 1, 6 o 7, es fan servir per les autoritats de garantia del compliment de la llei, de control de fronteres, d'immigració o d'asil i quan aquesta divulgació posi en perill els interessos públics i de seguretat nacional. Aquest intercanvi d'informació no ha de cobrir dades operatives sensibles en relació amb les activitats de les autoritats garants del compliment de la llei, de control de fronteres, d'immigració o d'asil.

Quan les autoritats garants del compliment de la llei, d'immigració o d'asil siguin proveïdores de sistemes d'IA d'alt risc esmentat a l'annex III, punts 1, 6 o 7, la documentació tècnica a què es refereix l'annex IV ha de romandre dins les instal·lacions d'aquestes autoritats. Aquestes autoritats han de vetllar perquè les autoritats de vigilància del mercat a què es refereix l'article 74, apartats 8 i 9, segons escaigui, puguin, prèvia sol·licitud, accedir immediatament a la documentació o obtenir-ne una còpia. Només el personal de l'autoritat de vigilància del mercat que tingui el nivell adequat de seguretat ha de poder accedir a aquesta documentació o a qualsevol còpia d'aquesta.

4. Els apartats 1, 2 i 3 no han d'afectar els drets o obligacions de la Comissió, els Estats membres i les seves autoritats pertinents, ni els drets o obligacions dels organismes notificats pel que fa a l'intercanvi d'informació i la difusió d'avertiments, també en el context de la cooperació transfronterera, ni les obligacions de facilitar informació en virtut del dret penal dels Estats membres que incumbeixin a les parts interessades.

5. Quan sigui necessari i d'acord amb les disposicions pertinents dels acords internacionals i comercials, la Comissió i els Estats membres poden intercanviar informació confidencial amb autoritats reguladores de tercers països amb les quals hagin celebrat acords de confidencialitat bilaterals o multilaterals que garanteixin un nivell de confidencialitat adequat.

Article 79

Procediment aplicable a escala nacional als sistemes d'IA que presentin un risc

1. Els sistemes d'IA que presentin un risc s'han de considerar "producte que presenta un risc", tal com es defineix a l'article 3, apartat 19, del Reglament (UE) 2019/1020, en la mesura que presentin riscos per a la salut o la seguretat, o per als drets fonamentals de les persones.

2. Quan tingui motius suficients per considerar que un sistema d'IA presenta un risc esmentat a l'apartat 1 del present article, l'autoritat de vigilància del mercat d'un Estat membre ha d'avaluar el sistema d'IA de què es tracti per verificar-ne el compliment de tots els requisits i obligacions establerts en el present Reglament. S'ha de prestar especial atenció als sistemes d'IA que presentin un risc per als grups vulnerables. Quan es detectin riscos per als drets fonamentals, l'autoritat de vigilància del mercat n'ha d'informar també les autoritats o organismes públics nacionals pertinents a què es refereix l'article 77, apartat 1, i cooperar-hi plenament. Els operadors pertinents han de cooperar, segons sigui necessari, amb l'autoritat de vigilància del mercat i amb les altres autoritats o organismes públics nacionals a què es refereix l'article 77, apartat 1.

Quan, en el transcurs d'aquesta avaluació, consideri que el sistema d'IA no compleix els requisits i obligacions establerts en el Reglament, l'autoritat de vigilància del mercat o, si escau, l'autoritat de vigilància del mercat en cooperació amb l'autoritat pública nacional a què es refereix l'article 77, apartat 1, ha de requerir, sense dilació indeguda, a l'operador corresponent que adopti totes les accions correctores perquè el sistema d'IA compleixi, per retirar-lo del mercat o per recuperar-lo en el termini que l'autoritat de vigilància del mercat determini, sense que en cap cas puguin passar més de quinze dies o un altre termini que la legislació d'harmonització de la Unió corresponent estableixi.

L'autoritat de vigilància del mercat ha d'informar l'organisme notificat corresponent. L'article 18 del Reglament (UE) 2019/1020 s'ha d'aplicar a les mesures a què es refereix el paràgraf segon d'aquest apartat.

3. Quan consideri que l'incompliment no es limita al seu territori nacional, l'autoritat de vigilància del mercat ha d'informar la Comissió i els altres Estats membres sense demora indeguda dels resultats de l'avaluació i de les accions que ha requerit l'operador.

4. L'operador ha d'assegurar que es prenen totes les mesures correctores apropiades respecte de tots els sistemes d'IA afectats que ha posat a disposició en el mercat de la Unió.

5. Quan l'operador d'un sistema d'IA no adopti les mesures correctores adequades en el període a què es refereix l'apartat 2, l'autoritat de vigilància del mercat ha d'aplicar totes les mesures provisionals apropiades per prohibir o restringir la posada a disposició del sistema d'IA en el seu mercat nacional o posar-lo en funcionament, retirar el producte o el sistema d'IA independent d'aquest mercat o recuperar-lo. Aquesta autoritat ha de notificar les mesures, sense dilació indeguda, a la Comissió i als altres estats membres.

6. La notificació a què es refereix l'apartat 5 ha d'incloure totes les dades disponibles; en particular, la informació necessària per a la identificació del sistema d'IA no compatible, l'origen del sistema d'IA i de la cadena de subministrament, la naturalesa de l'incompliment al·legat i el risc implicat, la naturalesa i durada de les mesures nacionals adoptades i els arguments proposats per l'operador corresponent. En particular, les autoritats de vigilància del mercat han d'indicar si l'incompliment es deu a un o més dels fets següents:

(a) l'incompliment de la prohibició de les pràctiques d'IA a què es refereix l'article 5;

(b) Una fallada d'un sistema d'IA d'alt risc per complir els requisits establerts en el capítol III, secció 2;

(c) deficiències en les normes harmonitzades o especificacions comunes a què es refereix l'article 40 i 41 que confereixen una presumpció de conformitat;

(d) incompliment de l'article 50.

7. Les autoritats de vigilància del mercat diferents de l'autoritat de vigilància del mercat de l'Estat membre que va iniciar el procediment han de comunicar sense demora indeguda a la Comissió i als altres Estats membres tota mesura que adoptin i qualsevol informació addicional de què disposin en relació amb la no conformitat del sistema d'IA de què es tracti i, en cas de desacord amb la mesura nacional notificada, les objeccions que hi tenen.

8. Si, en el termini de tres mesos des de la recepció de la notificació esmentada a l'apartat 5 del present article, cap autoritat de vigilància del mercat d'un Estat membre ni la Comissió presenten cap objecció sobre una mesura provisional adoptada per una autoritat de vigilància del mercat d'un altre Estat membre, la mesura s'ha de considerar justificada. Això s'ha d'entendre sense perjudici dels drets processals de l'operador interessat, de conformitat amb l'article 18 del Reglament (UE) 2019/1020. El termini de tres mesos a què es refereix aquest apartat es redueix a trenta dies en cas d'incompliment de la prohibició de les pràctiques d'IA a què es refereix l'article 5 del present Reglament.

9. Les autoritats de vigilància del mercat han de garantir que es prenguin les mesures restrictives adequades pel que fa al producte o al sistema d'IA en qüestió, com ara la retirada del producte o del sistema d'IA del seu mercat, sense demora indeguda.

Article 80

Procediment aplicable als sistemes d'IA classificats pel proveïdor com a no d'alt risc en aplicació de l'annex III

1. Quan una autoritat de vigilància del mercat tingui motius suficients per considerar que un sistema d'IA que el proveïdor ha classificat com a no d'alt risc d'acord amb l'article 6, apartat 3, sí que ho és, l'esmentada autoritat ha d'avaluar el sistema d'IA de què es tracti pel que fa a la classificació com a sistema d'IA d'alt risc en funció de les condicions establertes a l'article 6, apartat 3, i les directrius de la Comissió.

2. Quan, en el transcurs d'aquesta avaluació, trobi que el sistema d'IA en qüestió és d'alt risc, l'autoritat de vigilància del mercat ha de requerir sense dilació indeguda que el proveïdor pertinent prengui totes les accions necessàries per fer que el sistema d'IA compleixi els requisits i obligacions establerts en el Reglament, i prengui les mesures correctores adequades en un termini que l'autoritat de vigilància del mercat pugui prescriure.

3. Quan consideri que l'ús del sistema d'IA en qüestió no es limita al seu territori nacional, l'autoritat de vigilància del mercat ha d'informar sense demora la Comissió i els altres Estats membres dels resultats de l'avaluació i de les accions que ha requerit que el proveïdor prengui.

4. El proveïdor ha de garantir que es prenen totes les mesures necessàries per fer que el sistema d'IA compleixi els requisits i obligacions establerts en el present Reglament. Quan no compleixi amb aquests requisits i obligacions en el termini previst en l'apartat 2 d'aquest article, el proveïdor del sistema d'IA de què es tracti estarà subjecte a multes d'acord amb l'article 99.

5. El proveïdor ha de garantir que es prenen totes les mesures correctores apropiades respecte de tots els sistemes de IA afectats que ha posat a disposició en el mercat de la Unió.
6. Quan el proveïdor del sistema de IA en qüestió no prengui les mesures correctores adequades en el termini previst en l'apartat 2 d'aquest article, s'aplicarà l'article 79, apartat 5 a 9.
7. Quan, en el transcurs de l'avaluació de conformitat amb l'apartat 1 d'aquest article, l'autoritat de vigilància del mercat estableix que el sistema d'IA va ser classificat pel proveïdor com a no alt risc per eludir l'aplicació dels requisits en el capítol III, secció 2, el proveïdor podrà ser multat d'acord amb l'article 99.
8. En l'exercici de la potestat per controlar l'aplicació d'aquest article, i d'acord amb l'article 11 del Reglament (UE) 2019/1020, les autoritats de vigilància del mercat poden fer controls apropiats, tenint en compte en particular la informació emmagatzemada a la base de dades de la UE a què es refereix l'article 71 del Reglament.

Article 81

Procediment de salvaguarda de la Unió

1. Quan, en el termini de tres mesos des de la recepció de la notificació a què es refereix l'article 79, apartat 5, o en el termini de trenta dies en el cas d'incompliment de la prohibició de les pràctiques d'IA a què es refereix l'article 5, l'autoritat de vigilància del mercat d'un Estat membre planteja objeccions a una mesura presa per una altra autoritat de vigilància del mercat, o quan la Comissió consideri que la mesura és contrària al dret de la Unió, la Comissió, sense dilació, ha d'iniciar consultes amb l'autoritat de vigilància del mercat de l'Estat membre corresponent i l'operador o operadors, i avaluar la mesura nacional. Basant-se en els resultats d'aquesta avaluació, la Comissió, en el termini de sis mesos, o en el termini de seixanta dies en el cas d'incompliment de la prohibició de les pràctiques d'IA a què es refereix l'article 5, a partir de la notificació a què es refereix l'article 79, apartat 5), ha de decidir si la mesura nacional està justificada i notificar la decisió a l'autoritat de vigilància del mercat de l'estat membre interessat. La Comissió també ha d'informar la resta d'autoritats de vigilància del mercat sobre la seva decisió.
2. Quan la Comissió consideri justificada la mesura adoptada per l'estat membre corresponent, tots els estats membres han d'assegurar-se que adoptin mesures restrictives adequades pel que fa al sistema d'IA en qüestió, com ara exigir-ne la retirada del seu mercat sense dilació indeguda i informar-ne la Comissió en consonància. Quan la Comissió consideri que la mesura nacional és injustificada, l'estat membre interessat l'ha de retirar i informar-ne la Comissió.
3. Quan la mesura nacional es consideri justificada i s'atribueixi l'incompliment del sistema d'IA a deficiències en les normes harmonitzades o especificacions comunes a què es refereixen els articles 40 i 41 del present Reglament, la Comissió ha d'aplicar el procediment previst en l'article 11 del Reglament (UE) 1025/2012.

Article 82

Sistemes d'IA conformes que presenten un risc

1. Si, havent avaluat segons l'article 79 i consultat l'autoritat nacional a què l'article 77, apartat 1, es refereix, conclou que un sistema d'IA d'alt risc, malgrat complir el present Reglament, presenta un risc per a la salut o la seguretat de les persones, per als drets fonamentals o per a

altres aspectes de protecció de l'interès públic, l'autoritat de vigilància del mercat ha de demanar a l'operador interessat que, sense dilacions indegudes i en el termini que l'autoritat estableixi, adopti totes les mesures adequades perquè el sistema d'IA en qüestió ja no presenti el risc en introduir-lo en el mercat o posar-lo en servei.

2. El proveïdor o un altre operador pertinent ha de garantir que es prenguin mesures correctores respecte de tots els sistemes d'IA afectats que s'hagin comercialitzat en el mercat de la Unió, en el termini establert per l'autoritat de vigilància del mercat de l'estat membre a què l'apartat 1 es refereix.

3. Els Estats membres han de comunicar immediatament a la Comissió i als altres estats membres una conclusió segons l'apartat 1. Aquesta informació inclourà tots els detalls disponibles, en particular les dades necessàries per a la identificació del sistema d'IA en qüestió, l'origen i la cadena de subministrament del sistema d'IA, la naturalesa del risc implicat i la naturalesa i durada de les mesures nacionals adoptades.

4. La Comissió ha d'entrar sense dilació indeguda en consulta amb els estats membres interessats i els operadors pertinents, i ha d'avaluar les mesures nacionals adoptades. Sobre la base dels resultats d'aquesta avaluació, la Comissió ha de decidir si la mesura està justificada i, si cal, proposar-ne altres d'apropiades.

5. La Comissió ha de comunicar immediatament la decisió als estats membres interessats i als operadors pertinents. També ha d'informar els altres estats membres.

Article 83

Incompliment formal

1. Quan l'autoritat de vigilància del mercat d'un Estat membre constati una de les situacions indicades a continuació, ha d'exigir al proveïdor corresponent que esmenti l'incompliment de què es tracti, en un termini que l'esmentada autoritat determini:

(a) s'ha col·locat el marcatge CE contravenint l'article 48;

(b) no s'ha col·locat el marcatge CE;

(c) no s'ha elaborat la declaració UE de conformitat a què es refereix l'article 47.

(d) no s'ha elaborat correctament la declaració UE de conformitat amb l'article 47;

(e) no s'ha efectuat el registre a la base de dades de la UE de conformitat amb l'article 71;

(f) quan escaigui, no s'ha nomenat cap representant autoritzat;

(g) no hi ha documentació tècnica disponible.

2. Si l'incompliment a què es refereix l'apartat 1 persisteix, l'autoritat de vigilància del mercat de l'Estat membre de què es tracti ha d'adoptar mesures adequades i proporcionades per restringir o prohibir la comercialització del sistema d'IA d'alt risc o per assegurar-se que es recupera o retira del mercat sense demora.

Article 84

Estructures de suport als assaigs d'IA de la Unió

1. La Comissió ha de designar una o més estructures de suport a les proves d'intel·ligència artificial de la Unió per dur a terme les tasques enumerades en l'article 21, apartat 6, del Reglament (UE) 2019/1020 en l'àmbit de la IA.

2. Sense perjudici de les tasques a què es refereix l'apartat 1, les estructures de suport a les proves d'intel·ligència artificial de la Unió també han de proporcionar assessorament tècnic o científic independent a petició del Consell, la Comissió o les autoritats de vigilància del mercat.

SECCIÓ 4

Vies de recurs

Article 85

Dret a presentar una reclamació davant una autoritat de vigilància del mercat

Sens perjudici d'altres vies administratives o judicials de recurs, tota persona física o jurídica que tingui motius per considerar que s'ha infringit el que disposa el present Reglament podrà presentar reclamacions davant l'autoritat de vigilància del mercat pertinent.

De conformitat amb el Reglament (UE) 2019/1020, aquestes reclamacions s'han de tenir en compte a l'hora de dur a terme activitats de vigilància del mercat i s'han de tramitar de conformitat amb els procediments específics establerts amb aquesta finalitat per les autoritats de vigilància del mercat.

Article 86

Dret a explicació de decisions preses individualment

1. Qualsevol persona afectada subjecta a una decisió presa pel responsable del desplegament sobre la base del resultat de sortida d'un sistema d'IA d'alt risc que figura a l'annex III, a excepció dels sistemes enumerats en el punt 2 d'aquest, i que produeixi efectes legals o que afectin significativament aquesta persona de manera que consideri que té un efecte advers en la seva salut, la seguretat o els drets fonamentals, tenen dret a obtenir del responsable del desplegament explicacions clares i significatives del paper del sistema d'IA en el procediment de presa de decisions i els elements principals de la decisió presa.

2. L'apartat 1 no s'aplica a l'ús de sistemes d'IA per als quals les excepcions o restriccions a l'obligació d'aquest paràgraf es deriven del dret de la Unió o del dret nacional en compliment de la llei de la Unió.

3. Aquest article només s'aplicarà en la mesura que el dret esmentat a l'apartat 1 no estigui previst d'una altra manera en virtut del dret de la Unió.

Article 87

Denúncia d'infraccions i protecció dels denunciants

La Directiva (UE) 2019/1937 s'aplica a la denúncia d'infraccions del present Reglament i a la protecció de les persones que denunciïn.

SECCIÓ 5

Supervisió, investigació, execució i control respecte als proveïdors de models d'IA d'ús general

Article 88

Compliment de les obligacions dels proveïdors de models d'IA d'ús general

1. La Comissió té competències exclusives per supervisar i fer complir el Capítol V, tenint en compte les garanties processals de l'article 94. La Comissió n'ha d'encomanar l'execució a l'Oficina d'IA, sens perjudici de les competències d'organització de la Comissió i del repartiment de competències entre els estats membres i la Unió en virtut dels Tractats.

2. Sense perjudici de l'article 75, apartat 3, les autoritats de vigilància del mercat poden sol·licitar a la Comissió l'exercici de les competències establertes en aquesta secció, quan sigui necessari i proporcionat per ajudar en el compliment de les seves funcions en virtut del present Reglament.

Article 89

Mesures de seguiment

1. A l'efecte de dur a terme les tasques assignades en aquesta secció, l'Oficina d'Intel·ligència Artificial pot prendre les accions necessàries per controlar l'aplicació efectiva i el compliment del Reglament per part dels proveïdors de models d'IA d'ús general, inclosa la seva adhesió als codis de bones pràctiques aprovats.

2. Els proveïdors posteriors tenen dret a presentar reclamacions al·legant infraccions del present Reglament. Les reclamacions s'hauran de motivar degudament i indicar, com a mínim:

(a) el punt de contacte del proveïdor del model IA d'ús general;

(b) una descripció dels fets, les disposicions del present Reglament afectades i els motius pels quals el proveïdor posterior considera que el proveïdor del model d'IA d'ús general de què es tracta ha infringit el present Reglament;

(c) qualsevol altra informació que el proveïdor posterior que presenti la reclamació consideri pertinent, com, per exemple, informació que hagi recopilat per iniciativa pròpia.

Article 90

Alertes del grup d'experts científics sobre riscos sistèmics

1. El comitè científic pot emetre una alerta qualificada per a l'Oficina d'IA, quan tingui motius per sostenir les sospites següents:

(a) un model d'IA d'ús general planteja un risc concret identificable en l'àmbit de la Unió; o

(b) un model d'IA d'ús general compleix les condicions a què es refereix l'article 51.

2. Davant d'aquesta alerta qualificada, la Comissió, a través de l'Oficina d'IA i després d'haver informat el Consell, pot exercir les competències establertes en aquesta secció amb la finalitat d'avaluar l'afer. L'Oficina d'IA ha d'informar el Consell de qualsevol mesura d'acord amb els articles 91 a 94.

3. Les alertes qualificades s'han de motivar degudament i indicar, com a mínim:

(a) el punt de contacte del proveïdor del model d'IA d'ús general amb risc sistèmic en qüestió;

(b) una descripció dels fets rellevants i els motius de l'alerta per part del comitè científic;

(c) qualsevol altra informació que el comitè científic consideri rellevant, inclosa, si escau, la informació recopilada per iniciativa pròpia.

Article 91

Poders per demanar documentació i informació

1. La Comissió pot sol·licitar al proveïdor del model general d'IA a què es refereix que proporcioni la documentació elaborada pel proveïdor d'acord amb els articles 53 i 55, o qualsevol informació addicional que sigui necessària per avaluar el compliment del proveïdor amb el Reglament.

2. Abans d'enviar la sol·licitud d'informació, l'Oficina d'Intel·ligència Artificial pot iniciar un diàleg estructurat amb el proveïdor del model d'IA d'ús general.

3. A petició degudament fonamentada del comitè científic, la Comissió pot fer una sol·licitud d'informació a un proveïdor d'un model d'IA d'ús general, quan l'accés a la informació sigui necessari i proporcionat per al compliment de les tasques del comitè científic en virtut de l'article 68, apartat 2.

4. La sol·licitud d'informació ha de fixar la base legal i la finalitat de la sol·licitud, especificar quina informació es requereix, establir un termini dins del qual s'ha de facilitar la informació, i indicar les multes previstes a l'article 101 per subministrar informació incorrecta, incompleta o enganyosa.

5. El proveïdor del model general de la IA en qüestió o el seu representant ha de subministrar la informació sol·licitada. En el cas de persones jurídiques, empreses o empreses, o quan el proveïdor no tingui personalitat jurídica, les persones autoritzades a representar-les per llei o pels seus estatuts, han de subministrar la informació sol·licitada en nom del proveïdor del model de IA de finalitat general de què es tracti. Els advocats degudament autoritzats per actuar poden proporcionar informació en nom dels seus clients. No obstant això, els clients han d'assumir tota la responsabilitat si la informació subministrada és incompleta, incorrecta o enganyosa.

Article 92

Capacitat per avaluar

1. L'Oficina d'IA, després de consultar el Consell, pot avaluar model d'IA d'ús general en qüestió:
 - (a) per avaluar el compliment de les obligacions del proveïdor en virtut del present Reglament, quan la informació recopilada de conformitat amb l'article 91 sigui insuficient; o
 - (b) investigar els riscos sistèmics en l'àmbit de la Unió de models d'IA d'ús general amb risc sistèmic, en particular després d'una alerta qualificada del comitè científic d'acord amb l'article 90, apartat 1, lletra a).
2. La Comissió pot decidir nomenar experts independents per dur a terme avaluacions en nom seu, fins i tot del comitè científic establert de conformitat amb l'article 68. Els experts independents designats per a aquesta funció han de complir els criteris descrits en l'article 68, apartat 2.
3. A l'efecte de l'apartat 1, la Comissió pot sol·licitar l'accés al model d'IA d'ús general que es tracti a través d'API o altres mitjans i eines tècniques apropiades, inclòs el codi font.
4. La sol·licitud d'accés ha de fixar la base legal, la finalitat i els motius de la sol·licitud i establir el termini dins el qual s'ha de facilitar l'accés, i les multes previstes en l'article 101 per no facilitar l'accés.
5. Els proveïdors del model general d'IA en qüestió o el seu representant han de subministrar la informació sol·licitada. En el cas de persones jurídiques, empreses o societats, o quan el proveïdor no tingui personalitat jurídica, les persones autoritzades a representar-les per llei o pels seus estatuts, han de facilitar l'accés sol·licitat en nom del proveïdor del model d'IA d'ús general de què es tracti.
6. La Comissió ha d'adoptar actes d'execució que estableixin les disposicions detallades i les condicions per a les avaluacions, incloses les disposicions detallades per a la participació d'experts independents, i el procediment per seleccionar-los. Els actes d'execució s'han d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.
7. Abans de sol·licitar l'accés al model d'IA d'ús general, l'Oficina d'Intel·ligència Artificial pot iniciar un diàleg estructurat amb el proveïdor del model d'IA d'ús general per recopilar més informació sobre les proves internes del model, les salvaguardes internes per prevenir riscos sistèmics i altres procediments i mesures internes que el proveïdor ha pres per mitigar aquests riscos.

Article 93

Poders per demanar l'adopció de mesures

1. Quan sigui necessari i apropiat, la Comissió pot sol·licitar als proveïdors que:
 - (a) adoptin les mesures oportunes per complir les obligacions establertes als articles 53 i 54;
 - (b) apliquin mesures de reducció de riscos quan l'avaluació realitzada de conformitat amb l'article 92 apunti que existeixen motius seriosos i fundats de preocupació per l'existència d'un risc sistèmic a escala de la Unió;

(c) restringir la posada a disposició en el mercat, retirar o recuperar el model.

2. Abans de sol·licitar una mesura, l'Oficina d'Intel·ligència Artificial pot iniciar un diàleg estructurat amb el proveïdor del model d'IA d'ús general.

3. Si, durant el diàleg estructurat a què es refereix l'apartat 2, el proveïdor del model d'IA d'ús general amb risc sistèmic es compromet a adoptar mesures de reducció per fer front a un risc sistèmic a escala de la Unió, la Comissió podrà, mitjançant una decisió, fer aquests compromisos vinculants i declarar que no hi ha ja motius per actuar.

Article 94

Garanties processals dels operadors econòmics del model d'IA d'ús general

L'article 18 del Reglament (UE) 2019/1020 s'aplicarà mutatis mutandis als proveïdors del model d'IA d'ús general, sense perjudici de les garanties processals més específiques previstes en el present Reglament.

CAPÍTOL X

CODIS DE CONDUCTA I DIRECTRIUS

Article 95

Codis de conducta per a l'aplicació voluntària de requisits específics

1. L'Oficina d'Intel·ligència Artificial i els Estats membres han d'encoratjar i facilitar l'elaboració de codis de conducta, inclosos els mecanismes de governança relacionats, destinats a fomentar l'aplicació voluntària als sistemes d'IA, que no siguin sistemes d'IA d'alt risc, d'alguns o tots els requisits establerts en el capítol III, secció 2, tenint en compte les solucions tècniques disponibles i les millors pràctiques de la indústria que permeten l'aplicació d'aquests requisits.

2. L'Oficina d'IA i els estats membres han de facilitar l'elaboració de codis de conducta relatius a l'aplicació voluntària, també per part dels responsables del desplegament, de requisits específics per a tots els sistemes d'IA, sobre la base d'objectius clars i indicadors clau de resultats per mesurar la consecució d'aquests objectius, inclosos, entre d'altres però no exclusivament, elements com:

(a) els elements aplicables establerts en les Directrius ètiques de la Unió per a una IA fiable;

(b) l'avaluació i reducció al mínim de les repercussions dels sistemes d'IA en la sostenibilitat mediambiental, també pel que fa a la programació eficient des del punt de vista energètic i les tècniques per dissenyar, entrenar i utilitzar la IA de manera eficient;

(c) la promoció de l'alfabetització en matèria d'IA, en particular en el cas de les persones que s'ocupen del desenvolupament, funcionament i utilització de la IA;

(d) la facilitació d'un disseny inclusiu i divers dels sistemes d'IA, per exemple mitjançant la creació d'equips de desenvolupament inclusius i diversos i la promoció de la participació de les parts interessades en aquest procés;

(e) l'avaluació i prevenció dels perjudicis dels sistemes d'IA per a les persones vulnerables o els col·lectius de persones vulnerables, també pel que fa a accessibilitat per a les persones amb discapacitat, així com per a la igualtat de gènere.

3. Els codis de conducta podran ser elaborats per proveïdors o responsables del desplegament de sistemes d'IA particulars, per les organitzacions que els representin o per ambdós, també amb la participació de qualsevol part interessada i les seves organitzacions representatives, com, per exemple, les organitzacions de la societat civil i el món acadèmic. Els codis de conducta podran comprendre un o diversos sistemes d'IA en funció de la similitud de la finalitat prevista dels diferents sistemes.

4. L'Oficina d'Intel·ligència Artificial i els Estats membres han de tenir en compte els interessos i necessitats específics de les pimes, incloses les empreses emergents, a l'hora de fomentar i facilitar l'elaboració de codis de conducta.

Article 96

Directrius de la Comissió sobre l'aplicació del present Reglament

1. La Comissió elaborarà directrius sobre l'aplicació pràctica del present Reglament i, en particular, sobre:

(a) aplicació dels requisits i obligacions a què es refereixen els articles 8 a 15 i l'article 25;

(b) les pràctiques prohibides a què es refereix l'article 5;

(c) l'aplicació pràctica de les disposicions relatives a modificacions substancials;

(d) l'aplicació pràctica de les obligacions de transparència establertes a l'article 50;

(e) informació detallada sobre la relació del present Reglament amb la legislació d'harmonització de la Unió enumerada a l'annex i, així com amb altres lleis pertinents de la Unió, inclosa la coherència en l'aplicació.

(f) l'aplicació de la definició d'un sistema d'IA tal com s'estableix a l'article 3, apartat 1.

En emetre aquestes directrius, la Comissió ha de prestar especial atenció a les necessitats de les pimes, incloses les empreses emergents, de les autoritats públiques locals i dels sectors més susceptibles de ser afectats pel present Reglament.

Les directrius a què es refereix el paràgraf primer del present apartat han de tenir degudament en compte l'estat de la tècnica generalment reconegut en matèria d'IA, així com les normes harmonitzades i especificacions comunes pertinents a què es refereixen els articles 40 i 41, o les normes harmonitzades o especificacions tècniques que s'estableixin d'acord amb el Dret d'harmonització de la Unió.

2. A petició dels Estats membres o de l'Oficina d'Intel·ligència Artificial, o per iniciativa pròpia, la Comissió ha d'actualitzar les directrius adoptades prèviament quan ho consideri necessari.

CAPÍTOL XI

DELEGACIÓ DE PODERS I PROCEDIMENT DE COMITÈ

Article 97

Exercici de la delegació

1. S'atorguen a la Comissió els poders per adoptar actes delegats en les condicions establertes en el present article.

2. Els poders per adoptar actes delegats esmentats a l'article 6, apartat 6 i 7, l'article 7, apartats 1 i 3, l'article 11, apartat 3, l'article 43, apartats 5 i 6, l'article 47, apartat 5, l'article 51, apartat 3, l'article 52, apartat 4, i l'article 53, apartats 5 i 6, s'atorguen a la Comissió per un període de cinc anys a partir de l'1 d'agost de 2024. La Comissió ha d'elaborar un informe respecte a la delegació de poders amb una antelació mínima de nou mesos al final del període de cinc anys. La delegació de poders s'ha de prorrogar tàcitament per períodes d'igual durada, excepte si el Parlament Europeu o el Consell s'hi oposen amb una antelació mínima de tres mesos al final de cada període.

3. La delegació de poders esmentada a l'article 6, apartats 6 i 7, l'article 7, apartats 1 i 3, l'article 11, apartat 3, l'article 43, apartats 5 i 6, l'article 47, apartat 5, l'article 51, apartat 3, l'article 52, apartat 4, i l'article 53, apartats 5 i 6, podrà ser revocada en qualsevol moment pel Parlament Europeu o pel Consell. La decisió de revocació posarà fi a la delegació dels poders que s'hi especifiquin. La decisió tindrà efecte l'endemà de la seva publicació en el Diari Oficial de la Unió Europea o en una data posterior que s'hi indiqui. Entrarà en vigor l'endemà de la seva publicació en el diari oficial de la Unió Europea o en una data posterior que s'hi especifiqui. No ha d'afectar la validesa dels actes delegats que ja siguin vigents.

4. Abans de l'adopció d'un acte delegat, la Comissió consultarà els experts designats per cada Estat membre de conformitat amb els principis establerts en l'Acord interinstitucional de 13 d'abril de 2016 sobre la millora de la legislació.

5. Tan aviat com adopti una llei delegada, la Comissió ho ha de notificar simultàniament al Parlament Europeu i al Consell.

6. Els actes delegats adoptats en virtut de l'article 6, apartats 6 o 7, l'article 7, apartats 1 o 3, l'article 11, apartat 3, l'article 43, apartats 5 o 6, l'article 47, apartat 5, l'article 51, apartat 3, l'article 52, apartat 4, o l'article 53, apartats 5 o 6, entraran en vigor únicament si, en un termini de tres mesos a partir de la seva notificació al Parlament Europeu i al Consell, cap d'aquestes institucions formula objeccions o si, abans del venciment d'aquest termini, ambdues informen la Comissió que no les formularan. Aquest període es pot ampliar per tres mesos a iniciativa del Parlament Europeu o del Consell.

Article 98

Procediment de comitè

1. La Comissió serà assistida per un comitè. Aquesta comissió serà una comissió en el sentit del Reglament (UE) 182/2011.
2. Quan es faci referència a aquest paràgraf, s'ha d'aplicar l'article 5 del Reglament (UE) 182/2011.

CAPÍTOL XII

SANCIONS

Article 99

Sancions

1. D'acord amb els termes i condicions establerts en el present Reglament, els estats membres han d'establir les normes sobre sancions i altres mesures d'aplicació, que també poden incloure advertències i mesures no monetàries aplicables a les infraccions del Reglament per part dels operadors. També han de prendre totes les mesures necessàries per assegurar que s'apliquin correctament i eficaçment, tenint en compte les directrius emeses per la Comissió en virtut de l'article 96. Les sancions previstes han de ser efectives, proporcionades i dissuasives. Han de tenir en compte els interessos de les pimes, incloses les empreses emergents, i la seva viabilitat econòmica.
2. Sense demora i a tot tardar en la data d'entrada en aplicació, els estats membres han de notificar a la Comissió les normes sobre sancions i altres mesures d'aplicació esmentades a l'apartat 1 i, també sense demora, qualsevol modificació que s'hi introdueixi posteriorment.
3. L'incompliment de la prohibició de les pràctiques d'IA a què es refereix l'article 5 estarà subjecte a multes administratives de fins a 35 000 000 euros o, si l'infractor és una empresa, fins a un 7% del total de la seva facturació anual mundial per a l'exercici anterior, el que sigui superior.
4. L'incompliment de qualsevol de les disposicions següents relatives als operadors o organismes notificats, diferents de les previstes a l'article 5, estarà subjecte a multes administratives de fins a 15 000 000 euros o, si el delinqüent és una empresa, fins a un 3% del total de la seva facturació anual mundial per a l'exercici anterior, el que sigui superior:
 - (a) Obligacions dels proveïdors, de conformitat amb l'article 16.
 - (b) Obligacions dels representants autoritzats, de conformitat amb l'article 22;
 - (c) Obligacions dels importadors, de conformitat amb l'article 23.
 - (d) Obligacions dels distribuïdors, d'acord amb l'article 24.

- (e) Obligacions dels responsables del desplegament, de conformitat amb l'article 26;
- (f) Requisits i obligacions dels organismes notificats de conformitat amb l'article 31, article 33, apartat 1, 3 i 4 o l'article 34;
- (g) Obligacions de transparència per als proveïdors i responsables del desplegament de conformitat amb l'article 50.
5. El subministrament d'informació incorrecta, incompleta o enganyosa als organismes notificats o a les autoritats nacionals competents en resposta a una sol·licitud està subjecte a multes administratives de fins a 7 500 000 euros o, si el delinqüent és una empresa, fins a un 1% del total de la seva facturació anual mundial per a l'exercici anterior, el que sigui més alt.
6. En el cas de les pimes, incloses les empreses emergents, cada multa a què es refereix aquest article ha de ser igual als percentatges o l'import a què es refereixen els apartats 3, 4 i 5, sigui quin sigui el seu valor més baix.
7. En decidir si s'ha d'imposar una multa administrativa i en decidir l'import de la multa administrativa en cada cas particular, s'han de tenir en compte totes les circumstàncies pertinents de la situació concreta i, si escau, s'han de tenir en compte les següents:
- (a) La naturalesa, la gravetat i la durada de la infracció i de les seves conseqüències, tenint en compte la finalitat del sistema d'IA, així com, si escau, el nombre de persones afectades i el nivell de danys soferts per aquestes.
- (b) si les multes administratives ja han estat aplicades per altres autoritats de vigilància del mercat al mateix operador per la mateixa infracció;
- (c) si les multes administratives ja han estat aplicades per altres autoritats al mateix operador per infraccions d'altres lleis de la Unió o nacionals, quan aquestes infraccions siguin conseqüència de la mateixa activitat o omissió que constitueixi una infracció pertinent del present Reglament;
- (d) les dimensions, la facturació anual i la quota de mercat de l'operador que cometi la infracció;
- (e) qualsevol altre factor agreujant o atenuant aplicable a les circumstàncies del cas, com els beneficis financers obtinguts, o les pèrdues evitades, directament o indirectament, per la infracció;
- (f) el grau de cooperació amb les autoritats nacionals competents, amb la finalitat de posar remei a la infracció i mitigar-ne els possibles efectes adversos;

(g) el grau de responsabilitat de l'operador tenint en compte les mesures tècniques i organitzatives aplicades per aquest;

(h) la forma en què la infracció es va conèixer per les autoritats nacionals competents, en particular si, i en quina mesura, l'operador va notificar la infracció;

(i) el caràcter intencional o negligent de la infracció;

(j) qualsevol acció de l'operador per mitigar els danys soferts per les persones afectades.

8. Cada estat membre establirà normes sobre fins a quin punt es poden imposar multes administratives a les autoritats i organismes públics que hi ha establerts.

9. En funció del règim jurídic dels Estats membres, les normes sobre multes administratives poden aplicar-se de manera que les multes siguin imposades pels tribunals nacionals competents o per altres organismes, segons correspongui en aquests Estats membres. L'aplicació d'aquestes normes en aquests estats membres tindrà un efecte equivalent.

10. L'exercici de les competències en virtut d'aquest article estarà subjecte a les garanties processals apropiades d'acord amb el dret de la Unió i el dret nacional, incloent-hi les vies de recurs efectives i el procés degut.

11. Els estats membres han d'informar anualment Comissió de les multes administratives que hagin expedit durant aquest any, de conformitat amb aquest article, i de qualsevol litigi o procediment judicial relacionat.

Article 100

Multes administratives sobre institucions, organismes, oficines i òrgans de la Unió

1. El Supervisor Europeu de Protecció de dades pot imposar multes administratives a les institucions, organismes, oficines i organismes de la Unió que estiguin en l'àmbit d'aplicació del present Reglament. En decidir la imposició d'una multa administrativa i la seva quantia en cada cas concret es prendran en consideració totes les circumstàncies pertinents de la situació de què es tracti i es tindrà degudament en compte el següent:

(a) La naturalesa, la gravetat i la durada de la infracció i de les seves conseqüències, tenint en compte la finalitat del sistema de IA en qüestió, així com, si escau, el nombre de persones afectades i el nivell de danys que pateixen.

(b) el grau de responsabilitat de la institució, organisme, oficina o organisme de la Unió, tenint en compte les mesures tècniques i organitzatives aplicades per aquests;

(c) qualsevol acció de la institució, organisme, oficina o òrgan de la Unió per mitigar els danys patits per les persones afectades;

(d) el grau de cooperació amb el Supervisor Europeu de Protecció de dades per esmenar la infracció i mitigar-ne els possibles efectes adversos, inclòs el compliment de qualsevol de les mesures prèviament ordenades pel Supervisor Europeu de Protecció de dades contra la institució de la Unió, l'organisme, oficina o òrgan interessat en el mateix tema;

(e) infraccions similars anteriors de la institució, organisme, oficina o òrgan de la Unió;

(f) La forma en què la infracció es va conèixer pel Supervisor Europeu de Protecció de dades; en particular si, i en quina mesura, la institució, organisme, oficina o òrgan de la Unió va notificar la infracció;

(g) el pressupost anual de la institució, organisme, oficina o òrgan de la Unió.

2. L'incompliment de la prohibició de les pràctiques d'IA a què es refereix l'article 5 estarà subjecte a multes administratives de fins a 1 500 000 euros.

3. L'incompliment del sistema d'IA de qualsevol requisit o obligació d'acord amb el Reglament, diferent de les previstes en l'article 5, estarà subjecte a multes administratives de fins a 750 000 euros.

4. Abans de prendre decisions de conformitat amb aquest article, el Supervisor Europeu de Protecció de dades ha de donar, a la institució, organisme, oficina o organisme de la Unió que sigui objecte dels procediments duts a terme pel Supervisor Europeu de Protecció de dades, l'oportunitat que se l'escolti sobre la matèria en relació amb la possible infracció. El Supervisor Europeu de Protecció de Dades ha de basar-se les seves decisions únicament en els elements i les circumstàncies sobre els quals les parts afectades hagin pogut manifestar-se. Les persones denunciants, si n'hi ha, estaran estretament relacionades amb el procediment.

5. Els drets de defensa de les parts interessades seran plenament respectats en el procediment. Tindran dret a accedir al fitxer del Supervisor Europeu de Protecció de dades, subjecte a l'interès legítim de les persones o empreses en la protecció de les seves dades personals o secrets empresarials.

6. Els fons recaptats per imposició de multes en aquest article contribuiran al pressupost general de la Unió. Les multes no han d'afectar el funcionament efectiu de la institució, organisme, oficina o òrgan de la Unió objecte de multa.

7. El Supervisor Europeu de Protecció de dades ha de notificar anualment a la Comissió les multes administratives que ha imposat en virtut d'aquest article i de qualsevol litigi o procediment judicial que hagi iniciat.

Article 101

Multes per a proveïdors de models d'IA d'ús general

1. La Comissió pot imposar als proveïdors de models d'IA d'ús general multes que no superin el 3 % del total anual de la seva facturació mundial en l'exercici financer anterior o 15 000 000 euros, el que sigui més elevat, quan la Comissió consideri que el proveïdor actua intencionadament o amb negligència en:

(a) Infringir les disposicions pertinents del Reglament;

(b) Desatendre la sol·licitud d'un document o d'informació de conformitat amb l'article 91, o proporcionar informació incorrecta, incompleta o enganyosa.

(c) No complir una mesura sol·licitada en virtut de l'article 93.

(d) No posar a disposició de la Comissió l'accés al model d'IA d'ús general o al model d'IA d'ús general amb risc sistèmic per tal de dur a terme una avaluació de conformitat amb l'article 92.

En fixar la quantia de la multa o pagament periòdic, cal tenir en compte la naturalesa, la gravetat i la durada de la infracció, tenint degudament presents els principis de proporcionalitat i adequació. La Comissió també ha de tenir en compte els compromisos adquirits de conformitat amb l'article 93, apartat 3, o realitzats en els codis de bones pràctiques pertinents, de conformitat amb l'article 56.

2. Abans d'adoptar la decisió de conformitat amb el paràgraf 1, la Comissió ha de comunicar les seves conclusions preliminars al proveïdor del model general d'IA i li donarà l'oportunitat de ser escoltat.

3. Les multes imposades de conformitat amb aquest article han de ser efectives, proporcionades i dissuasives.

4. La informació sobre les multes imposades en virtut d'aquest article també s'ha de comunicar al Consell, segons correspongui.

5. El Tribunal de Justícia de la Unió Europea tindrà jurisdicció il·limitada per revisar les decisions de la Comissió per les quals s'estableixi una multa en virtut d'aquest article. Pot cancel·lar, reduir o augmentar la multa imposada.

6. La Comissió ha d'adoptar actes d'execució que continguin disposicions detallades i salvaguardes processals per als procediments tenint present la possible adopció de decisions de conformitat amb l'apartat 1 d'aquest article. Els actes d'execució s'han d'adoptar d'acord amb el procediment d'examen a què es refereix l'article 98, apartat 2.

CAPÍTOL XIII

DISPOSICIONS FINALS

Article 102

Modificació del Reglament (CE) 300/2008

En l'article 4, apartat 3, del Reglament (CE) 300/2008, s'afegeix el següent paràgraf:

Quan s'adoptin mesures detallades relatives a les especificacions tècniques i als procediments d'aprovació i ús d'equips de seguretat relatius als sistemes d'IA en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*1\)](#), els requisits establerts al capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

Article 103

Modificació del Reglament (UE) 167/2013

A l'article 17, apartat 5, del Reglament (UE) 167/2013, s'afegeix el següent paràgraf:

Quan s'adoptin actes delegats de conformitat amb el paràgraf primer dels sistemes d'IA que siguin components de seguretat en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*2\)](#), els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

Article 104

Modificació del Reglament (UE) 168/2013

A l'article 22, apartat 5, del Reglament (UE) 168/2013, s'afegeix el següent paràgraf:

Quan s'adoptin actes delegats de conformitat amb el primer paràgraf relatiu als sistemes d'IA que siguin components de seguretat en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*3\)](#), els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

Article 105

Modificació de la Directiva 2014/90/UE

En l'article 8 de la Directiva 2014/90/UE, s'afegeix el següent apartat:

"5. Per als sistemes d'IA que siguin components de seguretat en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*4\)](#), quan dugui a terme les seves activitats de conformitat amb l'apartat 1 i quan s'adoptin especificacions tècniques i normes de prova d'acord amb els paràgrafs 2 i 3, la Comissió ha de tenir en compte els requisits establerts en el capítol III, secció 2, del reglament esmentat.

Article 106

Modificació de la Directiva (UE) 2016/797

A l'article 5 de la Directiva (UE) 2016/797, s'afegeix el següent apartat:

"12. En adoptar actes delegats de conformitat amb l'apartat 1 i en els actes d'execució de conformitat amb l'apartat 11 dels sistemes d'Intel·ligència Artificial que són components de seguretat en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*5\)](#), els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

Article 107

Modificació del Reglament (UE) 2018/858

A l'article 5 del Reglament (UE) 2018/858 s'afegeix el següent apartat:

"4. En adoptar actes delegats de conformitat amb l'apartat 3 relatiu als sistemes d'intel·ligència artificial que són components de seguretat en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*6\)](#), els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

Article 108

Modificació del Reglament (UE) 2018/1139

El Reglament (UE) 2018/1139 es modifica de la manera següent:

(1) A l'article 17 s'afegeix el següent apartat:

"3. Sense perjudici de l'apartat 2, en adoptar actes d'execució de conformitat amb l'apartat 1 sobre els sistemes d'Intel·ligència Artificial que siguin components de seguretat en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*7\)](#), els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

[\(*7\)](#) Reglament (UE) 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 pel qual es modifiquen els reglaments (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858 i (UE) 2018/1139 i (UE) 2019/2144 i les directives 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Llei d'Intel·ligència Artificial) ([DO L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/DOUE>](#)).

(2) A l'article 19 s'afegeix el següent apartat:

"4. En adoptar actes delegats de conformitat amb els paràgrafs 1 i 2 sobre els sistemes d'IA que són components de seguretat en el sentit del Reglament (UE) 2024/1689, els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.'

;

(3) A l'article 43 s'afegeix el següent apartat:

"4. En adoptar actes d'execució d'acord amb l'apartat 1 en relació amb els sistemes d'intel·ligència artificial que són components de seguretat en el sentit del Reglament (UE) 2024/1689, els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

;

(4) A l'article 47 s'afegeix el següent apartat:

"3. En adoptar actes delegats de conformitat amb els paràgrafs 1 i 2 sobre els sistemes d'IA que són components de seguretat en el sentit del Reglament (UE) 2024/1689, els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.'

;

(5) A l'article 57 s'afegeix el següent paràgraf:

‘Quan s'adoptin els actes d'execució relatius als sistemes d'IA que són components de seguretat en el sentit del Reglament (UE) 2024/1689, els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.’

;

(6) A l'article 58 s'afegeix el següent apartat:

"3. En adoptar actes delegats de conformitat amb els paràgrafs 1 i 2 sobre els sistemes d'IA que són components de seguretat en el sentit del Reglament (UE) 2024/1689, els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.’

Article 109

Modificació del Reglament (UE) 2019/2144

A l'article 11 del Reglament (UE) 2019/2144, s'afegeix el següent apartat:

"3. En adoptar els actes d'execució de conformitat amb l'apartat 2, sobre els sistemes d'IA que són components de seguretat en el sentit del Reglament (UE) 2024/1689 del Parlament Europeu i del Consell [\(*8\)](#), els requisits establerts en el capítol III, secció 2, del reglament esmentat s'han de tenir en compte.

Article 110

Modificació de la Directiva (UE) 2020/1828

En l'annex I de la Directiva (UE) 2020/1828 del Parlament Europeu i del Consell [\(58\)](#) s'afegeix el punt següent:

‘(68) Reglament (UE) 2024/1689 2016/797 del Parlament Europeu i del Consell, de 13 2020/1828 de juny de 2024 90, pel qual s'estableixen normes harmonitzades sobre intel·ligència artificial i pel qual es modifiquen els Reglaments (CE) 2018/858, (UE) 2018/1139/2013, (UE) 168/2013, (UE) 2019/2144/2008, (UE) 167 i (Llei d'Intel·ligència Artificial) 300 i (UE) 2014 (Llei d'Intel·ligència Artificial). ([DO L, 2024/1689, 12.7.2024, ELI: HTTP://DATA.EUROPA.UE/ELI/REG/2024/1689/DOUE](#)).

Article 111

Sistemes d'IA ja introduïts en el mercat o posats en servei i models d'IA d'ús general ja introduïts en el mercat

1. Sense perjudici de l'aplicació de l'article 5 a què es refereix l'article 113, apartat 3, lletra a), els sistemes d'IA que siguin components dels sistemes de tecnologies de la informació a gran escala establerts pels actes legislatius enumerats a l'annex X que s'hagin introduït en el mercat o posat en servei abans del 2 d'agost de 2027 s'han de conformar amb el Reglament abans del 31 de desembre de 2030.

Els requisits establerts en el Reglament s'han de tenir en compte en l'avaluació de cada sistema INFORMÀTIC a gran escala establert pels actes legislatius enumerats a l'annex X que es faran

segons s'indica en els actes legislatius i quan aquests actes legislatius siguin substituïts o modificats.

2. Sense perjudici de l'aplicació de l'article 5 a què es refereix l'article 113, apartat 3, lletra a), el Reglament s'aplica als operadors de sistemes d'IA d'alt risc, diferents dels sistemes a què es refereix l'apartat 1 d'aquest article, que s'hagin introduït en el mercat o posat en servei abans del 2 d'agost de 2026, només si, a partir d'aquesta data, aquests sistemes estan subjectes a canvis significatius en els dissenys. En tot cas, els proveïdors i els responsables del desplegament de sistemes d'IA d'alt risc que s'han de fer servir per les autoritats públiques han de prendre les mesures necessàries per complir els requisits i obligacions del present Reglament abans del 2 d'agost de 2030.

3. Els proveïdors de models d'IA d'ús general que s'hagin introduït en el mercat abans del 2 d'agost de 2025 han de prendre les mesures necessàries per complir les obligacions establertes en el present Reglament abans del 2 d'agost de 2027.

Article 112

Avaluació i revisió

1. La Comissió ha d'avaluar la necessitat de modificar la llista establerta a l'annex III i de la llista de pràctiques d'IA prohibides a l'article 5, un cop a l'any després que el present Reglament sigui vigent i, així, fins al final del període de la delegació del poder establert a l'article 97. La Comissió ha de presentar els resultats de l'avaluació al Parlament Europeu i al Consell.

2. Abans del 2 d'agost de 2028 i cada quatre anys a partir d'aleshores, la Comissió ha d'avaluar el següent i informar-ne el Parlament Europeu i el Consell:

(a) La necessitat de modificacions que ampliïn els encapçalaments de les àrees existents o que afegixin noves capçaleres d'àrea a l'annex III;

(b) Les modificacions a la llista de sistemes d'IA que requereixin mesures de transparència addicionals a l'article 50;

(c) modificacions que millorin l'eficàcia del sistema de supervisió i governança.

3. Abans del 2 d'agost de 2029 i cada quatre anys a partir d'aleshores, la Comissió ha de presentar un informe sobre l'avaluació i revisió del present Reglament al Parlament Europeu i al Consell. L'informe ha d'incloure una avaluació sobre l'estructura de l'aplicació i la possible necessitat que una agència de la Unió resolgui les deficiències identificades. En funció de les conclusions, l'informe s'ha d'acompanyar amb una proposta de modificació del present Reglament. Els informes s'han de fer públics.

4. Els informes a què es refereix l'apartat 2 han de prestar especial atenció als aspectes:

(a) La condició dels recursos financers, tècnics i humans de les autoritats nacionals competents per dur a terme amb eficàcia les funcions assignades en virtut del present Reglament.

(b) L'estat de les sancions, en particular les multes administratives a què es refereix l'article 99, apartat 1, que apliquen els estats membres per infraccions del present Reglament.

(c) Les normes harmonitzades adoptades i les especificacions comunes desenvolupades com a suport per al present Reglament.

(d) El nombre d'empreses que entren al mercat després de l'entrada en aplicació del present Reglament, i quantes d'elles són pimes.

5. Abans del 2 d'agost de 2028, la Comissió ha d'avaluar el funcionament de l'Oficina d'IA, si l'Oficina d'IA ha rebut els poders i les competències suficients per complir les seves funcions, i valorar si seria rellevant i necessari, per a la correcta implantació i aplicació del Reglament, actualitzar l'Oficina d'IA i les seves competències d'execució i augmentar-ne els recursos. La Comissió ha de presentar un informe sobre la seva avaluació al Parlament Europeu i al Consell.

6. Per al 2 d'agost de 2028 i cada quatre anys a partir de llavors, la Comissió ha de presentar un informe sobre la revisió dels progressos assolits en el desenvolupament dels lliurables de normalització sobre el desenvolupament eficient de l'energia dels models d'IA d'ús general, i avalua la necessitat de noves mesures o accions, incloses mesures o accions vinculants. L'informe s'ha de presentar al Parlament Europeu i al Consell i s'ha de fer públic.

7. Abans del 2 d'agost de 2028 i cada tres anys a partir de llavors, la Comissió ha d'avaluar l'impacte i l'eficàcia dels codis de conducta voluntaris per fomentar l'aplicació dels requisits establerts al capítol III, secció 2, per a sistemes d'IA diferents dels sistemes d'IA d'alt risc i possiblement altres requisits addicionals per a sistemes d'IA diferents dels sistemes d'IA d'alt risc, incloent-hi la sostenibilitat ambiental.

8. Als efectes dels paràgrafs 1 a 7, el Consell, els Estats membres i les autoritats nacionals competents han de facilitar a la Comissió informació quan aquesta en sol·liciti i sense dilacions indegudes.

9. En fer les avaluacions i revisions a què es refereixen els apartats 1 a 7, la Comissió ha de tenir en compte les posicions i conclusions del Consell d'IA, del Parlament Europeu, del Consell i d'altres organismes o fonts pertinents.

10. La Comissió ha de presentar, si és necessari, propostes adequades per a la modificació del present Reglament, en particular tenint en compte els avenços tecnològics, l'efecte dels sistemes d'IA sobre la salut i la seguretat, i sobre els drets fonamentals, i tenint en compte l'estat de progrés en la societat de la informació.

11. Per guiar les avaluacions i revisions a què es refereixen els apartats 1 a 7 d'aquest article, l'Oficina d'Intel·ligència Artificial es compromet a desenvolupar una metodologia objectiva i participativa per a l'avaluació dels nivells de risc basada en els criteris descrits en els articles pertinents i la inclusió de nous sistemes en:

(a) la llista establerta de l'annex III, inclosa l'extensió de les capçaleres de les àrees existents o l'addició de noves capçaleres d'àrea en aquest annex;

(b) la llista de pràctiques prohibides establertes a l'article 5; i

(c) la llista de sistemes d'IA que requereixen mesures de transparència addicionals d'acord amb l'article 50.

12. Qualsevol modificació del Reglament, de conformitat amb l'apartat 10, o actes delegats o d'execució pertinents, que es refereixi a la legislació d'harmonització de la Unió sectorial que s'enumera a l'annex I, secció B, ha de tenir en compte les especificitats reglamentàries de cada sector, i els mecanismes i autoritats reguladores existents, d'avaluació de la conformitat i de garantia de compliment de la llei que s'hi estableixen.

13. Abans del 2 d'agost de 2031, la Comissió ha d'avaluar l'aplicació del Reglament i informar-ne el Parlament Europeu, el Consell i el Comitè econòmic i Social Europeu, tenint en compte els primers anys d'aplicació del present Reglament. Partint de les conclusions, l'informe, si fa al cas, s'ha d'acompanyar amb una proposta de modificació del present Reglament pel que fa a l'estructura d'aplicació i a la necessitat que un organisme de la Unió resolgui les deficiències identificades.

Article 113

Entrada en vigor i aplicació

El present Reglament entrarà en vigor el vintè dia següent al de la publicació en el Diari oficial de la Unió Europea.

S'ha d'aplicar a partir del 2 d'agost de 2026.

No obstant això:

(a) Els capítols I i II s'han d'aplicar a partir del 2 de febrer de 2025.

(b) El capítol III, secció 4, capítol V, capítol VII i Capítol XII i l'article 78 s'han d'aplicar a partir del 2 d'agost de 2025, a excepció de l'article 101;

(c) L'article 6, apartat 1, i les obligacions corresponents del present Reglament s'han d'aplicar a partir del 2 d'agost de 2027.

El present Reglament és totalment vinculant i d'aplicació directa a tots els estats membres.

Brussel·les, 13 de juny de 2024.

En nom del Parlament Europeu

El president

R. METSOLA

En nom del Consell

El president

M. MICHEL

(1) [DOUE C 517, 22.12.2021, p. 56.](#)

(2) [DOUE C 115, 11.3.2022, p. 5.](#)

(3) [DOUE C 97, 28.2.2022, p. 60.](#)

(4) posició del Parlament Europeu de 13 de març de 2024 (encara no publicada al diari oficial) i decisió del Consell de 21 de maig de 2024.

(5) Consell Europeu, reunió especial del Consell Europeu (1 i 2 d'octubre de 2020) — Conclusions, EUCO 13/20, 2020, p. 6.

(6) Resolució del Parlament Europeu, de 20 d'octubre de 2020, per la qual es recomana a la Comissió un marc d'aspectes ètics de la intel·ligència artificial, la robòtica i les tecnologies relacionades, 2020/2012(INL).

(7) Reglament (CE) 765/2008 del Parlament Europeu i del Consell, de 9 de juliol de 2008 pel qual s'estableixen els requisits d'acreditació i es deroga el Reglament (CEE) 339/93 ([DOUE L 218, 13.8.2008, p. 30](#)).

(8) Decisió 768/2008/CE del Parlament Europeu i del Consell, de 9 de juliol de 2008, relativa a un marc comú per a la comercialització de productes, i per la qual es deroga la decisió 93/465/CEE del Consell ([DOUE L 218, 13.8.2008, p. 82](#)).

(9) Reglament (UE) 2019/1020 del Parlament Europeu i del Consell, de 20 de juny de 2019, relatiu a la vigilància del mercat i al compliment dels productes i pel qual es modifiquen la Directiva 2004/42/CE i els Reglaments (CE) 765/2008 i (UE) 305/2011 ([DO L 169, 25.6.2019, p. 1](#)).

(10) Directiva 85/374/CEE del Consell, de 25 de juliol de 1985, relativa a l'aproximació de les disposicions legals, reglamentàries i administratives dels estats membres relatives a la responsabilitat per productes defectuosos ([DOUE L 210, 7.8.1985, p. 29](#)).

(11) Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament General de Protecció de dades) ([DOUE L 119, 4.5.2016, p. 1](#)).

(12) Reglament (UE) 2018/1725 del Parlament Europeu i del Consell, de 23 d'octubre de 2018, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les institucions, organismes, oficines i organismes de la Unió i sobre la lliure circulació d'aquestes dades. Reglament (CE) 45/2001 i decisió 1247/2002/CE ([DOUE L 295, 21.11.2018, p. 39](#)).

(13) Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de les dades personals per part de les autoritats competents a l'efecte de la prevenció, la investigació, detecció o enjudiciament de delictes penals o execució de sancions penals, i sobre la lliure circulació d'aquestes dades, per la qual es deroga la decisió marc 2008/977/JAI del Consell ([DO L 119, 4.5.2016, p. 89](#)).

(14) Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la privadesa en el sector de les

comunicacions electròniques (Directiva relativa a la privadesa i les comunicacions electròniques) ([DOUE L 201, 31.7.2002, p. 37](#)).

(15) Reglament (UE) 2022/2065 del Parlament Europeu i del Consell, de 19 d'octubre de 2022, relatiu a un mercat únic de serveis digitals i pel qual es modifica la Directiva 2000/31/CE (Llei de serveis digitals) ([DOUE L 277, 27.10.2022, p. 1](#)).

(16) Directiva (UE) 2019/882 del Parlament Europeu i del Consell, de 17 d'abril de 2019, relativa als requisits d'accessibilitat dels productes i serveis ([DOUE L 151, 7.6.2019, p. 70](#)).

(17) Directiva 2005/29/CE del Parlament Europeu i del Consell, d'11 de maig de 2005, relativa a les pràctiques comercials deslleials entre les empreses i els consumidors en el mercat interior i per la qual es modifiquen la Directiva 84/450/CE del Consell, les Directives 97/7/CE, 98/27/CE i 2002/65/CE del Parlament Europeu i del Consell i el Reglament (CE) 2006/2004 del Parlament Europeu i del Consell (Directiva sobre pràctiques comercials deslleials) ([DOUE L 149, 11.6.2005, p. 22](#)).

(18) Decisió marc 2002/584/JAI del Consell, de 13 de juny de 2002, relativa a l'ordre de detenció europea i als procediments de rendició entre els estats membres ([DOUE L 190, 18.7.2002, p. 1](#)).

(19) Directiva (UE) 2022/2557 del Parlament Europeu i del Consell, de 14 de desembre de 2022, relativa a la resiliència de les entitats crítiques i per la qual es deroga la Directiva 2008/114/CE del Consell ([DOUE L 333, 27.12.2022, p. 164](#)).

(20) [DOUE C 247, 29.6.2022, p. 1](#).

(21) Reglament (UE) 2017/745 del Parlament Europeu i del Consell, de 5 d'abril de 2017, sobre productes sanitaris, pel qual es modifiquen la Directiva 2001/83/CE, el Reglament (CE) 178/2002 i el Reglament (CE) 1223/2009 i es deroguen les Directives 90/385/CEE del Consell i 93/42/CEE ([DOUE L 117, 5.5.2017, p. 1](#)).

(22) Reglament (UE) 2017/746 del Parlament Europeu i del Consell, de 5 d'abril de 2017, relatiu als productes sanitaris de diagnòstic in vitro i pel qual es deroga la Directiva 98/79/CE i la Decisió 2010/227/UE de la Comissió ([DOUE L 117, 5.5.2017, p. 176](#)).

(23) Directiva 2006/42/CE del Parlament Europeu i del Consell, de 17 de maig de 2006, relativa a la maquinària i per la qual es modifica la Directiva 95/16/CE ([DOUE L 157, 9.6.2006, p. 24](#)).

(24) Reglament (CE) 300/2008 del Parlament Europeu i del Consell, d'11 de març de 2008, sobre normes comunes en matèria de seguretat de l'aviació civil i pel qual es deroga el Reglament (CE) 2320/2002 ([DOUE L 97, 9.4.2008, p. 72](#)).

(25) Reglament (UE) 167/2013 del Parlament Europeu i del Consell, de 5 de febrer de 2013, relatiu a l'aprovació i vigilància del mercat dels vehicles agrícoles i forestals ([DOUE L 60, 2.3.2013, p. 1](#)).

(26) Reglament (UE) 168/2013 del Parlament Europeu i del Consell, de 15 de gener de 2013, relatiu a l'aprovació i vigilància del mercat de vehicles de dues o tres rodes i quadricicles ([DOUE L 60, 2.3.2013, p. 52](#)).

(27) Directiva 2014/90/UE del Parlament Europeu i del Consell, de 23 de juliol de 2014, relativa als equips marins i per la qual es deroga la Directiva 96/98/CE del Consell ([DOUE L 257, 28.8.2014, p. 146](#)).

[\(28\)](#) Directiva (UE) 2016/797 del Parlament Europeu i del Consell, d'11 de maig de 2016, relativa a la interoperabilitat del sistema ferroviari dins de la Unió Europea ([DO L 138, 26.5.2016, p. 44](#)).

[\(29\)](#) Reglament (UE) 2018/858 del Parlament Europeu i del Consell, de 30 de maig de 2018, relatiu a l'aprovació i vigilància del mercat dels vehicles de motor i els seus remolcs, i dels sistemes, components i unitats tècniques separades destinades a aquests vehicles, pel qual es modifiquen els Reglaments (CE) 715/2007 i (CE) 595/2009 i es deroga la Directiva 2007/46/CE ([DOUE L 151, 14.6.2018, p. 1](#)).

[\(30\)](#) Reglament (UE) 2018/1139 del Parlament Europeu i del Consell, de 4 de juliol de 2018, relatiu a les normes comunes en matèria d'aviació civil i pel qual s'estableix una Agència de Seguretat Aèria de la Unió Europea, i es modifiquen els reglaments (CE) 2111/2005, (CE) 1008/2008, (UE) 996/2010, (UE) 376/2014 i les directives 2014/30/UE i 2014/53/UE del Parlament Europeu i del Consell, i es deroguen els Reglaments (CE) 552/2004 i (CE) 216/2008 del Parlament Europeu i del Consell i el Reglament (CEE) 3922/91 ([DOUE L 212, 22.8.2018, p. 1](#)).

[\(31\)](#) Reglament (UE) 2019/2144 del Parlament Europeu i del Consell, de 27 de novembre de 2019, relatiu als requisits d'homologació de tipus per als vehicles de motor i els seus remolcs, i els sistemes, components i unitats tècniques separades destinades a aquests vehicles, pel que fa a la seva seguretat general i a la protecció dels ocupants de vehicles i usuaris vulnerables de la carretera, pel qual es modifica el Reglament (UE) 2018/858 del Parlament Europeu i del Consell i es deroguen els Reglaments (CE) 78/2009, (CE) 79/2009 i (CE) 661/2009 del Parlament Europeu i del Consell i els reglaments de la Comissió (CE) 631/2009, (UE) 406/2010, (UE) 672/2010, (UE) 1003/2010, (UE) 1005/2010, (UE) 1008/2010, (UE) 1009/2010, (UE) 19/2011, (UE) 109/2011, (UE) 458/2011, (UE) 65/2012, (UE) 130/2012, (UE) 347/2012, (UE) 351/2012, (UE) 1230/2012 i (UE) 2015/166 ([DOUE L 325, 16.12.2019, p. 1](#)).

[\(32\)](#) Reglament (CE) 810/2009 del Parlament Europeu i del Consell, de 13 de juliol de 2009, pel qual s'estableix un Codi comunitari sobre visats (Codi de visats) ([DO L 243, 15.9.2009, p. 1](#)).

[\(33\)](#) Directiva 2013/32/UE del Parlament Europeu i del Consell, de 26 de juny de 2013, relativa als procediments comuns de concessió i retirada de la protecció internacional ([DOUE L 180, 29.6.2013, p. 60](#)).

[\(34\)](#) Reglament (UE) 2024/900 del Parlament Europeu i del Consell, de 13 de març de 2024, sobre transparència i orientació a la publicitat política ([DO L, 2024/900, 34.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj](#)).

[\(35\)](#) Directiva 2014/31/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, relativa a l'harmonització de les legislacions dels estats membres en relació amb la posada a disposició en el mercat d'instruments de ponderació no automàtics ([DOUE L 96 de 29.3.2014 p. 107](#)).

[\(36\)](#) Directiva 2014/32/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, relativa a l'harmonització de les legislacions dels estats membres en relació amb la posada a disposició en el mercat d'instruments de mesurament ([DOUE L 96, 29.3.2014, p. 149](#)).

[\(37\)](#) Reglament (UE) 2019/881 del Parlament Europeu i del Consell, de 17 d'abril de 2019, sobre la certificació de ciberseguretat de les tecnologies de la informació i la comunicació i pel qual es deroga el Reglament (UE) 526/2013 (Llei de ciberseguretat) ([DOUE L 151 de 7.6.2019, p. 15](#)).

[\(38\)](#) Directiva (UE) 2016/2102 del Parlament Europeu i del Consell, de 26 d'octubre de 2016, relativa a l'accessibilitat dels llocs web i aplicacions mòbils dels organismes del sector públic ([DOUE L 327, 2.12.2016, p. 1](#)).

39) Directiva 2002/14/CE del Parlament Europeu i del Consell, d'11 de març de 2002, per la qual s'estableix un marc general per a la informació i la consulta dels empleats de la Comunitat Europea ([DOUE L 80, 23.3.2002, p. 29](#)).

[\(40\)](#) Directiva (UE) 2019/790 del Parlament Europeu i del Consell, de 17 d'abril de 2019, relativa als drets d'autor i drets afins en el mercat únic digital i per la qual es modifiquen les Directives 96/9/CE i 2001/29/CE ([DOUE L 130, 17.5.2019, p. 92](#)).

[\(41\)](#) Reglament (UE) 1025/2012 del Parlament Europeu i del Consell, de 25 d'octubre de 2012, sobre normalització europea, pel qual es modifiquen les Directives 89/97/CEE i 93/15/CEE del Consell i les Directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE i 2009/105/CE del Parlament Europeu i del Consell, i per la qual es deroga la decisió 87/95/CEE del Consell i la decisió 1673/2006/CE del Parlament Europeu i del Consell ([DOUE L 316, 14.11.2012, p. 12](#)).

[\(42\)](#) Reglament (UE) 2022/868 del Parlament Europeu i del Consell, de 30 de maig de 2022, relatiu a la governança de dades europea i pel qual es modifica el Reglament (UE) 2018/1724 (Llei de Governança de dades) ([DOUE L 152, 3.6.2022, p. 1](#)).

[\(43\)](#) Reglament (UE) 2023/2854 del Parlament Europeu i del Consell, de 13 de desembre de 2023, relatiu a les normes harmonitzades sobre l'accés i l'ús equitatiu de les dades i pel qual es modifica el Reglament (UE) 2017/2394 i la Directiva (UE) 2020/1828 (Llei de dades) ([DOUE L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/DOUE>](#))

[\(44\)](#) Recomanació de la Comissió, de 6 de maig de 2003, relativa a la definició de microempreses, petites i mitjanes empreses ([DOUE L 124, 20.5.2003, p. 36](#)).

[\(45\)](#) decisió de la Comissió de 24.1.2024 per la qual es crea l'Oficina Europea d'Intel·ligència Artificial C(2024) 390.

[\(46\)](#) Reglament (UE) 575/2013 del Parlament Europeu i del Consell, de 26 de juny de 2013, sobre els requisits prudencials de les entitats de crèdit i de les empreses d'inversió i pel qual es modifica el Reglament (UE) 648/2012 ([DOUE L 176, 27.6.2013, p. 1](#)).

[\(47\)](#) Directiva 2008/48/CE del Parlament Europeu i del Consell, de 23 d'abril de 2008, relativa als acords de crèdit per als consumidors i per la qual es deroga la Directiva 87/102/CEE del Consell ([DOUE L 133, 22.5.2008, p. 66](#)).

[\(48\)](#) Directiva 2009/138/CE del Parlament Europeu i del Consell, de 25 de novembre de 2009, relativa a la contractació i el seguiment del negoci de les assegurances i reassegurances (Solvència II) ([DOUE L 335, 17.12.2009, p. 1](#)).

[\(49\)](#) Directiva 2013/36/UE del Parlament Europeu i del Consell, de 26 de juny de 2013, relativa a l'accés a l'activitat de les entitats de crèdit i a la supervisió prudencial de les entitats de crèdit i de les empreses d'inversió, per la qual es modifica la Directiva 2002/87/CE i es deroguen les Directives 2006/48/CE i 2006/49/CE ([DO L 176, 27.6.2013, p. 338](#)).

[\(50\)](#) Directiva 2014/17/UE del Parlament Europeu i del Consell, de 4 de febrer de 2014, relativa als acords de crèdit per als consumidors en matèria de béns immobles residencials i per la qual

es modifiquen les Directives 2008/48/CE i 2013/36/UE i el Reglament (UE) 1093/2010 ([DOUE L 60, 28.2.2014, p. 34](#)).

(51) Directiva (UE) 2016/97 del Parlament Europeu i del Consell, de 20 de gener de 2016, relativa a la distribució de les assegurances ([DOUE L 26, 2.2.2016, p. 19](#)).

(52) Reglament (UE) 1024/2013 del Consell, de 15 d'octubre de 2013, pel qual es confereixen al Banc Central Europeu funcions específiques relatives a les polítiques de supervisió prudencial de les entitats de crèdit ([DO L 287, 29.10.2013, p. 63](#)).

Reglament (UE) 2023/988 del Parlament Europeu i del Consell, de 10 de maig de 2023, relatiu a la seguretat general dels productes, pel qual es modifica el Reglament (UE) 1025/2012 del Parlament Europeu i del Consell i la Directiva (UE) 2020/1828 del Parlament Europeu i del Consell. Directiva 2001/95/CE del Parlament Europeu i del Consell i Directiva 87/357/CEE del Consell ([DOUE L 1, 23.5.2023, p. 135](#)).

(54) Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre de 2019, relativa a la protecció de les persones que informen d'infraccions del dret de la Unió ([DOUE L 305, 26.11.2019, p. 17](#)).

(55) [DOUE L 123, 12.5.2016, p. 1](#).

(56) Reglament (UE) 182/2011 del Parlament Europeu i del Consell, de 16 de febrer de 2011, pel qual s'estableixen les normes i els principis generals relatius als mecanismes de control per part dels estats membres de l'exercici de les competències d'execució de la Comissió ([DOUE L 55, 28.2.2011, p. 13](#)).

(57) Directiva (UE) 2016/943 del Parlament Europeu i del Consell, de 8 de juny de 2016, relativa a la protecció del coneixement i la informació empresarial no revelats (secrets comercials) contra la seva adquisició, ús i divulgació il·lícits ([DOUE L 157, 15.6.2016, p. 1](#)).

(58) Directiva (UE) 2020/1828 del Parlament Europeu i del Consell, de 25 de novembre de 2020, relativa a les accions representatives per a la protecció dels interessos col·lectius dels consumidors i per la qual es deroga la Directiva 2009/22/CE ([DOUE L 409, de 4.12.2020 p. 1](#)).

ANNEX I

Llista de legislació d'harmonització de la Unió

Secció A. Llista de legislació d'harmonització de la Unió basada en el nou marc legislatiu

1. Directiva 2006/42/CE del Parlament Europeu i del Consell, de 17 de maig de 2006, relativa a la maquinària, i per la qual es modifica la Directiva 95/16/CE ([DOUE L 157, 9.6.2006, p. 24](#));

2. Directiva 2009/48 /CE del Parlament Europeu i del Consell, de 18 de juny de 2009, relativa a la seguretat de les joguines ([DOUE L 170, 30.6.2009, p. 1](#));

3. Directiva 2013/53/UE del Parlament Europeu i del Consell, de 20 de novembre de 2013, relativa a les embarcacions d'esbarjo i a les embarcacions personals i per la qual es deroga la Directiva 94/25/CE ([DOUE L 354, 28.12.2013, p. 90](#)).
4. Directiva 2014/33 del Parlament Europeu i del Consell, de 26 de febrer de 2014, relativa a l'harmonització de les legislacions dels Estats membres en matèria d'ascensors i components de seguretat per a ascensors ([DOUE L 96, 29.3.2014, p. 251](#));
5. Directiva 2014/34/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, relativa a l'harmonització de les lleis dels Estats membres relatives als equips i sistemes de protecció destinats a l'ús en atmosferes potencialment explosives ([DOUE L 96, 29.3.2014, p. 309](#));
6. Directiva 2014/53/UE del Parlament Europeu i del Consell, de 16 d'abril de 2014, relativa a l'harmonització de les lleis dels estats membres relatives a la posada a disposició en el mercat d'equips de ràdio i per la qual es deroga la Directiva 1999/5/CE ([DOUE L 153, 22.5.2014, p. 62](#));
7. Directiva 2014/68/UE del Parlament Europeu i del Consell, de 15 de maig de 2014, relativa a l'harmonització de les lleis dels estats membres relatives a la posada a disposició en el mercat d'equips de pressió ([DOUE L 189, 27.6.2014, p. 164](#));
8. Reglament (UE) 2016/424 del Parlament Europeu i del Consell, de 9 de març de 2016, relatiu a les instal·lacions de les vies de comunicació i pel qual es deroga la Directiva 2000/9/CE ([DO L 81, 31.3.2016, p. 1](#));
9. Reglament (UE) 2016/425 del Parlament Europeu i del Consell, de 9 de març de 2016, relatiu als equips de protecció personal i pel qual es deroga la Directiva 89/686/CEE del Consell ([DOCE L 81, 31.3.2016, p. 51](#));
10. Reglament (UE) 2016/426 del Parlament Europeu i del Consell, de 9 de març de 2016, sobre els aparells que cremen combustibles gasosos i pel qual es deroga la Directiva 2009/142/CE ([DO L 81, 31.3.2016, p. 99](#));
11. Reglament (UE) 2017/745 del Parlament Europeu i del Consell, de 5 d'abril de 2017, sobre dispositius mèdics, pel qual es modifiquen la Directiva 2001/83 /CE, el Reglament 178/2002 i el Reglament (CE) 1223/2009 i es deroguen les Directives 90/385/CEE i 93/42/CEE del Consell ([DOUE L 117, 5.5.2017, p. 1](#));

12. Reglament (UE) 2017/746 del Parlament Europeu i del Consell, de 5 d'abril de 2017, sobre els productes sanitaris de diagnòstic in vitro i pel qual es deroga la Directiva 98/79/CE i la decisió 2010/227/UE de la Comissió (DOUE [L 117, 5.5.2017, p. 176](#)).

Secció B. Llista d'altres lleis d'harmonització de la Unió

13. Reglament (CE) 300/2008 del Parlament Europeu i del Consell, d'11 de març de 2008, sobre normes comunes en matèria de seguretat de l'aviació civil i pel qual es deroga el Reglament (CE) 2320/2002 ([DOUE L 97, 9.4.2008, p. 72](#)).

14. Reglament (UE) 168/2013 del Parlament Europeu i del Consell, de 15 de gener de 2013, relatiu a l'aprovació i vigilància del mercat de vehicles de dues o tres rodes i quadricicles ([DOUE L 60, 2.3.2013, p. 52](#));

15. Reglament (UE) 167/2013 del Parlament Europeu i del Consell, de 5 de febrer de 2013, relatiu a l'aprovació i vigilància del mercat dels vehicles agrícoles i forestals (DOUE [L 60 de 2.3.2013, p. 1](#));

16. Directiva 2014/90/UE del Parlament Europeu i del Consell, de 23 de juliol de 2014, relativa als equips marins i per la qual es deroga la Directiva 96/98/CE del Consell ([DO L 257, 28.8.2014, p. 146](#));

17. Directiva (UE) 2016/797 del Parlament Europeu i del Consell, d'11 de maig de 2016, relativa a la interoperabilitat del sistema ferroviari dins la Unió Europea ([DO L 138, 26.5.2016, p. 44](#));

18. Reglament (UE) 2018/858 del Parlament Europeu i del Consell, de 30 de maig de 2018, relatiu a l'aprovació i vigilància del mercat dels vehicles de motor i els seus remolcs, i dels sistemes, components i unitats tècniques separades destinades a aquests vehicles, pel qual es modifiquen els Reglaments (CE) 715/2007 i (CE) 595/2009 i es deroga la Directiva 2007/46/CE ([DOUE L 151, 14.6.2018, p. 1](#));

19. Reglament (UE) 2019/2144 del Parlament Europeu i del Consell, de 27 de novembre de 2019, relatiu als requisits d'aprovació de tipus per als vehicles de motor i els seus remolcs, i els sistemes, components i unitats tècniques separades destinades a aquests vehicles, pel que fa a la seva seguretat general i la protecció dels ocupants de vehicles i usuaris vulnerables de la carretera. Reglament (UE) 2018/858 del Parlament Europeu i del Consell, pel qual es deroguen els Reglaments 78/2009, (CE) 79/2009 i (CE) 661/2009 del Parlament Europeu i dels Reglaments del Consell i de la Comissió (CE) 631/2009, (UE) 406/2010, (UE) 672/2010, (UE) 1003/2010, (UE) 1005/2010, (UE) 1008/2010, (UE) 1009/2010, (UE) 19/2011, (UE) 109/2011, (UE) 458/2011, (UE) 65/2012, (UE) 130/2012, (UE) 347/2012, (UE) 351/2012, (UE) 1230/2012 i (UE) 2015/166 ([DOUE L 325, 16.12.2019, p. 1](#));

20. Reglament (UE) 2018/1139 del Parlament Europeu i del Consell, de 4 de juliol de 2018, relatiu a les normes comunes en matèria d'aviació civil i pel qual s'estableix una Agència Europea de Seguretat Aèria. Reglament (CE) 2111/2005, (CE) 1008/2008, (UE) 996/30, (UE) 376/2014 i Directives 2014/2010/UE i 2014/53/UE del Parlament Europeu i del Consell, pel qual es deroguen els Reglaments (CE) 552/2004 i (CE) 216/2008 del Parlament Europeu i del Consell i el Reglament (CE) 3922/91 del Consell ([DOUE L 212, 22.8.2018, p. 1](#)), en la mesura que afecti el disseny, la producció i la introducció en el mercat d'aeronaus a què l'article 2, apartat 1, lletres a) i b), es refereix, pel que fa a les aeronaus no tripulades i els seus motors, hèlixs, components i equips per controlar-les a distància.

ANNEX II

Llista de delictes a què l'article 5, apartat 1, lletra h), punt (iii) es refereix

Infraccions penals a què l'article 5, apartat 1, lletra h), (iii) es refereix:

- terrorisme,

- tràfic d'éssers humans,

- l'explotació sexual i la pornografia infantils.

- tràfic il·lícit de drogues narcòtiques o substàncies psicotròpiques,

- tràfic il·lícit d'armes, municions o explosius,

- mort, ferida greu,

- comerç il·lícit d'òrgans o teixits humans,

- tràfic il·lícit de materials nuclears o radioactius,

- segrest, detenció il·legal o presa d'ostatges,

- delictes dins la jurisdicció del Tribunal Penal Internacional,

- confiscació il·legal d'aeronaus o vaixells,

 - violació,

 - delictes mediambientals,

 - robatori organitzat o armat,

 - sabotatge,
- la participació en una organització criminal implicada en un o més dels delictes esmentats.

ANNEX III

Sistemes d'IA d'alt risc a què fa referència l'article 6, apartat 2

Els sistemes d'IA d'alt risc, d'acord amb l'article 6, apartat 2, són els sistemes d'IA que figuren en qualsevol de les àrees següents:

1. Biometria, en la mesura que la legislació de la Unió o nacional en permeti l'ús:

(a) sistemes d'identificació biomètrica remota.

Això no inclou els sistemes d'IA destinats a la verificació biomètrica que tenen com a finalitat única confirmar que una persona física específica qui diu ser;

(b) Els sistemes d'IA que han de servir per a la categorització biomètrica, d'acord amb atributs o característiques sensibles o protegides basats en la inferència d'aquests atributs o característiques;

(c) Els sistemes d'IA que han de servir per al reconeixement d'emocions.

2. Infraestructures crítiques: Els sistemes d'IA que han de servir com a components de seguretat en la gestió i operació d'infraestructures digitals crítiques, trànsit rodat, o en el subministrament d'aigua, gas, calefacció o electricitat.

3. Educació i formació professional:

- (a) Els sistemes d'IA destinats a determinar l'accés o admissió o a assignar persones físiques a institucions de formació educativa i professional a tots els nivells;
- (b) Els sistemes d'IA que han de servir per avaluar els resultats de l'aprenentatge, fins i tot quan aquests resultats s'utilitzen per dirigir el procés d'aprenentatge de les persones físiques en les institucions de formació educativa i professional a tots els nivells;
- (c) Els sistemes d'IA que han de servir a la finalitat d'avaluar el nivell d'educació adequat que una persona rebrà o a què podrà accedir, en el context o dins de les institucions de formació educativa i professional a tots els nivells;
- (d) Els sistemes d'IA que han de servir per al seguiment i detecció de comportaments prohibits dels estudiants durant les proves en el context o dins d'institucions de formació educativa i professional a tots els nivells.

4. Ocupació, gestió dels treballadors i accés a l'autoocupació:

- (a) Els sistemes d'IA que han de servir per a la contractació o selecció de persones físiques, en particular per col·locar anuncis de treball específics, per analitzar i filtrar les sol·licituds d'ocupació, i per avaluar els candidats;
- (b) Els sistemes d'IA que han de servir per prendre decisions que afectin els termes de les relacions laborals, la promoció o la finalització de les relacions contractuals relacionades amb el treball, per assignar funcions basades en el comportament individual o trets o característiques personals o per supervisar i avaluar el rendiment i el comportament de les persones en aquestes relacions.

5. Accés i gaudi dels serveis privats essencials i dels serveis i beneficis públics essencials:

- (a) Els sistemes d'IA que s'han de fer servir per les autoritats públiques o en nom de les autoritats públiques per avaluar l'elegibilitat de les persones físiques per a beneficis i serveis d'assistència pública essencials, inclosos els serveis sanitaris, així com per concedir, reduir, revocar o reclamar aquests beneficis i serveis;
- (b) Els sistemes d'IA que han de servir per avaluar la solvència creditícia de les persones físiques o per establir-ne la puntuació de crèdit, exceptuant-ne els sistemes d'IA utilitzats amb la finalitat de detectar frau financers;

(c) Els sistemes d'IA que han de servir per a l'avaluació i el preu del risc en relació amb les persones físiques en el cas de l'assegurança de vida i salut;

(d) Els sistemes d'IA destinats a avaluar i classificar les trucades d'emergència de persones físiques o a ser utilitzats per enviar, o per establir prioritat en l'enviament de serveis de primera resposta d'emergència, inclosos els serveis de policia, bombers i assistència mèdica, així com els sistemes de triatge de pacients d'assistència sanitària d'emergència.

6. Garantia del compliment de la llei, en la mesura que se'n permeti l'ús segons la legislació de la Unió o nacional pertinent:

(a) sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió en suport de les autoritats garants del compliment de la llei o en nom seu per avaluar el risc que una persona física es converteixi en víctima de delictes;

(b) sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió en suport de les autoritats garants del compliment de la llei com a polígrafs o eines similars;

(c) sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió en suport de les autoritats garants del compliment de la llei, en suport de les autoritats policials per avaluar la fiabilitat de les proves en el curs de la investigació o l'enjudiciament de delictes;

(d) Els sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió en suport de les autoritats garants del compliment de la llei per avaluar el risc d'una persona física que delinqueixi o torni a delinquir partint no només del perfil de les persones físiques tal com s'esmenta a l'article 3, apartat 4, de la Directiva (UE) 2016/680, o per avaluar els trets i característiques de la personalitat o el comportament criminal passat de persones o grups naturals;

(e) Els sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió en suport de les autoritats garants del compliment de la llei de les autoritats policials per al perfil de les persones físiques tal com es refereix l'article 3, apartat 4, de la Directiva (UE) 2016/680 en el curs de la detecció, investigació o enjudiciament de delictes penals.

7. La gestió de la migració, l'asil i el control de fronteres, en la mesura que se'n permeti l'ús segons la legislació de la Unió o nacional:

- (a) Els sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió com a polígrafs o eines similars;
- (b) Els sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió per avaluar un risc, inclòs un risc de seguretat, un risc de migració irregular o un risc per a la salut, plantejat per una persona física que té la intenció d'entrar o que hagi entrat en el territori d'un estat membre;
- (c) Els sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió per ajudar les autoritats públiques competents a examinar les sol·licituds d'asil; permisos de visat o residència i per a les queixes associades en relació amb l'elegibilitat de les persones físiques que sol·licitin un estatus, incloses les avaluacions relacionades de la fiabilitat de les proves;
- (d) Sistemes d'IA destinats a l'ús per les autoritats garants del compliment de la llei o en nom seu, o per institucions, organismes, oficines o òrgans de la Unió, en el context de la gestió de la migració, l'asil o el control de fronteres, amb la finalitat de detectar, reconèixer o identificar les persones físiques, amb l'excepció de la verificació de documents de viatge.

8. Administració de justícia i processos democràtics:

- (a) els sistemes d'IA destinats a l'ús per una autoritat judicial o en nom seu per ajudar una autoritat judicial en la investigació i interpretació de fets i la llei i la garantia del compliment de la llei a un conjunt concret de fets, o per ser utilitzats de manera similar en la resolució alternativa de conflictes;
- (b) els sistemes d'IA destinats a influir en el resultat d'una elecció o referèndum o en el comportament de vot de les persones físiques en l'exercici del vot en eleccions o referèndums. Això no inclou els sistemes d'IA als resultats de sortida dels quals les persones físiques no estan directament exposades, com ara eines utilitzades per organitzar, optimitzar o estructurar campanyes polítiques des d'un punt de vista administratiu o logístic.

ANNEX IV

Documentació tècnica a què es refereix l'article 11, apartat 1

La documentació tècnica a què es refereix l'article 11, apartat 1, ha de contenir, com a mínim, la següent informació, segons correspongui al sistema d'IA pertinent:

1. Una descripció general del sistema d'IA que inclogui:

- (a) la finalitat que té prevista, el nom del proveïdor i la versió del sistema que reflecteix la seva relació amb versions anteriors;
- (b) com el sistema d'IA interactua o es pot fer servir per interactuar amb el maquinari o el programari, incloent-hi altres sistemes d'IA, que no formen part del mateix sistema d'IA, si escau;
- (c) les versions del programari o del microprogramari pertinents, i qualsevol requisit relacionat amb les actualitzacions de versions;
- (d) la descripció de totes les formes en què el sistema d'IA s'introdueix en el mercat o es posa en servei, com ara paquets de programari incrustats en maquinari, descàrregues o API;
- (e) la descripció del maquinari sobre el qual està destinat el sistema d'IA;
- (f) quan el sistema d'IA és un component de productes, fotografies o il·lustracions que mostren característiques externes, el marcatge i la disposició interna d'aquests productes;
- (g) una descripció bàsica de la interfície d'usuari proporcionada al responsable del desplegament;
- (h) instruccions d'ús per al responsable del desplegament, i una descripció bàsica de la interfície d'usuari proporcionada al responsable del desplegament, si escau;

2. Una descripció detallada dels elements del sistema d'IA i del procés per al seu desenvolupament, que inclogui:

- (a) els mètodes i els passos fets per al desenvolupament del sistema d'IA, incloent-hi, si escau, el recurs a sistemes o eines preentrenats proporcionats per tercers i la forma en què se'n farà ús, integrats o modificats pel proveïdor;
- (b) les especificacions de disseny del sistema, és a dir, la lògica general del sistema d'IA i dels algorismes; les decisions clau de disseny, incloent-hi la lògica i els supòsits de partida, també en relació amb les persones o els col·lectius de persones en relació amb els quals es preveu fer servir el sistema; les decisions principals de classificació; allò que el sistema està dissenyat per optimitzar i la pertinença dels diversos paràmetres; la descripció dels resultats de sortida esperats del sistema i la qualitat dels resultats esmentats; les decisions adoptades

respecte de qualsevol possible concessió pel que fa a les solucions tècniques adoptades per complir els requisits que s'estableixen en el capítol III, secció 2;

(c) La descripció de l'arquitectura del sistema explicant com els components del programari es construeixen o s'alimenten entre si i s'integren en el processament general; els recursos computacionals utilitzats per desenvolupar, entrenar, provar i validar el sistema d'IA;

(d) quan sigui pertinent, els requisits de dades en termes de conjunts de dades que les metodologies i tècniques de formació i els conjunts de dades de formació utilitzats esmenten, incloent-hi una descripció general d'aquests conjunts de dades, informació sobre la seva procedència, abast i característiques principals; forma d'obtenció i selecció de les dades; procediments d'etiquetatge (per exemple, per a l'aprenentatge supervisat), metodologies de neteja de dades (per exemple, detecció de valors atípics);

(e) l'avaluació de les mesures de supervisió humana necessàries de conformitat amb l'article 14, inclosa l'avaluació de les mesures tècniques necessàries per facilitar la interpretació dels resultats de sortida dels sistemes d'IA per part dels responsables del desplegament, d'acord amb l'article 13, apartat 3, lletra d);

(f) quan escaigui, una descripció detallada dels canvis predeterminats en el sistema d'IA i el seu rendiment, juntament amb tota la informació rellevant relacionada amb les solucions tècniques adoptades per garantir el compliment continu del sistema d'IA amb els requisits pertinents establerts en el capítol III, Secció 2;

(g) Els procediments de validació i prova utilitzats, inclosa la informació sobre les dades de validació i prova utilitzades i les seves principals característiques; les mètriques utilitzades per mesurar la precisió, solidesa i compliment d'altres requisits rellevants establerts al capítol III, secció 2, així com impactes potencialment discriminatoris; registres de proves i tots els informes de prova datats i signats pels responsables, incloent-hi els canvis predeterminats referits a la lletra f);

(h) mesures de seguretat cibernètica aplicades;

3. Informació detallada sobre el seguiment, el funcionament i el control del sistema d'IA, en particular pel que fa a: capacitats i limitacions en el rendiment, incloent-hi els graus de precisió per a persones o grups específics de persones en què es vol fer servir el sistema i el nivell total esperat de precisió en relació amb la finalitat que té prevista; els resultats imprevistos i les fonts de riscos per a la salut i la seguretat, els drets fonamentals i la discriminació, tenint en compte la finalitat prevista del sistema d'IA; les mesures de supervisió humana necessàries de conformitat amb l'article 14, incloses les mesures tècniques establertes per facilitar la

interpretació dels resultats de sortida dels sistemes d'IA per part dels responsables del desplegament; les especificacions sobre les dades d'entrada, segons correspongui;

4. una descripció de la conveniència de les mètriques de rendiment per al sistema d'IA específic;

5. una descripció detallada del sistema de gestió de riscos d'acord amb l'article 9;

6. una descripció dels canvis rellevants fets pel proveïdor del sistema a través del seu cicle de vida;

7. una llista de les normes harmonitzades aplicades íntegrament o en part de les quals se n'han publicat les referències al Diari oficial de la Unió Europea; quan no s'hagin aplicat aquestes normes harmonitzades, una descripció detallada de les solucions adoptades per complir els requisits establerts al capítol III, secció 2, incloent-hi una llista d'altres normes pertinents i especificacions tècniques aplicades;

8. una còpia de la declaració de conformitat de la UE a què es refereix l'article 47;

9. una descripció detallada del sistema en vigor per avaluar el rendiment del sistema d'IA en la fase postcomercialització de conformitat amb l'article 72, inclòs el pla de seguiment postcomercialització a què es refereix l'article 72, apartat 3.

ANNEX V

Declaració UE de conformitat

La declaració UE de conformitat a què l'article 47 es refereix ha de contenir tota la informació següent:

1. nom i tipus del sistema d'IA i qualsevol referència addicional inequívoca que en permeti la identificació i traçabilitat;

2. el nom i l'adreça del proveïdor o, si escau, del representant autoritzat;

3. declaració de conformitat a què l'article 47 es refereix de la Unió Europea sota la responsabilitat exclusiva del proveïdor;

4. una declaració que el sistema d'IA és conforme amb el Reglament i, si escau, amb qualsevol altra legislació de la Unió que prevegi l'emissió de la declaració de conformitat de la UE a què es refereix l'article 47;
5. Quan un sistema d'IA implica el tractament de dades personals, una declaració que el sistema d'IA compleix els Reglaments (UE) 2016/679 i (UE) 2018/1725 i la Directiva (UE) 2016/680;
6. Referències a qualsevol norma harmonitzada pertinent utilitzada o qualsevol altra especificació comuna en relació amb la qual es declari la conformitat;
7. quan escaigui, el nom i el número d'identificació de l'organisme notificat, una descripció del procediment d'avaluació de la conformitat realitzat i la identificació del certificat expedit;
8. El lloc i la data d'emissió de la declaració, el nom i la funció de la persona que la va signar, així com una indicació per, o en nom de qui, aquesta persona va signar, una signatura.

ANNEX VI

Procediment d'avaluació de la conformitat basat en el control intern

1.

El procediment d'avaluació de la conformitat basat en el control intern és el procediment d'avaluació de la conformitat basat en els apartats 2, 3 i 4.

2.

El proveïdor verifica que el sistema de gestió de qualitat establert està és conforme amb els requisits de l'article 17.

3.

El proveïdor examina la informació continguda en la documentació tècnica per avaluar el compliment pel sistema d'IA dels requisits essencials pertinents establerts en el capítol III, Secció 2.

4.

El proveïdor també verifica que el procés de disseny i desenvolupament del sistema d'IA i el seu seguiment de postcomercialització, tal com es refereix a l'article 72, sigui coherent amb la documentació tècnica.

ANNEX VII

Conformitat basada en una avaluació del sistema de gestió de la qualitat i en una valoració de la documentació tècnica

1. Introducció

La conformitat basada en una avaluació del sistema de gestió de la qualitat i una avaluació de la documentació tècnica és el procediment d'avaluació de la conformitat basat en els apartats 2 a 5.

2. Visió general

El sistema de gestió de la qualitat aprovat per al disseny, desenvolupament i prova de sistemes d'IA de conformitat amb l'article 17 s'ha d'examinar d'acord amb l'apartat 3 i estar subjecte a la vigilància segons s'especifica en l'apartat 5. La documentació tècnica del sistema d'IA s'ha d'examinar d'acord amb l'apartat 4.

3. Sistema de gestió de la qualitat

3.1. La sol·licitud del proveïdor ha d'incloure:

- (a) el nom i l'adreça del proveïdor i, si l'aplicació és presentada per un representant autoritzat, també el seu nom i adreça;
- (b) La llista de sistemes d'IA coberts pel mateix sistema de gestió de qualitat;
- (c) La documentació tècnica per a cada sistema d'IA cobert pel mateix sistema de gestió de qualitat;
- (d) La documentació relativa al sistema de gestió de la qualitat que cobreix tots els aspectes enumerats en l'article 17;
- (e) una descripció dels procediments establerts per garantir que el sistema de gestió de la qualitat es mantingui adequat i eficaç;
- (f) una declaració per escrit que la mateixa sol·licitud s'ha presentat a cap altre organisme notificat.

3.2.El sistema de gestió de la qualitat s'ha d'avaluar per l'organisme notificat, el qual ha de determinar si compleix els requisits a què es refereix l'article 17.

La decisió s'ha de notificar al proveïdor o al seu representant autoritzat.

La notificació ha de contenir les conclusions de l'avaluació del sistema de gestió de la qualitat i de la decisió d'avaluació raonada.

3.3.El sistema de gestió de la qualitat tal com s'ha aprovat continuarà aplicant-se i mantenint-se pel proveïdor de manera que romangui adequat i eficient.

3.4.Qualsevol canvi previst en el sistema de gestió de la qualitat aprovat o en la llista de sistemes d'IA coberts per aquest últim s'ha de comunicar a l'organisme notificat per part del proveïdor.

Els canvis proposats s'han d'examinar per l'organisme notificat, al qual correspon decidir si el sistema de gestió de la qualitat modificat continua satisfent els requisits esmentats en el punt 3.2 o si és necessària una reavaluació.

L'organisme notificat ha de comunicar al proveïdor la seva decisió. La notificació ha de contenir les conclusions de l'examen dels canvis i de la decisió d'avaluació raonada.

4. Control de la documentació tècnica.

4.1.A més de la sol·licitud a què es refereix l'apartat 3, el proveïdor ha de presentar una sol·licitud davant l'organisme notificat que hagi escollit per a l'avaluació de la documentació tècnica relativa al sistema d'IA que el proveïdor vulgui introduir en el mercat o posar en servei i al qual s'apliqui el sistema de gestió de la qualitat esmentat en l'apartat 3.

4.2.La sol·licitud ha d'incloure:

(a) el nom i l'adreça del proveïdor;

(b) una declaració per escrit que la mateixa sol·licitud no s'ha presentat a cap altre organisme notificat;

(c) La documentació tècnica a què es refereix l'annex IV.

4.3.La documentació tècnica ha de ser examinada per l'organisme notificat. Quan sigui pertinent, i limitat al necessari per complir les seves funcions, l'organisme notificat tindrà accés complet als conjunts de dades de formació, validació i prova utilitzats, incloent-hi, si escau i subjecte a garanties de seguretat, a través de l'API o altres mitjans tècnics i eines pertinents que permetin l'accés remot.

4.4.En examinar la documentació tècnica, l'organisme notificat pot requerir que el proveïdor proporcioni més proves o faci altres proves per permetre una avaluació adequada de la

conformitat del sistema d'IA amb els requisits establerts en el capítol III, secció 2. Quan no estigui satisfet amb les proves fetes pel proveïdor, l'organisme notificat ha de fer directament les proves adequades, segons correspongui.

4.5. Quan sigui necessari per avaluar la conformitat del sistema d'AI d'alt risc amb els requisits establerts en el capítol III, Secció 2, després que tots els altres mitjans raonables per verificar la conformitat s'han esgotat i han demostrat ser insuficients, i a petició motivada, l'organisme notificat també ha de tenir accés als models en entrenament i entrenats del sistema d'IA, incloent-ne els paràmetres pertinents. Aquest accés estarà subjecte a la legislació vigent de la Unió en matèria de protecció de la propietat intel·lectual i dels secrets comercials.

4.6. La decisió de l'organisme notificat s'ha de notificar al proveïdor o al seu representant autoritzat. La notificació contindrà les conclusions de l'avaluació de la documentació tècnica i de la decisió d'avaluació motivada.

Quan el sistema d'IA sigui conforme amb els requisits establerts en el capítol III, secció 2, l'organisme notificat ha d'expedir un certificat d'avaluació de documentació tècnica de la Unió. El certificat indicarà el nom i l'adreça del proveïdor, les conclusions de l'examen, les condicions (si n'hi ha) per a la seva validesa i les dades necessàries per a la identificació del sistema d'IA.

El certificat i els seus annexos han de contenir tota la informació pertinent per permetre avaluar la conformitat del sistema d'IA, i permetre el control del sistema d'IA mentre s'utilitzi, si escau.

Quan el sistema d'IA no sigui conforme amb els requisits establerts en el capítol III, secció 2, l'organisme notificat es negarà a emetre un certificat d'avaluació de documentació tècnica de la Unió i informarà el sol·licitant en conseqüència, motivant la negativa de forma detallada.

Quan el sistema d'IA no compleixi el requisit relatiu a les dades utilitzades per entrenar-lo, caldrà tornar a entrenar el sistema d'IA abans de sol·licitar una nova avaluació de la conformitat. En aquest cas, la decisió d'avaluació raonada de l'organisme notificat que es negui a emetre el certificat d'avaluació de la documentació tècnica de la Unió ha de contenir consideracions específiques sobre les dades de qualitat utilitzades per entrenar el sistema d'IA, en particular sobre els motius de l'incompliment.

4.7. Qualsevol canvi en el sistema d'IA que pugui afectar el compliment del sistema d'IA amb els requisits o la finalitat prevista s'avaluarà per l'organisme notificat que hagi emès el certificat d'avaluació de la documentació tècnica de la Unió. El proveïdor ha de comunicar a aquest organisme notificat la intenció d'introduir qualsevol dels canvis esmentats, o si d'una altra manera es pren consciència de l'ocurrència d'aquests canvis. Els canvis previstos s'avaluaran per l'organisme notificat, el qual decidirà si requereixen una nova avaluació de la conformitat d'acord amb l'article 43, apartat 4, o si es podrien abordar mitjançant un suplement al certificat d'avaluació de la documentació tècnica de la Unió. En aquest últim cas, l'organisme notificat avaluarà els canvis, notificarà al proveïdor la seva decisió i, quan s'aprovin els canvis, expedirà al proveïdor un suplement al certificat d'avaluació de documentació tècnica de la Unió.

5. Control del sistema de gestió de la qualitat aprovat.

5.1.La finalitat de la vigilància feta per l'organisme notificat a què es refereix l'apartat 3 és assegurar-se que el proveïdor compleix degudament els termes i condicions del sistema de gestió de qualitat aprovat.

5.2.A efectes d'avaluació, el proveïdor ha de permetre a l'organisme notificat accedir a les instal·lacions on es dissenyen, desenvolupen i proven els sistemes d'IA. El proveïdor ha de compartir amb l'organisme notificat tota la informació necessària.

5.3.L'organisme notificat ha d'auditar periòdicament per assegurar-se que el proveïdor manté i aplica el sistema de gestió de la qualitat i ha de proporcionar al proveïdor un informe d'auditoria. En el context d'aquestes auditories, l'organisme notificat pot dur a terme proves addicionals dels sistemes d'intel·ligència artificial per als quals es va emetre un certificat d'avaluació de documentació tècnica de la Unió.

ANNEX VIII

Informació que s'ha de presentar en el registre de sistemes d'IA d'alt risc d'acord amb l'article 49

Secció A - informació que han de presentar els proveïdors de sistemes d'IA d'alt risc d'acord amb l'article 49, apartat 1.

La informació següent s'ha de facilitar i mantenir actualitzada en relació amb els sistemes d'IA d'alt risc que es registraran d'acord amb l'article 49, apartat 1:

1. El nom, l'adreça i les dades de contacte del proveïdor;
2. Quan l'enviament d'informació el faci una altra persona en nom del proveïdor, el nom, l'adreça i les dades de contacte d'aquesta persona;
3. El nom, adreça i dades de contacte del representant autoritzat, si escau;
4. El nom comercial del sistema d'IA i qualsevol referència addicional inequívoca que permeti la identificació i traçabilitat del sistema d'IA;
5. Una descripció de la finalitat prevista del sistema d'IA i dels components i funcions suportats a través d'aquest sistema d'IA;
6. Una descripció bàsica i concisa de la informació utilitzada pel sistema (dades, entrades) i la seva lògica de funcionament;

7. La situació del sistema d'IA (en el mercat, en servei, no present en el mercat/fora de servei, recuperat).
8. El tipus, número i data de caducitat del certificat expedit per l'organisme notificat i el nom o número d'identificació d'aquest organisme notificat, si escau.
9. Una còpia escanejada del certificat a què es refereix l'apartat 8, si escau;
10. Els estats membres en els quals el sistema d'IA ha estat introduït en el mercat, posat en servei o posat a disposició dins la Unió.
11. una còpia de la declaració de conformitat de la UE a què es refereix l'article 47;
12. Instruccions electròniques d'ús; aquesta informació no s'ha de proporcionar per als sistemes d'IA d'alt risc en les àrees de garantia del compliment de la llei o migració, asil i control de fronteres a què es refereix l'annex III, punts 1, 6 i 7;
13. URL per a informació addicional (opcional).

Secció B - informació que han de presentar els proveïdors de sistemes d'IA d'alt risc d'acord amb l'article 49, apartat 2.

La següent informació s'ha de facilitar i mantenir actualitzada pel que fa als sistemes d'IA que s'han de registrar d'acord amb l'article 49, apartat 2:

1. El nom, l'adreça i les dades de contacte del proveïdor;
2. Quan l'enviament d'informació el faci una altra persona en nom del proveïdor, el nom, l'adreça i les dades de contacte d'aquesta persona;
3. El nom, adreça i dades de contacte del representant autoritzat, si escau;
4. El nom comercial del sistema d'IA i qualsevol referència addicional inequívoca que permeti la identificació i traçabilitat del sistema d'IA;
5. Una descripció del propòsit previst del sistema d'IA;

6.La condició o condicions en virtut de l'article 6, apartat 3, que es prenen com a base per considerar que el sistema d'IA no és d'alt risc;

7.Un breu resum dels motius pels quals es considera que el sistema d'IA no és d'alt risc en l'aplicació del procediment en virtut de l'article 6, apartat 3;

8.La situació del sistema d'IA (en el mercat, en servei, no present en el mercat/fora de servei, recuperat).

9.Els estats membres en els quals el sistema d'IA ha estat introduït en el mercat, posat en servei o posat a disposició dins la Unió.

Secció C - informació que han de presentar els responsables del desplegament de sistemes d'IA d'alt risc d'acord amb l'article 49, apartat 3.

La informació següent s'ha de facilitar i mantenir actualitzada en relació amb els sistemes d'IA d'alt risc que es registraran d'acord amb l'article 49, apartat 3:

1. El nom, adreça i dades de contacte del responsable del desplegament;

2.El nom, adreça i dades de contacte de la persona que envia informació en nom del responsable del desplegament;

3.L'URL de l'entrada del sistema d'IA a la base de dades de la UE per part del seu proveïdor;

4.Un resum de les conclusions de l'avaluació d'impacte en els drets fonamentals feta d'acord amb l'article 27;

5.Un resum de l'avaluació d'impacte de la protecció de dades feta d'acord amb l'article 35 del Reglament (UE) 2016/679 o l'article 27 de la Directiva (UE) 2016/680 segons s'especifica en l'article 26, apartat 8, del Reglament, si escau.

ANNEX IX

Informació que s'ha de presentar en el registre de sistemes d'IA d'alt risc que figuren a l'annex III en relació amb les proves en condicions reals d'acord amb l'article 60

La següent informació s'ha de facilitar i mantenir actualitzada en relació amb les proves en condicions reals a registrar d'acord amb l'article 60:

1. Un número d'identificació únic a tota la Unió de les proves en condicions reals;

- 2.El nom i les dades de contacte del proveïdor o proveïdor potencial i dels responsables del desplegament involucrats en les proves en condicions reals;
- 3.Una breu descripció del sistema d'IA, la seva finalitat prevista i altra informació necessària per a la identificació del sistema;
4. Un resum de les principals característiques del pla de proves en condicions reals;
5. Informació sobre la suspensió o finalització de les proves en condicions reals.

ANNEX X

La legislació de la Unió actua sobre sistemes INFORMÀTICS a gran escala en l'àmbit de la llibertat, la seguretat i la justícia

1. Sistema d'informació Schengen

(a)Reglament (UE) 2018/1860 del Parlament Europeu i del Consell, de 28 de novembre de 2018, relatiu a l'ús del sistema d'informació Schengen per al retorn de nacionals de tercers països en situació irregular ([DO L 312, 7.12.2018, p. 1](#)).

(b)Reglament (UE) 2018/1861 del Parlament Europeu i del Consell, de 28 de novembre de 2018, relatiu a l'establiment, el funcionament i l'ús del sistema d'informació Schengen (SIS) en l'àmbit dels controls fronterers, i pel qual es modifica el Conveni d'aplicació del Tractat de Schengen i pel qual es modifica i es deroga el Reglament (CE) 1987/2006 ([DO L 312, 7.12.2018, p. 14](#)).

(c)Reglament (UE) 2018/1862 del Parlament Europeu i del Consell, de 28 de novembre de 2018, relatiu a l'establiment, el funcionament i l'ús del sistema d'informació Schengen (sis) en l'àmbit de la cooperació policial i la cooperació judicial en matèria penal, pel qual es modifica i es deroga la decisió 2007/533/JAI del Consell. Reglament (CE) 1986/2006 del Parlament Europeu i del Consell i de la Comissió, de 2010/261/UE ([DO L 312, 7.12.2018, pàg. 56](#)).

2. Sistema d'informació de visats.

(a)Reglament (UE) 2021/1133 del Parlament Europeu i del Consell, de 7 de juliol de 2021, pel qual es modifiquen els Reglaments (UE) 2019/816/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 603 i (UE) 2019/818 pel que fa a l'establiment de les condicions per a l'accés a altres sistemes d'informació de la UE a l'efecte del sistema d'informació de visats ([DO L 248, 13.7.2021, p. 1](#)).

(b)Reglament (UE) 2021/1134 del Parlament Europeu i del Consell, de 7 de juliol de 2021, pel qual es modifiquen els Reglaments (CE) 767 /2008, (CE) 2018/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 810/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 i (UE) 2019/1896 del Parlament Europeu i del Consell i per la qual es deroguen les decisions 2004/512/CE i 2008/633/JAI del Consell, amb la finalitat de reformar el sistema d'informació de visats (DOUE [L 248, 13.7.2021, p. 11](#)).

3. Eurodac

Reglament (UE) 2024/1358 del Parlament Europeu i del Consell, de 14 de maig de 2024, relatiu a l'establiment d'Eurodac per a la comparació de dades biomètriques amb la finalitat d'aplicar eficaçment els Reglaments (UE) 2024/1315 i (UE) 2024/1350 del Parlament Europeu i del Consell i la Directiva 2001/55/CE del Consell i identificar els nacionals de tercers països en situació il·legal i les persones apàtrides i les sol·licituds de comparació amb les dades d'Eurodac per part de les autoritats policials dels estats membres i l'Europol amb finalitats d'aplicació de la llei, modificació dels Reglaments (UE) 2018/1240 i (UE) 2019/818 del Parlament Europeu i del Consell i pel qual es deroga el Reglament (UE) 603/2013 del Parlament Europeu i del Consell ([DO L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/DOUE](#)).

4. Sistema d'entrada/sortida

Reglament (UE) 2017/2226 del Parlament Europeu i del Consell, de 30 de novembre de 2017, pel qual s'estableix un sistema d'entrada/sortida (EES) per registrar les dades d'entrada i sortida i denegació de dades d'entrada de nacionals de tercers països que travessen les fronteres exteriors dels estats membres i determinar les condicions d'accés a la CEE aplicació de la llei es modifica la Convenció que aplica el Tractat i els Reglaments de Schengen (CE) 767/2008 i (UE) 1077/2011 ([DO L 327, 9.12.2017, p. 20](#)).

5. Sistema Europeu d'informació i autorització de viatges

(a)Reglament (UE) 2018/1240 del Parlament Europeu i del Consell, de 12 de setembre de 2018, pel qual s'estableix un sistema europeu d'informació i autorització de viatges (ETIAS) i es modifiquen els Reglaments (UE) 2016/1624/2011, (UE)1/2014, (UE) 2016/399, (UE) 1077 i (UE) 2017/2226 ([DOUE L 236, 19.9.2018, p. 515](#)).

(b)Reglament (UE) 2018/1241 del Parlament Europeu i del Consell, de 12 de setembre de 2018, pel qual es modifica el Reglament (UE) 2016/794 amb la finalitat d'establir un sistema europeu d'informació i autorització de viatges (ETIAS) ([DOUE L 236, 19.9.2018, p. 72](#)).

6. Sistema Europeu d'informació de registres penals sobre nacionals de tercers països i apàtrides

Reglament (UE) 2019/816 del Parlament Europeu i del Consell, de 17 d'abril de 2019, pel qual s'estableix un sistema centralitzat per a la identificació dels estats membres titulars d'informació sobre condemnes de nacionals de tercers països i apàtrides (ECRIS-TCN) per complementar el sistema Europeu d'informació sobre registres penals i modificar el Reglament (UE) 2018/1726 ([DO L 135, 22.5.2019, p. 1](#)).

7. Interoperabilitat

(a)Reglament (UE) 2019/817 del Parlament Europeu i del Consell, de 20 de maig de 2019, relatiu a l'establiment d'un marc d'interoperabilitat entre els sistemes d'informació de la UE en matèria de fronteres i visats i pel qual es modifiquen els Reglaments (CE) 2018/1240, (UE) 2016/399, (UE) 2017/2226, (UE) 767/2008, (UE) 2018/1726 i (UE) 2018/1861 del Parlament Europeu i del Consell i decisions 2004/512/CE i 2008/633/JAI ([DOUE L 135, 22.5.2019, p. 27](#)).

(b)Reglament (UE) 2019/818 del Parlament Europeu i del Consell, de 20 de maig de 2019, relatiu a l'establiment d'un marc d'interoperabilitat entre els sistemes d'informació de la UE en matèria de cooperació policial i judicial, asil i migració i pel qual es modifiquen els Reglaments (UE) 2018/1726, (UE) (UE) 2019/1862 i (UE) 2019/816 ([DOUE L 135 de 22.5.2019, p. 85](#)).

ANNEX XI

Documentació tècnica a què es refereix l'article 53, apartat 1, lletra a): documentació tècnica per a proveïdors de models d'IA d'ús general

Secció 1

Informació que han de facilitar tots els proveïdors de models d'IA d'ús general

La documentació tècnica a què es refereix l'article 53, apartat 1, lletra a) ha de contenir, com a mínim, la següent informació, segons correspongui a la mida i el perfil de risc del model:

1. Una descripció general del model AI d'ús general incloent-hi:

- (a) les funcions que el model està destinat a realitzar i el tipus i la naturalesa dels sistemes d'IA en els quals es pot integrar;
- (b) les polítiques d'ús acceptables aplicables;
- (c) la data de publicació i els mètodes de distribució;
- (d) l'arquitectura i el nombre de paràmetres
- (e) la modalitat (per exemple, text, imatge) i format d'informació d'entrada i resultats de sortida;
- (f) la llicència.

2. Una descripció detallada dels elements del model a què es refereix el punt 1, i informació rellevant del procés de desenvolupament, inclosos els elements següents:

(a) els mitjans tècnics (per exemple, instruccions d'ús, infraestructura, eines) necessaris perquè el model d'IA d'ús general s'integri en els sistemes d'IA;

(b) les especificacions de disseny del model i el procés de formació, incloses les metodologies i tècniques de formació, les opcions de disseny clau, incloent-hi la racionalitat i les suposicions fetes; per a què està dissenyat el model per optimitzar i la rellevància dels diferents paràmetres, segons correspongui;

(c) informació sobre les dades utilitzades per a entrenament, proves i validació, si escau, incloent-hi el tipus i la procedència de les dades i les metodologies de curació (per exemple, neteja, filtrat, etc.), el nombre de punts de dades, l'abast i les característiques principals; com es van obtenir i seleccionar les dades, i totes les altres mesures per detectar la inadequació de les fonts i mètodes de dades per detectar biaixos identificables, si escau;

(d) els recursos computacionals utilitzats per formar el model (per exemple, el nombre d'operacions de punt flotant), el temps d'entrenament i altres detalls rellevants relacionats amb l'entrenament.

(e) consum energètic conegut o estimat del model.

Pel que fa a la lletra e), quan es desconeix el consum energètic del model, el consum energètic es pot basar en informació sobre els recursos computacionals utilitzats.

Secció 2

Informació addicional que han de proporcionar els proveïdors de models d'IA d'ús general amb risc sistèmic

1. Una descripció detallada de les estratègies d'avaluació, inclosos els resultats d'avaluació, sobre la base dels protocols i eines d'avaluació públics disponibles o d'una altra manera d'altres metodologies d'avaluació. Les estratègies d'avaluació han d'incloure criteris d'avaluació, mètriques i la metodologia sobre la identificació de limitacions.

2. Quan escaigui, una descripció detallada de les mesures aplicades amb la finalitat de dur a terme proves internes o externes adverses (per exemple, "equips vermells"), adaptacions de models, incloent-hi l'alineació i la posada a punt.

3. Si és el cas, una descripció detallada de l'arquitectura del sistema que explica com els components del programari es construeixen o s'alimenten entre si i s'integren en el processament general.

Informació de transparència a què es refereix l'article 53, apartat 1, lletra b): documentació tècnica per a proveïdors de models d'IA d'ús general als proveïdors de serveis d'intel·ligència artificial que integren el model en el seu sistema d'IA

La informació a què es refereix l'article 53, apartat 1, lletra b), ha de contenir com a mínim el següent:

1. Una descripció general del model AI d'ús general incloent-hi:

(a) Les funcions que el model està destinat a fer i el tipus i la naturalesa dels sistemes d'IA en què es pot integrar;

(b) les polítiques d'ús acceptables aplicables;

(c) la data de publicació i els mètodes de distribució;

(d) com interactua el model o es pot fer servir per interactuar amb maquinari o programari que no forma part del model en si, si escau;

(e) Les versions de programari rellevant relacionades amb l'ús del model d'IA d'ús general, si escau;

(f) l'arquitectura i el nombre de paràmetres

(g) la modalitat (per exemple, text, imatge) i format d'informació d'entrada i resultats de sortida;

(h) la llicència del model.

2. Una descripció dels elements del model i del procés per al seu desenvolupament, incloent-hi:

(a) els mitjans tècnics (per exemple, instruccions d'ús, infraestructura, eines) necessaris perquè el model d'IA d'ús general s'integri en els sistemes d'IA;

(b) la modalitat (per exemple, text, imatge, etc.) i el format de les dades d'entrada i resultats de sortida i la seva mida màxima (per exemple, longitud de la finestra de context, etc.);

(c) informació sobre les dades utilitzades per a entrenament, proves i validació, si escau, incloent-hi el tipus i la procedència de les dades i metodologies de cura.

ANNEX XIII

Criteria per a la designació de models d'IA d'ús general amb risc sistèmic a què es refereix l'article 51

A l'efecte de determinar que un model d'IA d'ús general té capacitats o un impacte equivalent als establerts en l'article 51, apartat 1, lletra a), la Comissió ha de tenir en compte els criteris següents:

- (a) el nombre de paràmetres del model;

- (b) la qualitat o la mida del conjunt de dades: per exemple, mesurada amb fitxes;

- (c) la quantitat de càlcul utilitzada per a l'entrenament del model, mesurada en operacions de punt flotant o indicada per una combinació d'altres variables com el cost estimat de l'entrenament, el temps estimat requerit per a l'entrenament, o el consum d'energia estimat per a l'entrenament;

- (d) Les modalitats d'entrada i sortida del model, com ara text a text (grans models de llenguatge), text a imatge, multimodalitat, i els límits d'última generació per determinar les capacitats d'alt impacte per a cada modalitat, i el tipus específic d'entrades i resultats de sortida (per exemple, seqüències biològiques);

- (e) els punts de referència i les avaluacions de les capacitats del model, incloent-hi la consideració del nombre de funcions sense formació addicional, l'adaptabilitat per aprendre noves funcions diferents, el seu nivell d'autonomia i escalabilitat, les eines a les quals té accés;

- (f) Si té un alt impacte en el mercat interior a causa del seu abast, que es presumeix quan s'ha posat a disposició d'almenys 10 000 usuaris comercials registrats establerts a la Unió;

- (g) nombre d'usuaris finals registrats.

ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>

ISSN 1977-0677 (edició electrònica)

