

REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 13 de junio de 2024

por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

(Texto pertinente a efectos del EEE)

(EB) 2024/1689 ERREGELAMENDUA, EUROPAKO PARLAMENTUARENA ETA KONTSEILUARENA

2024ko ekainaren 13koa

adimen artifizialaren arloan arau harmonizatuak ezartzen dituen eta (EE) 300/2008, (EB) 167/2013, (EB) 168/2013, (EB) 2018/858, (EB) 2018/1139 eta (EB) 2019/2144 erregelamenduak eta 2014/90/EB, (EB) 2016/797 eta (EB) 2020/1828 zuzentarauak aldatzen dituen (Adimen Artifizialari buruzko Erregelamendua).

(Testu egokia, EEEren ondorioetarako)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA
UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión
Europea, y en particular sus artículos 16 y 114,

Vista la propuesta de la Comisión Europea,

Prevía transmisión del proyecto de acto legislativo a los
Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social
Europeo (1),

Visto el dictamen del Banco Central Europeo (2),

Visto el dictamen del Comité de las Regiones (3),

De conformidad con el procedimiento legislativo
ordinario (4),

Considerando lo siguiente:

(1) El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme, en particular para el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de inteligencia artificial (en lo sucesivo, «sistemas de IA») en la Unión, de conformidad con los valores de la Unión, a fin de promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en

EUROPAKO PARLAMENTUAK ETA EUOPAR
BATASUNEKO KONTSEILUAK,

Europar Batasunaren Funtzionamenduari buruzko
Tratatua eta, bereziki, haren 16. eta 114. artikulua
aztertuta,

Europako Batzordearen proposamena aztertuta,

Lege-egintzaren proiektua alde aurretik helarazita
parlamentu nazionalai,

Europako Ekonomia eta Gizarte Komitearen irizpena
aztertuta (1),

Europako Banku Zentralaren irizpena aztertuta (2),

Erregioen Komitearen irizpena aztertuta (3),

Legegintza-prozedura arruntarekin bat etorrita (4),

Honako hau kontuan hartuta:

(1) Erregelamendu honen xedea da barne-merkatuaren funtzionamendua hobetzea esparru juridiko uniforme bat ezarriz, bereziki Batasunean adimen artifizialeko sistemak (aurrerantzean, «AA-sistemak») garatzeko eta sistema horiek merkatuan jartzeko, zerbitzuan ipintzeko eta erabiltzeko, betiere Batasunaren balioekin bat etorritik. Hartara, gizakian oinarritutako adimen artifizial (AA) fidagarria garatu nahi da, aldi berean babes-maila handia bermatuta, bai osasunaren eta segurtasunaren arloetan, bai Europar Batasuneko Oinarrizko Eskubideen Gutunean



la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, proteger frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación. El presente Reglamento garantiza la libre circulación transfronteriza de mercancías y servicios basados en la IA, con lo que impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el presente Reglamento lo autorice expresamente.

(2) El presente Reglamento debe aplicarse de conformidad con los valores de la Unión consagrados en la Carta, lo que facilitará la protección de las personas físicas, las empresas, la democracia, el Estado de Derecho y la protección del medio ambiente y, al mismo tiempo, impulsará la innovación y el empleo y convertirá a la Unión en líder en la adopción de una IA fiable.

(3) Los sistemas de IA pueden desplegarse con facilidad en sectores muy diversos de la economía y en muchas partes de la sociedad, también a escala transfronteriza, y circular fácilmente por toda la Unión. Algunos Estados miembros ya han estudiado adopción de normas nacionales destinadas a garantizar que la IA sea fiable y segura y se desarrolle y utilice de conformidad con las obligaciones relativas a los derechos fundamentales. La existencia de normas nacionales divergentes puede dar lugar a la fragmentación del mercado interior y reducir la seguridad jurídica de los operadores que desarrollan, importan o utilizan sistemas de IA. Por lo tanto, es preciso garantizar un nivel elevado y coherente de protección en toda la Unión para lograr una IA fiable, así como evitar las divergencias que obstaculizan la libre circulación, la innovación, el despliegue y la adopción en el mercado interior de los sistemas de IA y los productos y servicios conexos mediante el establecimiento de obligaciones uniformes para los operadores y la garantía de una protección uniforme de los fines imperiosos de interés general y de los derechos de las personas en todo el mercado interior, sobre la base del artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE). En la medida en que el presente Reglamento contiene normas específicas para la protección de las personas en relación con el tratamiento de datos personales que restringen el uso de sistemas de IA para la identificación biométrica remota con fines de garantía del cumplimiento del Derecho, el uso de sistemas de IA para la realización de evaluaciones de riesgos de personas físicas con fines de garantía del cumplimiento del Derecho y el uso de sistemas de IA de categorización biométrica con fines de garantía del cumplimiento del Derecho, resulta adecuado basar este Reglamento, en lo que atañe a dichas normas específicas, en el artículo 16 del TFUE. A la luz de dichas normas específicas y del recurso al artículo 16 del TFUE,

(aurrerantzean, «Gutuna») jasotako oinarritzko eskubideen eremuan, haien barruan direla demokrazia, zuzenbide-estatua eta ingurumenaren babesa; eta, horrekin guztiarekin batera, Batasuna AA-sistemen ondorio kaltegarrietatik babestu nahi da eta berrikuntzarako laguntza eman. Erregelamendu honek AAn oinarritutako salgaien eta zerbitzuen mugaz gaindiko zirkulazio askea bermatzen du, eta, era horretara, eragotzi egiten du estatu kideek AA-sistemen garapena, merkaturatzea eta erabilera muga ditzaten, non eta erregelamendu honek ez duen berariaz baimentzen.

(2) Erregelamendu hau Gutunean jasotako Batasunaren balioen arabera aplikatu behar da, hartara egokiro babestuko baitira pertsona fisikoak, enpresak, demokrazia eta zuzenbide-estatua, baita ingurumena ere, eta, aldi berean, berrikuntza eta enplegua bultzatu ahal izango dira, Batasuna lider izan dadin AA fidagarri bat edukitzeko prozesuan.

(3) AA-sistemak aise zabal daitezke ekonomiaren askotariko sektoreetan eta gizartearen eremu ugartan, baita mugaz haraindi ere, eta erraz zirkula dezakete Batasun osoan. Estatu kide batzuek dagoeneko aztergai hartu dute beren estatu-eremurako arauak ezartzea AA fidagarria eta segurua izango dela bermatzeko eta oinarritzko eskubideen gaineko betebeharren arabera garatzen eta erabiltzen dela ziurtatzeko. Alabaina, arauok elkarrengandik desberdinak izateak bide eman dezake barne-merkatua zatitzeko eta AA-sistemak garatzen, inportatzen eta baliatzen dituzten operadoreen segurtasun juridikoa murrizteko. Hortaz, beharrezkoa da Batasun osoan babes-maila handia eta koherentea bermatzea AA fidagarria lortzeko, bai eta desadostasunak saihestea ere oztoporik ez eragiteko barne-merkatuan AA-sistemen eta horiei lotutako produktu eta zerbitzuen zirkulazio askean, berrikuntzan, hedapenean eta onarpenean, eta, horretarako, betebeharrak uniformek ezarri behar dira operadoreentzat, eta barne-merkatu osoan babes uniformea bermatu interes orokorreko ezinbesteko xedeetarako eta pertsonen eskubideetarako, Europar Batasunaren Funtzionamenduari buruzko Tratatuaren (EBFT) 114. artikuluan oinarrituta. Erregelamendu honek pertsonak babesteko arau espezifikoak jasotzen ditu, datu pertsonalen tratamenduari dagokionez pertsonen babes egokia emateko, mugak ezarrita urruneko identifikazio biometrikoko AA-sistemak erabiltzeko orduan, zuzenbidea betearazte aldera, pertsona fisikoen arriskuen ebaluazioak egiteko AA-sistemak erabiltzeko orduan, zuzenbidea betearazte aldera, eta kategorizazio biometrikoko AA-sistemak erabiltzeko orduan, zuzenbidea betearazte aldera; hala, bada, egokia da erregelamendu hau, arau espezifiko horiei dagokienez, EBFTren 16. artikuluan oinarritzea. Arau espezifiko horiek eta EBFTren 16. artikuluen aurkako errekurtsoa



conviene consultar al Comité Europeo de Protección de Datos.

(4) La IA es un conjunto de tecnologías en rápida evolución que contribuye a generar beneficios económicos, medioambientales y sociales muy diversos en todos los sectores económicos y las actividades sociales. El uso de la IA puede proporcionar ventajas competitivas esenciales a las empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental en los ámbitos de la asistencia sanitaria, la agricultura, la seguridad alimentaria, la educación y la formación, los medios de comunicación, el deporte, la cultura, la gestión de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia de los recursos y la energía, el seguimiento ambiental, la conservación y restauración de la biodiversidad y los ecosistemas, y la mitigación del cambio climático y la adaptación a él, entre otros, al mejorar la predicción, optimizar las operaciones y la asignación de los recursos, y personalizar las soluciones digitales que se encuentran a disposición de la población y las organizaciones.

(5) Al mismo tiempo, dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concretos, la IA puede generar riesgos y menoscabar los intereses públicos y los derechos fundamentales que protege el Derecho de la Unión. Dicho menoscabo puede ser tangible o intangible e incluye los perjuicios físicos, psíquicos, sociales o económicos.

(6) Dadas las importantes repercusiones que la IA puede tener en la sociedad y la necesidad de generar confianza, es fundamental que la IA y su marco reglamentario se desarrollen de conformidad con los valores de la Unión consagrados en el artículo 2 del Tratado de la Unión Europea (TUE), los derechos y libertades fundamentales consagrados en los Tratados y, de conformidad con el artículo 6 del TUE, la Carta. Como requisito previo, la IA debe ser una tecnología centrada en el ser humano. Además, debe ser una herramienta para las personas y tener por objetivo último aumentar el bienestar humano.

(7) Conviene establecer normas comunes para los sistemas de IA de alto riesgo al objeto de garantizar un nivel elevado y coherente de protección de los intereses públicos en lo que respecta a la salud, la seguridad y los derechos fundamentales. Estas normas deben ser coherentes con la Carta, no deben ser discriminatorias y deben estar en consonancia con los compromisos de la Unión en materia de comercio internacional. También deben tener en cuenta la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital y las Directrices éticas para una IA fiable del Grupo

kontuan hartuta, komeni da Datuak Babesteko Europako Komiteari kontsulta egitea.

(4) AA bilakaera azkarreko teknologien multzo bat da, eta askotariko onurak dakartza ekonomian, ingurumenean eta gizartean, sektore ekonomiko eta gizarte-jarduera guztietarako. AAre erabilerak funtsezko lehia-abantailak ekar diezazkieke enpresei, eta laguntza eman gizarte- eta ingurumen-ikuspegitik emaitza positiboak lortzeko eremu ugartan: hor dira osasun-laguntza, nekazaritza, elikagaien segurtasuna, hezkuntza eta prestakuntza, komunikabideak, kirola, kultura, azpiegituren kudeaketa, energia, garraioa eta logistika, zerbitzu publikoak, segurtasuna, justizia, baliabideen eta energiaren efizientzia, ingurumen-jarraipena, biodibertsitatearen eta ekosistemen kontserbazioa eta leheneratzea, eta klima-aldaketa arintzea eta horretara egokitzeko prozesuak, besteak beste; izan ere, AA baliagarria da iragarpenak hobetzeko, eragiketak eta baliabideen esleipena optimizatzeko, eta herritarren eta antolakundearen eskura dauden soluzio digitalak pertsonalizatzeko.

(5) Alabaina, aldi berean, haren aplikazio, erabilera eta garapen teknologikoaren maila zehatzen arabera, AAk arriskuak ere sor ditzake eta Batasuneko zuzenbideak babesten dituen interes publikoak eta oinarritzko eskubideak kaltetu. Kalte hori ukigarria edo ukiezina izan daiteke, eta barnean hartzen ditu kalte fisikoak, psikikoak, sozialak edo ekonomikoak.

(6) Ikusita nolako ondorio garrantzitsuak izan ditzakeen AAk gizartean eta, aldi berean, beharrezkoa dela konfiantza sortzea, funtsezkoa da AA eta haren erregelamendu-esparrua bat etortzea Europar Batasunaren Tratatuaren (EBT) 2. artikuluan finkatutako balioekin, tratatuetan finkatutako oinarritzko eskubide eta askatasunekin eta, EBTren 6. artikulua aintzat hartuta, Gutunarekin. Horretarako, lehenik eta behin, ezinbestekoa da gizakian oinarritutako teknologia izatea AA. Gainera, pertsonentzako tresna izan behar du eta gizakien ongizatea hobetzea helburutzat hartu.

(7) Komeni da arrisku handiko AA-sistemarako arau bateratuak ezartzea, hartara interes publikoen babes-maila handia eta koherentea izango dela bermatzeko osasunari, segurtasunari eta oinarritzko eskubideei dagokienez. Arauok ados egon behar dute Gutunarekin; ez dute diskriminatzaileak izan behar, eta Batasunaren konpromisoekin bat egin behar dute nazioarteko merkataritzaren arloan. Halaber, kontuan hartu behar dute Hamarkada Digitalerako Eskubide eta Printzipio Digitalei buruzko Europako Adierazpena, bai eta AAri



independiente de expertos de alto nivel sobre inteligencia artificial.

(8) En consecuencia, se necesita un marco jurídico de la Unión que establezca unas normas armonizadas en materia de IA para impulsar el desarrollo, la utilización y la adopción en el mercado interior de la IA y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad y la protección de los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, reconocidos y protegidos por el Derecho de la Unión. Para alcanzar dicho objetivo, conviene establecer normas que regulen la introducción en el mercado, la puesta en servicio y la utilización de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de libre circulación de mercancías y servicios. Esas normas deben ser claras y firmes por lo que respecta a proteger los derechos fundamentales, apoyar nuevas soluciones innovadoras, posibilitar un ecosistema europeo de agentes públicos y privados que creen sistemas de IA en consonancia con los valores de la Unión y liberar el potencial de la transformación digital en todas las regiones de la Unión. Al establecer tales normas, así como medidas en apoyo de la innovación que prestan especial atención a las pequeñas y medianas empresas (pymes), incluidas las empresas emergentes, el presente Reglamento respalda el objetivo de promover el enfoque europeo de la IA centrado en el ser humano y de ser un líder mundial en el desarrollo de IA segura, digna de confianza y ética, como indicó el Consejo Europeo (5), y garantiza la protección de los principios éticos, como solicitó específicamente el Parlamento Europeo (6).

(9) Deben establecerse normas armonizadas aplicables a la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA de alto riesgo en consonancia con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo (7), la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo (8) y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo (9) (en lo sucesivo, «nuevo marco legislativo»). Las normas armonizadas que se establecen en el presente Reglamento deben aplicarse en todos los sectores y, en consonancia con el nuevo marco legislativo, deben entenderse sin perjuicio del Derecho vigente de la Unión, en particular en materia de protección de datos, protección de los consumidores, derechos fundamentales, empleo, protección de los trabajadores y seguridad de los productos, al que complementa el presente Reglamento. En consecuencia, permanecen inalterados y siguen siendo plenamente aplicables todos los derechos y vías de recurso que el citado Derecho de la Unión otorga a los consumidores y demás personas que puedan verse afectados negativamente por los sistemas de IA,

buruzko goi-mailako adituen talde independenteak egindako Adimen Artifizialerako Gidalerro Etikoak ere.

(8) Ondorioz, Batasunaren eremuko esparru juridiko bat behar da, AArako arau harmonizatuak ezarriko dituen barne-merkatuan AAren garapena, erabilera eta eskuratzea bultzatzeko, eta, aldi berean, egokiro babestuko dituen interes publikoak, hala nola osasuna, segurtasuna eta oinarritzko eskubideak, barnean direla demokrazia, zuzenbide-estatua eta ingurumenaren babesa, guztiak ere Batasuneko zuzenbideak aitortuak eta babestuak. Helburu hori lortzeko, komeni da arauak ezartzea, haien bidez AA-sistema jakin batzuk merkatuan nola jarri, zerbitzuan nola ipini eta nola erabili zehazteko. Horrek barne-merkatuaren funtzionamendu ona bermatuko du, eta aukera emango du sistema horiek salgaien eta zerbitzuen zirkulazio askearen printzipioaz baliu daitezen. Arauok argiak eta irmoak izan behar dute, bidea eman dezaten oinarritzko eskubideak babesteko, soluzio berritzaileak bultzatzeko, eragile publiko eta pribatuen sare europarra eratzeke AA-sistemak Batasuneko balioekin bat etorrita sortzeari begira, eta Batasuneko erregio guztietan eraldaketa digitalaren potentziala askatzeko. Arau horiek ezarrita eta berrikuntza bultzatzeko neurriak hartuta —bereziki enpresa txiki eta ertainei (ETEEi) zuzenduta, enpresa emergenteak barne—, erregelamendu honek babesa ematen die Batasunak arlo honetan dituen helburuei: alegia, AAren ikuspegi europarra sustatzea, zeinak gizakia hartzen baitu oinarri, eta mundu mailan lider izatea, AA segurua, konfiantzazkoa eta etikoa garatzeko, Europako Kontseiluak (5) adierazi zuen bezala; era berean, erregelamenduak printzipio etikoen babesa bermatzen du, Europako Parlamentuak berariaz eskatu zuen bezala (6).

(9) Arau harmonizatuak ezarri behar dira arrisku handiko AA-sistemak merkatuan jartzeari, zerbitzuan ipintzeari eta erabiltzeari buruz, bat etorrita Europako Parlamentuaren eta Kontseiluaren (EE) 765/2008 Erregelamenduarekin (7), Europako Parlamentuaren eta Kontseiluaren 768/2008/EE Erabakiarekin (8) eta Europako Parlamentuaren eta Kontseiluaren (EB) 2019/1020 Erregelamenduarekin (9) (aurrerantzean, «lege-esparru berria»). Erregelamendu honetan ezartzen diren arau harmonizatuak sektore guztietan aplikatu behar dira, hargatik eragotzi gabe, lege-esparru berriarekin bat etorrita, Batasunean indarrean dagoen zuzenbidea, bereziki arlo hauetan: datuen babesa, kontsumitzaileen babesa, oinarritzko eskubideak, enplegua, langileen babesa eta produktuen segurtasuna. Izan ere, erregelamendu hau Batasuneko zuzenbidearen osagarri da. Horrenbestez, beren horretan jarraitzen dute eta guztiz aplikagarriak izaten jarraitzen dute AA-sistemen ondorioz kaltetutako kontsumitzaileei eta gainerako pertsonen Batasuneko zuzenbideak ematen dizkien eskubide eta errekturorako bide guztiek, baita jasandako kalteen



también en lo que respecta a la reparación de los posibles daños de conformidad con la Directiva 85/374/CEE del Consejo (10). Además, en el contexto del empleo y la protección de los trabajadores, el presente Reglamento no debe afectar, por tanto, al Derecho de la Unión en materia de política social ni al Derecho laboral nacional —de conformidad con el Derecho de la Unión— relativa a las condiciones de empleo y de trabajo, incluidas la salud y seguridad en el trabajo y la relación entre empleadores y trabajadores. El presente Reglamento tampoco debe afectar en modo alguno al ejercicio de los derechos fundamentales reconocidos en los Estados miembros y a escala de la Unión, incluidos el derecho o la libertad de huelga o de emprender otras acciones contempladas en los sistemas de relaciones laborales específicos de los Estados miembros y el derecho a negociar, concluir y hacer cumplir convenios colectivos o a llevar a cabo acciones colectivas conforme al Derecho nacional. El presente Reglamento no debe afectar a las disposiciones destinadas a mejorar las condiciones laborales en el trabajo en plataformas digitales establecidas en una Directiva del Parlamento Europeo y del Consejo relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales. Además, el presente Reglamento tiene por objeto reforzar la eficacia de tales derechos y vías de recurso vigentes mediante el establecimiento de requisitos y obligaciones específicos, también en lo que respecta a la transparencia, la documentación técnica y la conservación de registros de los sistemas de IA. Asimismo, las obligaciones impuestas a los distintos operadores que participan en la cadena de valor de la IA en virtud del presente Reglamento deben aplicarse sin perjuicio del Derecho nacional que, de conformidad con el Derecho de la Unión, tenga por efecto limitar el uso de determinados sistemas de IA cuando dicho Derecho quede fuera del ámbito de aplicación del presente Reglamento o persiga objetivos legítimos de interés público distintos de los perseguidos por el presente Reglamento. Así, por ejemplo, el presente Reglamento no debe afectar al Derecho laboral nacional ni al Derecho en materia de protección de menores, a saber, de personas de menos de dieciocho años, que tienen en cuenta la Observación general n.º 25 (2021) de la Convención sobre los Derechos del Niño de las Naciones Unidas relativa a los derechos de los niños en relación con el entorno digital, en la medida en que no son específicas a los sistemas de IA y persiguen otros objetivos legítimos de interés público.

(10) El derecho fundamental a la protección de los datos personales está garantizado, en particular, por los Reglamentos (UE) 2016/679 (11) y (UE) 2018/1725 (12) del Parlamento Europeo y del Consejo y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo (13). Además, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo (14) protege la vida privada y la

erreparaziorako moduek ere, Kontseiluren 85/374/EEE Zuzentarauarekin bat (10). Gainera, enpleguari eta langileen babesari dagokionez, erregelamendu honek ez die eragin behar ez Batasuneko zuzenbideari —gizarte-politikari dagokionez— ezta, Batasuneko zuzenbidearekin bat, lan-zuzenbide nazionalari ere —enplegu- eta lan-baldintzei dagokienez, barnean direla laneko osasun eta segurtasuna eta enplegatzaileen eta langileen harremana—. Erregelamendu honek ez du inolako eraginik izan behar estatu kideetan eta Batasunean aitortutako oinarritzko eskubideak baliatzeko orduan —barruan direla grebarako eskubidea eta askatasuna—, ezta estatu kideetako lan-harremanen sistema espezifikoetan jasotako bestelako ekintzak egiteko orduan ere; era berean, ez du eraginik izan behar hitzarmen kolektiboak negoziatzeko, amaitzeko edo betearazteko eskubidea baliatzeko orduan, edo zuzenbide nazionalarekin bat datozen ekintza kolektiboak egiteko orduan. Erregelamendu honek ez die eragin behar plataforma digitaletako lanetako lan-baldintzak hobetzeko xedapenei, zeinak ezarrita baitaude plataforma digitaletako lanetako lan-baldintzak hobetzeari buruzko Europako Parlamentuaren eta Kontseiluaren zuzentarau batean. Gainera, erregelamendu honen xedea da indarrean diren eskubide eta errekurtso-bide horien efikazia sendotzea, betekizun eta betebeharrak zehatzak ezarrita, are AA-sistemen gardentasunaren, dokumentazio teknikoaren eta erregistroak gordetzearen eremuetan ere. Era berean, erregelamendu honen arabera AAREN balio-katean parte hartzen duten operadoreei ezarritako betekizunak betetzekoak dira hargatik eragotzi gabe AA-sistema jakin batzuen erabilera mugatzen duen zuzenbide nazionala, betiere Batasuneko zuzenbidearekin bat datorren heinean eta zuzenbide nazional hori erregelamendu honen aplikazio-eremutik at geratzen den heinean edo erregelamendu honen xedeez bestelako interes publikoko xede legítimoak helburu dituen heinean. Hala, adibidez, erregelamendu honek ez du eraginik izan behar, ez lan-zuzenbide nazionalan, ezta adingabeen babesaren arloko zuzenbidean ere —hau da, hemezortzi urtetik beherako pertsonen kasuan—, bat etorrita Haurren Eskubideei buruzko Nazio Batuen Konbentzioaren 25. ohar orokorrarekin (2021), zeinak ingurune digitalean haurrek dituzten eskubideak jorratzen baititu; izan ere, ez dira espezifikoak AA-sistemei buruzkoak eta interes publikoko beste helburu legítimo batzuk bilatzen dituzte.

(10) Datu pertsonalak babesteko oinarritzko eskubidea berariaz bermatzen dute Europako Parlamentuaren eta Kontseiluaren (EB) 2016/679 (11) eta (EB) 2018/1725 (12) erregelamenduek eta Europako Parlamentuaren eta Kontseiluaren (EB) 2016/680 Zuzentarauak (13). Europako Parlamentuaren eta Kontseiluaren 2002/58/EE Zuzentarauak (14), bestalde, bizitza



confidencialidad de las comunicaciones, también estableciendo condiciones para cualquier almacenamiento de datos personales y no personales en los equipos terminales, y el acceso desde estos. Dichos actos legislativos de la Unión constituyen la base para un tratamiento de datos sostenible y responsable, también cuando los conjuntos de datos contengan una combinación de datos personales y no personales. El presente Reglamento no pretende afectar a la aplicación del Derecho de la Unión vigente que regula el tratamiento de datos personales, incluidas las funciones y competencias de las autoridades de supervisión independientes competentes para vigilar el cumplimiento de dichos instrumentos. Tampoco afecta a las obligaciones de los proveedores y los responsables del despliegue de sistemas de IA en su papel de responsables o encargados del tratamiento de datos derivadas del Derecho de la Unión o nacional en materia de protección de datos personales en la medida en que el diseño, el desarrollo o el uso de sistemas de IA impliquen el tratamiento de datos personales. También conviene aclarar que los interesados siguen disfrutando de todos los derechos y garantías que les confiere dicho Derecho de la Unión, incluidos los derechos relacionados con las decisiones individuales totalmente automatizadas, como la elaboración de perfiles. Unas normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA establecidas en virtud del presente Reglamento deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos y otras vías de recurso de los interesados garantizados por el Derecho de la Unión en materia de protección de datos personales, así como de otros derechos fundamentales.

(11) El presente Reglamento debe interpretarse sin perjuicio de las disposiciones del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo (15) relativas a la responsabilidad de los prestadores de servicios intermediarios.

(12) Debe definirse con claridad el concepto de «sistema de IA» en el presente Reglamento y armonizarlo estrechamente con los trabajos de las organizaciones internacionales que se ocupan de la IA, a fin de garantizar la seguridad jurídica y facilitar la convergencia a escala internacional y una amplia aceptación, al mismo tiempo que se prevé la flexibilidad necesaria para dar cabida a los rápidos avances tecnológicos en este ámbito. Además, la definición debe basarse en las principales características de los sistemas de IA que los distinguen de los sistemas de software o los planteamientos de programación tradicionales y más sencillos, y no debe incluir los sistemas basados en las normas definidas únicamente por personas físicas para ejecutar automáticamente operaciones. Una característica principal de los sistemas de IA es su capacidad de inferencia. Esta capacidad de inferencia se refiere al proceso de

pribatua eta komunikazio-konfidentzialtasuna babesten ditu, eta zenbait baldintza ezartzen ditu terminalen ekipamenduetan datu pertsonalak eta ez-pertsonalak biltegiratzeo eta haietatik sarbidea izateko. Batasunaren lege-egintza horiek datuen tratamendu jasangarri eta arduratsurako oinarria dira, baita datu multzoek datu pertsonalen eta ez-pertsonalen konbinazioa dutenean ere. Erregelamendu honen helburua ez da datu pertsonalen tratamendua arautzeko Batasunak indarrean duen zuzenbidearen aplikazioari eragitea —barnean hartuta tresna horiek betetzen direla zaintzeko eskumena duten ikuskatze-agintaritzak independenteen eginkizunak eta eskumenak—. Era berean, ez die eragiten AA-sistemen hornitzaileen eta hedapenaren arduradunen betebeharreri, Batasuneko zuzenbidetik edo zuzenbide nazionaletik eratorritako datuen tratamenduaren arduradun diren aldetik, datu pertsonalen babesaren arloan, AA-sistemen diseinuak, garapenak edo erabilerak datu pertsonalak tratatzea dakarren heinean. Argitu beharra dago, halaber, interesdunek jarraitzen dutela Batasuneko zuzenbideak emandako eskubide eta berme guztiak izaten, barnean direla guztiz automatizatutako erabaki indibidualei —hala nola profilaketari— lotutako eskubideak. Behin erregelamendu honen bidez arauak egokiro harmonizatuta AA-sistemak merkatuan jartzeko, zerbitzuaren ipintzeko eta erabiltzeko, arauok bide eman behar dute interesdunen eskubideak eta bestelako errekurtsio-bideak eraginkortasunez aplikatu eta bete ahal izateko, datu pertsonalen eta oinarritzko beste eskubide batzuen arloan Batasunak ezarritako zuzenbideak bermatzen dituen heinean.

(11) Erregelamendu honen interpretazioak ez ditu eragotzi behar Europako Parlamentuaren eta Kontseiluaren (EB) 2022/2065 Erregelamenduak (15) bitarteko zerbitzuen emailen erantzukizunari buruz emandako xedapenak.

(12) Erregelamendu honetan, argi eta garbi definitu behar da «AA-sistemaren» kontzeptua, eta egokiro harmonizatu AAz arduratzen diren nazioarteko antolakundeekin lanekin, hartara segurtasun juridikoa bermatzeko eta nazioartean bateratasun eta onarpen zabala lortzen laguntzeko eta, aldi berean, esparru horretan aurrerapen teknologiko azkarrak jasotzeko behar den malgutasuna aurreikusi ahal izateko. AA-sistema definitzeko orduan, bestalde, aintzat hartu behar da zer ezaugarri nagusik bereizten duten sistema hori software-sistemetatik edo programazio-planteamendu tradizional eta sinpleagoetatik, kanpoan utzita eragiketarako automatikoki egiteko pertsona fisikoek bakarrik definitutako arauetan oinarritutako sistemak. AA-sistemen ezaugarri nagusietako bat sistema horien inferentzia-gaitasuna da; alegia, nolako gaitasuna duten sistema horiek irteera-emaitzak lortzeko (iragarpenak, edukiak, gomendioak edo erabakiak, eragina izan



obtención de resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos y virtuales, y a la capacidad de los sistemas de IA para deducir modelos o algoritmos, o ambos, a partir de información de entrada o datos. Las técnicas que permiten la inferencia al construir un sistema de IA incluyen estrategias de aprendizaje automático que aprenden de los datos cómo alcanzar determinados objetivos y estrategias basadas en la lógica y el conocimiento que infieren a partir de conocimientos codificados o de una representación simbólica de la tarea que debe resolverse. La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos, al permitir el aprendizaje, el razonamiento o la modelización. El término «basado en una máquina» se refiere al hecho de que los sistemas de IA se ejecutan en máquinas. La referencia a objetivos explícitos o implícitos subraya que los sistemas de IA pueden funcionar con arreglo a objetivos definidos explícitos o a objetivos implícitos. Los objetivos del sistema de IA pueden ser diferentes de la finalidad prevista del sistema de IA en un contexto específico. A los efectos del presente Reglamento, debe entenderse por entornos los contextos en los que funcionan los sistemas de IA, mientras que los resultados de salida generados por el sistema de IA reflejan las distintas funciones desempeñadas por los sistemas de IA e incluyen predicciones, contenidos, recomendaciones o decisiones. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. La capacidad de adaptación que un sistema de IA podría mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso. Los sistemas de IA pueden utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente del producto (integrado) o contribuye a la funcionalidad del producto sin formar parte de él (no integrado).

(13) El concepto de «responsable del despliegue» a que hace referencia el presente Reglamento debe interpretarse como cualquier persona física o jurídica, incluida cualquier autoridad pública, órgano u organismo, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. Dependiendo del tipo de sistema de IA, el uso del sistema puede afectar a personas distintas del responsable del despliegue.

(14) El concepto de «datos biométricos» empleado en el presente Reglamento debe interpretarse a la luz del concepto de «datos biométricos» tal como se define en

dezaketenak ingurune fisiko eta birtualetan) eta nolako gaitasuna duten, halaber, ereduak edo algoritmoak —edo biak— ondorioztatzeko, sarrera-informazioetatik edo datuetatik abiatuta. AA-sistema bat eraikitzean inferentzia hori ahalbidetzen duten tekniken artean daude ikaskuntza automatikoko estrategiak; bada, estrategia horiek datuetatik ikasten dute nola lortu helburu jakin batzuk edo logikan eta ezagutzan oinarritutako estrategia batzuk, zeinek inferitu egiten baitute ebatzi beharreko atazaren adierazpide sinbolikotik edo ezagutza kodetuetatik abiatuta. AA-sistema baten inferentzia-gaitasuna datuen oinarritzko tratamendutik harago doa, ikasteko, arrazoitze eta ereduak sortzeko modua baitu. «Makina batean oinarritua» terminoak aditzera ematen du AA-sistemak makinetan exekutatzen direla. Helburu esplizituak edo inplizituak egoteak, berriz, nabarmentzen du AA-sistemek bietara jardun dezaketela: helburu esplizituen arabera zein helburu inplizituen arabera. Gerta daiteke AA-sistemaren xedea ez izatea testuinguru jakin batean AA-sistemarako zehaztutako helburu aurrekusiaren berdina. Erregelamendu honen ondorioetarako, AA-sistemen funtzionamendu-testuinguruak ulertu behar dira ingurunetzat. AA-sistemak sortutako irteera-emaitez, berriz, AA-sistemek betetzen dituzten eginkizunak islatzen dituzte, barruan direla iragarpenak, edukiak, gomendioak eta erabakiak. AA-sistemek autonomia-maila batekin baino gehiagorekin lan egin dezakete; hau da, halako independentzia batez jardun dezakete, giza jardunetik bereiz, eta gizakiok esku hartu gabe funtzionatzeko nolabaiteko gaitasunak dituzte. AA-sistema batek hedatzen denean izan dezakeen egokitze-gaitasunak zera adierazten du: autoikaskuntzarako zer-nolako gaitasunak dituen sistemak, erabili ahal bere burua moldatu ahal izateko. AA-sistemak modu independentean erabili daitezke, edo produktu baten osagai gisa, eta, halakoetan, sistema produktuaren zati izan daiteke fisikoki (integratua) edo produktuaren funtzionalitatean parte hartu haren zati izan gabe (ez-integratua).

(13) Erregelamendu honetan aipatzen den «hedapenaren arduradunaren» kontzeptua honela interpretatu behar da: edozein pertsona fisiko edo juridiko —barnean direla agintaritza publikoak, organoak edo organismoak—, AA-sistema bat erabiltzen duena bere agintepean, salbu eta sistema izaera ez-profesionaleko jarduera pertsonal baterako erabiltzen bada. AA-sistema zer motatakoa den, hedapenaren arduradun ez diren pertsonen eragin diezaike sistemaren erabilerak.

(14) Erregelamendu honetan erabilitako «datu biometrikoen» kontzeptua bat dator honako arau hauetan «datu biometrikoen» kontzeptuak duen



el artículo 4, punto 14, del Reglamento (UE) 2016/679, en el artículo 3, punto 18, del Reglamento (UE) 2018/1725, y en el artículo 3, punto 13, de la Directiva (UE) 2016/680. Los datos biométricos pueden permitir la autenticación, la identificación o la categorización de las personas físicas y el reconocimiento de las emociones de las personas físicas.

(15) El concepto de «identificación biométrica» a que hace referencia el presente Reglamento debe definirse como el reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla, a fin de determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos de referencia, independientemente de que la persona haya dado o no su consentimiento. Quedan excluidos los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local.

(16) El concepto de «categorización biométrica» a que hace referencia el presente Reglamento debe definirse como la inclusión de personas físicas en categorías específicas en función de sus datos biométricos. Estas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de los ojos, los tatuajes, los rasgos conductuales o de la personalidad, la lengua, la religión, la pertenencia a una minoría nacional o la orientación sexual o política. No se incluyen los sistemas de categorización biométrica que sean una característica meramente accesorio intrínsecamente vinculada a otro servicio comercial, lo que significa que la característica no puede utilizarse, por razones técnicas objetivas, sin el servicio principal y que la integración de dicha característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas del presente Reglamento. Por ejemplo, los filtros que clasifican las características faciales o corporales utilizados en los mercados en línea podrían constituir una característica accesorio de este tipo, ya que solo pueden utilizarse en relación con el servicio principal, que consiste en vender un producto permitiendo al consumidor previsualizar cómo le quedaría y ayudarlo a tomar una decisión de compra. Los filtros utilizados en los servicios de redes sociales que clasifican las características faciales o corporales a fin de que los usuarios puedan añadir o modificar imágenes o vídeos también podrían considerarse una

definizioarekin: (EB) 2016/679 Erregelamenduaren 4.14 artikulua, (EB) 2018/1725 Erregelamenduaren 3.18 artikulua eta (EB) 2016/680 Zuzentarauaren 3.13 artikulua. Datu biometrikoek aukera eman dezakete pertsona fisikoak autentifikatzeko, identifikatzeko eta kategorizatzeke, baita pertsona fisikoen emozioak ezagutzeko ere.

(15) Erregelamendu honetan aipatzen den «identifikazio biometrikoaren» kontzeptua honela definitu behar da: giza ezaugarri fisiko, fisiologiko edo konduktualen ezagutza automatizatua, aztergai hartzen dituen aurpegia, begi-mugimendua, gorputzaren forma, ahotsa, intonazioa, ibilkera, jarrera, bihotz-maiztasuna, arteria-presioa, usaina, tekla-pultsazioen ezaugarriak eta beste, horietan oinarrituta pertsona baten identitatea zehazteko; horretarako, erreferentziako datu-base batean biltegiratutako pertsonen datu biometrikoekin alderatzen ditu pertsona horren datu biometrikoak, kontuan hartu gabe pertsonak erabilera horretarako adostasuna eman duen ala ez. Kanpoan geratzen dira egiaztapen biometrikora bideratutako AA-sistemak — egiaztapenaren barruan autentifikazioa ere barne hartzen dutenak —, baldin eta sistema horien helburu bakarra bada pertsona fisiko baten identitatea hark esandakoarekin bat datorrela ziurtatzea edo pertsona fisiko baten identitatea xede jakin eta bakar baterako egiaztatzea, hala nola zerbitzu zehatz baterako sarbidea izateko, gailu bat desblokeatzeko edo lokal bateko segurtasun-sarbidea izateko.

(16) Erregelamendu honetan aipatzen den «kategorizazio biometrikoaren» kontzeptua honela definitu behar da: pertsona fisikoak beren datu biometrikoen arabera kategorio espezifikoetan sailkatzea. Kategorio espezifiko horiek askotariko alderdietan oinarritu daitezke: sexua, adina, ile-kolorea, begi-kolorea, tatuajeak, portaera- edo izaera-bereizgarriak, hizkuntza, erlijioa, gutxiengo nazional bateko kide izatea edo orientazio sexuala edo politikoa. Kategorizazio biometrikoko beste sistema batzuk merkataritza-zerbitzu bati berez lotutako ezaugarri osagarri hutsa dira, eta sistema horiek ez dira kontzeptu honen barruan sartzen; izan ere, halako kasuetan, ezaugarri hori ezin da erabili, arrazoi tekniko objektiboengatik, zerbitzu nagusirik gabe, eta ezaugarri edo funtzionalitate hori integratzeak ez du bide ematen erregelamendu honetako arauen aplikagarritasuna saihesteko. Esate baterako, lineako merkatuetan erabiltzen diren aurpegiko edo gorputzeko ezaugarriak sailkatzeko iragazkiak mota horretako ezaugarri osagarriak izan daitezke; izan ere, zerbitzu nagusiari lotuta soilik erabili daitezke, zeina baita produktu bat saltzea, eta sistema horren bidez kontsumitzaileak jakin baitetzake produktu hori ondo egokituko zaion eta horren arabera erosiko duen erabaki. Ezaugarri osagarritzat har daitezke, halaber, sare sozialetan erabiltzen diren iragazkiak, aurpegi edo gorputzeko ezaugarriak sailkatzen dituztenak erabiltzaileek irudiak edo bideoak



característica accesorio, ya que dichos filtros no pueden utilizarse sin el servicio principal de las redes sociales, que consiste en compartir contenidos en línea.

(17) El concepto de «sistema de identificación biométrica remota» a que hace referencia el presente Reglamento debe definirse de manera funcional como un sistema de IA destinado a identificar a personas físicas sin su participación activa, generalmente a distancia, comparando sus datos biométricos con los que figuren en una base de datos de referencia, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen. Estos sistemas de identificación biométrica remota suelen utilizarse para detectar a varias personas o su comportamiento de forma simultánea, a fin de simplificar considerablemente la identificación de personas sin su participación activa. Quedan excluidos los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local. Esa exclusión se justifica por el hecho de que tales sistemas probablemente tengan una repercusión menor en los derechos fundamentales de las personas físicas que los sistemas de identificación biométrica remota que puedan utilizarse para el tratamiento de los datos biométricos de un gran número de personas sin su participación activa. En el caso de los sistemas «en tiempo real», la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea, casi instantánea o, en cualquier caso, sin una importante demora. En este sentido, no debe existir la posibilidad de eludir las normas contempladas en el presente Reglamento en relación con el uso «en tiempo real» de los sistemas de IA de que se trate generando demoras mínimas. Los sistemas «en tiempo real» implican el uso de materiales «en directo» o «casi en directo», como grabaciones de vídeo, generados por una cámara u otro dispositivo con funciones similares. En cambio, en los sistemas «en diferido» ya se han recabado los datos biométricos y la comparación e identificación se producen con una importante demora. A tal fin se utilizan materiales, como imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado o dispositivos privados, generados con anterioridad a la utilización del sistema en relación con las personas físicas afectadas.

(18) El concepto de «sistema de reconocimiento de emociones» a que hace referencia el presente Reglamento debe definirse como un sistema de IA destinado a distinguir o deducir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos. El concepto se refiere a emociones o intenciones como la felicidad, la tristeza, la indignación,

gehitu edo moldatu ahal izateko; izan ere, iragazki horiek ezin dira erabili sare sozialetan lineako edukiak partekatzeko eskaintako zerbitzu nagusitik bereiz.

(17) Erregelamendu honetan aipatzen den «urruneko identifikazio biometrikoko sistemaren» kontzeptua honela definitu behar da modu funtzionalean: AA-sistema bat, helburu duena pertsona fisikoak haien parte-hartze aktiborik gabe (oro har, urrunetik) identifikatzea, haien datu biometrikoak erreferentziako datu-base batean agertzen direnekin alderatuta, edozein direla ere erabiltzen diren teknologia, prozesuak edo datu biometrikoen mota zehatzak. Urruneko identifikazio biometrikoko sistema hauek pertsona bat baino gehiago edo pertsona horien jarrerak aldi berean hautemateko erabiltzen dira, eta, hartara, nabarmen errazten dute pertsonen identifikazioa, haien parte-hartze aktiborik gabe. Kanpoan geratzen dira egiaztapen biometrikora bideratutako AA-sistemak —egiaztapenaren barruan autentifikazioa ere barne hartzen dutenak—, baldin eta sistema horien helburu bakarra bada pertsona fisiko baten identitatea hark esandakoarekin bat datorrela ziurtatzea edo pertsona fisiko baten identitatea xede jakin eta bakar baterako egiaztatzea, hala nola zerbitzu zehatz baterako sarbidea izateko, gailu bat desblokeatzeko edo lokal bateko segurtasun-sarbidea izateko. Sistema horiek kanpoan uzteko arrazoia da sistema horiek seguruenik eragin txikia dutela pertsona fisikoen oinarritzko eskubideetan, pertsona talde handien datu biometrikoak haien parte-hartze aktiborik gabe tratatzeko erabiltzen diren urruneko identifikazio biometrikoko beste sistema batzuekin alderatuta. «Denbora errealeko» sistemen kasuan, datu biometrikoen bilketa, konparazioa eta identifikazioa berehala egiten dira, edo ia berehala baina betiere atzerapen handirik gabe. Hori horrela, ezin da modurik egon erregelamendu honetako arauak saihesteko AA-sistemak «denbora errealean» erabiltzeko orduan atzerapen minimoak sortuta. «Denbora errealeko» sistemetan, «zuzeneko» materialak erabiltzen dira edo «ia zuzenekoak», hala nola bideo-grabazioak, kamera batekin edo antzeko gailuren batekin hartuak. Aldiz, «gerorako» sistemetan, datu biometrikoak aurrez bildu dira, eta atzerapen nabarmenez egiten da datuen konparazioa eta identifikazioa. Horretarako, ukitutako pertsona fisikoen irudiak, bideo-grabazioak eta halako materialak baliatzen dira, sistema erabili aurretik sortuak zirkuitu itxiko telebistako kameran bidez edo gailu pribatuen bidez.

(18) Erregelamendu honetan aipatzen den «emozioak ezagutzeko sistemaren» kontzeptua honela definitu behar da: AA-sistema bat, helburutzat duena pertsona fisikoen emozioak edo asmoak bereiztea edo ondorioztatzea pertsona horien datu biometrikotatik abiatuta. Zoriontasuna, tristura, sumina, harridura, nazka, estuasuna, gogo bizia, lotsa, mespretxua,



la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión. No incluye los estados físicos, como el dolor o el cansancio, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes. Tampoco incluye la mera detección de expresiones, gestos o movimientos que resulten obvios, salvo que se utilicen para distinguir o deducir emociones. Esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro.

(19) A los efectos del presente Reglamento, debe entenderse que el concepto de «espacio de acceso público» se refiere a cualquier espacio físico al que pueda acceder un número indeterminado de personas físicas y con independencia de si es de propiedad privada o pública y de la actividad para la que pueda utilizarse el espacio, ya sean actividades comerciales, por ejemplo, tiendas, restaurantes, cafeterías; de prestación de servicios, por ejemplo, bancos, actividades profesionales, hostelería; deportivas, por ejemplo, piscinas, gimnasios, estadios; de transporte, por ejemplo, estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte; de entretenimiento, por ejemplo, cines, teatros, museos, salas de conciertos, salas de conferencias; de ocio o de otro tipo, por ejemplo, vías y plazas públicas, parques, bosques, parques infantiles. Asimismo, debe considerarse que un espacio es de acceso público si, con independencia de posibles restricciones de capacidad o de seguridad, el acceso está sujeto a determinadas condiciones previamente definidas que puede satisfacer un número indeterminado de personas, como la adquisición de una entrada o un título de transporte, el registro previo o tener una determinada edad. Por el contrario, un espacio no debe considerarse de acceso público si únicamente pueden acceder a él determinadas personas físicas definidas, ya sea en virtud del Derecho de la Unión o del Derecho nacional directamente relacionado con la seguridad pública o en virtud de una clara manifestación de voluntad de la persona que ejerza la autoridad pertinente sobre dicho espacio. La posibilidad real de acceso, como una puerta no cerrada con llave o una verja abierta, no implica por sí sola que el espacio sea de acceso público si hay indicios o circunstancias que sugieran lo contrario, como señales que prohíban o restrinjan el acceso. Los locales de empresas y fábricas, así como las oficinas y lugares de trabajo a los que solo se pretende que accedan los empleados y proveedores de servicios pertinentes, no son espacios de acceso público. No deben incluirse en los espacios de acceso público las prisiones ni las zonas en que se realizan inspecciones fronterizas. Algunos espacios pueden incluir tanto zonas de acceso

gogobetetasuna, dibertimendua... Halako emozioak hartzen ditu. Kanpoan geratzen dira egoera fisikoak, hala nola oinazea edo nekea. Hala, esaterako, ez daude kontzeptu honen barruan istripuak saiheste aldera pilotuen edo gidari profesionalen nekea hautematen dituzten sistemak. Era berean, kanpoan geratzen da begi-bistakoak diren espresioen, keinuen eta mugimenduen hautemate hutsa, non eta ezaugarri horiek ez diren erabiltzen emozioak bereizteko edo ondorioztatzeko. Espresioak modu batekoak baino gehiagokoak izan daitezke: pertsonaren oinarritzko aurpegierak —hala nola bekozkoa edo irribarrea—, keinuak —esku, beso edo buruarekin egiten diren mugimenduak— edo ahotsaren ezaugarriak —ozenki hitz egitea edo xuxurlaka—.

(19) Erregelamendu honen ondorioetarako, «sarbide publikoko eremuaren» kontzeptua honela ulertu behar da: pertsona fisikoen kopuru zehaztugabe bat sartzeko moduko edozein eremu fisiko, alde batera utzita eremu hori jabetza pribatukoa edo publikokoa den eta zer jardueratarako erabil daitekeen; hor daude merkataritza-jarduerak (dendak, jatetxeak, kafetegiak eta abar), zerbitzu-jarduerak (bankuak, jarduera profesionalak, ostalaritza, etab.), kirol-jarduerak (igerilekuak, gimnasioak, estadioak, etab.), garraio-jarduerak (autobus-, metro- eta tren-geltokiak, aireportuak, garraiobideak, etab.), entretenimendu-jarduerak (zinemak, antzokiak, museoak, kontzertu-aretoak, hitzaldi-aretoak, etab.), aisialdikoak eta bestelakoak (bide eta plaza publikoak, parkeak, basoak, haur-parkeak, etab.). Eremu bat sarbide publikokoa izango da, baldin eta, edukiera- eta segurtasun-murritzketak gorabehera, sarbidea alde zehatzetik definitutako baldintza jakin batzuen mende badago eta baldintza horiek pertsona kopuru zehaztugabe batek betetzeko modukoak badira, hala nola sarrera bat edo garraio-título bat eskuratzea, aurretiaz erregistroa egitea edo adin jakin bat izatea. Aitzitik, eremu bat ez da sarbide publikokotzat hartu behar pertsona fisiko jakin eta zehatz batzuk bakarrik sar badaitezke, bai segurtasun publikoarekin zuzenean lotutako Batasuneko zuzenbidean edo zuzenbide nazionalen hala zehaztuta dagoelako, bai eremu horren gaineko agintaritza duen pertsonak argi eta garbi adierazi duelako horixe dela bere borondatea. Eremu batera sartzeko aukera edukitzeak—adibidez, atea ez dagoelako giltzaz itxita edo hesia irekita dagoelako—, izatez, ez du esan nahi eremua sarbide publikokoa denik, baldin eta eremua sarbide publikokoa ez dela iradokitzen duten zantzuak edo inguruabarrak badira, hala nola gunera sartzeari debekatzen edo mugatzen duten seinaleak. Enpresetako eta fabriketako lokalak, bulegoak eta languneak ez dira sarbide publikoko eremuak, langileei eta behar diren zerbitzuetako hornitzaileei bakarrik badagokie haietara sartzeari. Espetxeak eta mugetako ikuskapen-guneak ere ez dira sarbide publikoko eremuak. Eremu batzuetan, bietariko eremuak egon daitezke: sarbide publikokoak eta pribatukoak. Hori



público como zonas que no son de acceso público, como los aeropuertos o el vestíbulo de un edificio residencial privado por el que se accede a una consulta médica. Los espacios en línea no son lugares de acceso público, ya que no son espacios físicos. No obstante, se debe determinar caso por caso si un espacio es de acceso público o no teniendo en cuenta las particularidades de la situación concreta.

(20) Con el fin de obtener los mayores beneficios de los sistemas de IA, protegiendo al mismo tiempo los derechos fundamentales, la salud y la seguridad, y de posibilitar el control democrático, la alfabetización en materia de IA debe dotar a los proveedores, responsables del despliegue y personas afectadas de los conceptos necesarios para tomar decisiones con conocimiento de causa en relación con los sistemas de IA. Esos conceptos pueden variar en función del contexto pertinente e incluir el entendimiento de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA, las medidas que deben aplicarse durante su uso, las formas adecuadas de interpretar los resultados de salida del sistema de IA y, en el caso de las personas afectadas, los conocimientos necesarios para comprender el modo en que las decisiones adoptadas con la ayuda de la IA tendrán repercusiones para ellas. En el contexto de la aplicación del presente Reglamento, la alfabetización en materia de IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución. Además, la puesta en práctica general de medidas de alfabetización en materia de IA y la introducción de acciones de seguimiento adecuadas podrían contribuir a mejorar las condiciones de trabajo y, en última instancia, sostener la consolidación y la senda de innovación de una IA fiable en la Unión. El Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA») debe apoyar a la Comisión para promover las herramientas de alfabetización en materia de IA, la sensibilización pública y la comprensión de los beneficios, los riesgos, las salvaguardias, los derechos y las obligaciones en relación con el uso de sistemas de IA. En cooperación con las partes interesadas pertinentes, la Comisión y los Estados miembros deben facilitar la elaboración de códigos de conducta voluntarios para promover la alfabetización en materia de IA entre las personas que se ocupan del desarrollo, el manejo y el uso de la IA.

(21) Con el objetivo de garantizar la igualdad de condiciones y la protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas en el presente Reglamento deben aplicarse a los proveedores de sistemas de IA sin discriminación, con independencia de si están establecidos en la Unión o en un tercer país, y a los

gertatzen da, adibidez, aireportuetan, baita egoitza-erakin pribatu batzuetako atarian ere, atari horretatik igaro behar bada mediku-konsulta batera joateko. Lineako eremuak ez dira sarbide publikokoak, ez direlako eremu fisikoak. Dena dela, kasuz kasu zehaztu behar da eremu bat sarbide publikokoa den ala ez, egoera zehatz bakoitzaren berezitasunak kontuan hartuta.

(20) AA-sistemei ahalik eta etekin handienak ateratzeko eta, aldi berean, oinarritzko eskubideak, osasuna eta segurtasuna babesteko eta kontrol demokratikoa ahalbidetzeko, beharrezkoa da bai hornitzaileak eta hedapenaren arduradunak, bai ukitutako pertsonak AAren arloan alfabetatzea, behar diren kontzeptuak bereganatu ditzaten AA-sistemei buruzko erabakiak jakinaren gainean hartu ahal izateko. Kontzeptu horiek desberdinak izan daitezke testuinguruaren arabera, eta barruan har ditzakete, adibidez, egokiro ulertzea nola aplikatu behar diren osagai teknikoak AA-sistemak garatzeko fasean, zer neurri aplikatu behar diren sistema erabiltzeko orduan, nola interpretatu egokiro AA-sistemen irteera-emaizak eta, ukitutako pertsonen kasuan, zer ezagutza behar dituzten egokiro ulertzeko nola eragingo dieten AAren laguntzaz hartutako erabakiek. Erregelamendu honen aplikazioari begira, AAren arloko alfabetatzeak behar dituzten ezagutzak eman behar dizkie AAren balio-kate barruan egoki diren eragile guztiei, behar bezala betetzen eta gauzatzen dela bermatzeko. Gainera, AAren arloan alfabetatzeko neurriak abian jartzea eta jarraipen-ekintzak txertatzea lagungarria gerta daiteke lan-baldintzak hobetzeko eta, azken batez, Batasunean AA fidagarri bat sustraitzen dela eta arlo honetan berrikuntzaren bidetik aurrera jarraitzen dela bermatzeko. Adimen Artifizialaren Europako Kontseiluak (aurrerantzean, «AA-kontseilua») babesa eman behar dio Batzordeari bultzada eman dakien AAren arloko alfabetatze-tresnei, sentsibilizazio publikoari eta AA-sistemen erabilerak dakartzan onura, arrisku, babes, eskubide eta betebeharren ulermenari. Egoki diren alderdi interesdunekin lankidetzan, Batzordeak eta estatu kideek borondatezko jokabide-kodeak egin daitezkeen bultzatu behar dute, AAren garapenaz, maneiuaz eta erabileraz arduratzen diren pertsonen artean AAren arloko alfabetatzea sustatzeko.

(21) Batasun osoan pertsonen baldintza-berdintasuna eta eskubide eta askatasunen babes eraginkorra bermatzeko, erregelamendu honetan ezarritako arauak bereizkeriarik gabe aplikatu behar zaizkie bai AA-sistemen hornitzaileei —Batasunean kokatuta egon zein



responsables del despliegue de sistemas de IA establecidos en la Unión.

(22) Debido a su carácter digital, algunos sistemas de IA deben entrar en el ámbito de aplicación del presente Reglamento aunque no se introduzcan en el mercado, se pongan en servicio ni se utilicen en la Unión. Esto sucede, por ejemplo, cuando un operador establecido en la Unión firma con un operador establecido en un tercer país un contrato para la prestación de determinados servicios en relación con una actividad que llevará a cabo un sistema de IA que se consideraría de alto riesgo. En dichas circunstancias, el sistema de IA usado en un tercer país por el operador podría tratar datos recabados lícitamente en la Unión y transferidos desde su territorio, y proporcionar al operador contratante ubicado en la Unión los resultados de salida generados por dicho sistema de IA a raíz de este tratamiento sin que el sistema de IA de que se trate se introduzca en el mercado, se ponga en servicio o se utilice en la Unión. Para evitar la elusión de este Reglamento y garantizar la protección efectiva de las personas físicas ubicadas en la Unión, el presente Reglamento también debe aplicarse a los proveedores y responsables del despliegue de sistemas de IA establecidos en un tercer país, en la medida en que los resultados de salida generados por dichos sistemas estén destinados a utilizarse en la Unión. No obstante, con el objetivo de tener en cuenta los acuerdos existentes y las necesidades especiales de cooperación futura con socios extranjeros con los que se intercambian información y pruebas, el presente Reglamento no debe aplicarse a las autoridades públicas de un tercer país ni a organizaciones internacionales cuando actúen en el marco de acuerdos internacionales o de cooperación celebrados a escala nacional o de la Unión con fines de cooperación policial y judicial con la Unión o sus Estados miembros si el tercer país o la organización internacional correspondiente ofrece garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas. Cuando proceda, ello podrá incluir las actividades de entidades a las que los terceros países hayan encomendado tareas específicas en apoyo de dicha cooperación policial y judicial. Dichos marcos de cooperación o acuerdos se han establecido bilateralmente entre los Estados miembros y terceros países o entre la Unión Europea, Europol y otros órganos de la Unión y terceros países y organizaciones internacionales. Las autoridades competentes para la supervisión de las autoridades policiales y judiciales en virtud del presente Reglamento deben evaluar si dichos marcos de cooperación o acuerdos internacionales incluyen garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas. Las autoridades nacionales y las instituciones, órganos y organismos de la Unión que sean destinatarios de dichos resultados de salida y que la utilicen en la Unión siguen siendo responsables de

hirugarren herrialde batean— baita Batasunean ezarritako AA-sistemen hedapenaren arduradunei ere.

(22) Digitalak direnez gero, AA-sistema batzuk erregelamendu honen aplikazio-eremuan sartu behar dira, nahiz eta Batasunean merkatuan jarri ez, zerbitzuan ipini ez eta erabili ez. Hala gertatzen da, esaterako, Batasunean ezarritako operadore batek kontratu bat sinatzen duenean hirugarren herrialde batean ezarritako operadore batekin, zerbitzu jakin batzuk eman ditzan arrisku handikotzat jotzekoa den AA-sistema baten bidez jardura bat egiteko. Egoera horretan, gerta liteke operadoreak hirugarren herrialde batean erabiltzen duen AA-sistemak Batasunean legez bildutako eta bere lurraldetik transferitutako datuak tratatzea, eta AA-sistema horrek tratamendu horren ondorioz sortutako irteera-emaizak ematea Batasunean kokatutako operadore kontratatzaileari, baliatutako AA-sistema hori Batasunean erabili gabe, merkatuan jarri gabe edo zerbitzuan ipini gabe. Erregelamendu hau saihesteko modua egon ez dadin eta Batasunean kokatutako pertsona fisikoek babes eraginkorra izan dezaten, hirugarren herrialde batean ezarritako AA-sistemen hornitzaileei eta sistema horien hedapenaren arduradunei ere aplikatuko zaie erregelamendu hau, sistema horiek sortutako irteera-emaizak Batasunean erabiltzekoak badira. Dena dela, atzerriko bazkideekin egindako informazio- eta saiakera- trukeko akordioak aintzat hartzeko eta etorkizuneko lankidetzak-premia bereziei erantzuteko, erregelamendu hau ez zaie aplikatu behar ez hirugarren herrialde bateko agintaritzak publikoei, ezta nazioarteko antolakundeei ere, nazioarteko akordioen edo lankidetzak-akordioen esparruan dihardutenean, akordioak estatu kideek egin zein Batasunak egin, helburua lankidetzak poliziala eta judiziala denean, izan Batasunarekin, izan estatu kideekin, baldin eta hirugarren herrialdeak edo nazioarteko antolakundeak berme nahikoa eskaintzen badu pertsonen oinarritzko eskubideak eta askatasunak babesteko. Egoki denean, baldintza horren barruan sartu ahal izango dira hirugarren herrialdeen eskariz lankidetzak polizial eta judizial horri laguntzeko zeregin zehatzak egiten ari diren entitateen jarduerak. Lankidetzak-esparru edo akordio horiek aldebikoak dira: estatu kideen eta hirugarren herrialdeen artekoak, batetik, eta Europar Batasunaren, Europol eta Batasuneko beste organo batzuen eta hirugarren herrialdeen eta nazioarteko antolakundeen artekoak, bestetik. Erregelamendu honen arabera agintaritzak polizial eta judizialak ikuskatzeko eskumena duten agintaritzen egitekoa izango da aztertzea ea nazioarteko lankidetzak-esparru edo akordio horiek berme nahikorik ematen duten pertsonen oinarritzko eskubideak eta askatasunak babesteko. Agintaritzak nazionalak eta Batasuneko instituzio, organo eta organismoek, irteera-emaizak horien hartzaile diren heinean eta Batasunean erabiltzen dituzten heinean, ardura izaten jarraituko dute bermatzeko informazioaren erabilera Batasuneko zuzenbidearekin bat datorrela. Etorkizunean nazioarteko



garantizar que su utilización de la información está en consonancia con el Derecho de la Unión. Cuando, en el futuro, dichos acuerdos internacionales se revisen o se celebren otros nuevos, las partes contratantes deben hacer todo lo posible por que dichos acuerdos se ajusten a los requisitos del presente Reglamento.

(23) El presente Reglamento también debe aplicarse a las instituciones, órganos y organismos de la Unión cuando actúen como proveedores o responsables del despliegue de un sistema de IA.

(24) En caso de que, y en la medida en que, los sistemas de IA se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificación, con fines militares, de defensa o de seguridad nacional, deben excluirse del ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades, por ejemplo, con independencia de que se trate de una entidad pública o de una entidad privada. Por lo que respecta a los fines militares y de defensa, dicha exclusión está justificada tanto por el artículo 4, apartado 2, del TUE como por las especificidades de la política de defensa de los Estados miembros y de la política común de defensa de la Unión a que se refiere el título V, capítulo 2, del TUE, que están sujetas al Derecho internacional público que, por lo tanto, es el marco jurídico más adecuado para la regulación de los sistemas de IA en el contexto del uso de la fuerza letal y de otros sistemas de IA en el contexto de las actividades militares y de defensa. Por lo que respecta a los fines de seguridad nacional, la exclusión está justificada tanto por el hecho de que la seguridad nacional sigue siendo responsabilidad exclusiva de los Estados miembros de conformidad con el artículo 4, apartado 2, del TUE, como por la naturaleza específica y las necesidades operativas de las actividades de seguridad nacional y por las normas nacionales específicas aplicables a dichas actividades. No obstante, si un sistema de IA desarrollado, introducido en el mercado, puesto en servicio o utilizado con fines militares, de defensa o de seguridad nacional se utilizara temporal o permanentemente fuera de estos ámbitos con otros fines (por ejemplo, con fines civiles o humanitarios, de garantía del cumplimiento del Derecho o de seguridad pública), dicho sistema entraría en el ámbito de aplicación del presente Reglamento. En tal caso, la entidad que utilice el sistema de IA con fines que no sean militares, de defensa o de seguridad nacional debe garantizar que el sistema de IA cumple lo dispuesto en el presente Reglamento, a menos que el sistema ya lo haga. Los sistemas de IA introducidos en el mercado o puestos en servicio para un fin excluido, a saber, militar, de defensa o de seguridad nacional, y uno o varios fines no excluidos, como fines civiles o de garantía del cumplimiento del Derecho, entran en el ámbito de aplicación del presente Reglamento y los proveedores de dichos sistemas deben garantizar el

akordio horiek berrikusten direnean edo beste batzuk egiten direnean, alderdi kontratugileak ahal beste ahaleginduko dira akordio horiek bat etor daitezen erregelamendu honetako betekizunekin.

(23) Erregelamendu hau Batasuneko instituzio, organo eta organismoei ere aplikatu behar zaie, AA-sistema baten hornitzaile edo hedapenaren arduradun gisa jarduten dutenean.

(24) AA-sistemak erregelamendu honen aplikazio-eremutik kanpo geratuko dira, baldin eta helburuak militarrek, defentsakoak edo segurtasun nazionalekoak izanda merkatuan jartzen, zerbitzuan ipintzen eta erabiltzen badira, moldatuta zein ez, edozein dela ere jarduera horiek egiten dituen entitatea —adibidez, entitate publikoa izan daiteke, zein pribatua—. Helburuak militarrek eta defentsakoak direnean, AA-sistemen arauketa erregelamendu honetatik salbuesteko egoera hori justifikatuta dago, bai EBTren 4.2 artikuluan, bai estatu kideen defentsa-politikaren eta Batasunaren defentsa-politika erkidearen berezitasunetan (EBTren V. tituluko 2. kapituluaren aipatuak), zeinak nazioarteko zuzenbide publikoaren mende baitaude; hala, zuzenbide hori da esparru juridiko egokiena AA-sistemen erabilera arautzeko, indar hilgarria erabiltzea eskatzen duten jardueren zein jarduera militar eta defentsa-jardueren testuinguruan. Segurtasun nazionaleko helburuak direnean, berriz, salbueste-egoera hori justifikatuta dago, batetik segurtasun nazionala estatu kideen erantzukizun eksklusiboa delako EBTren 4.2 artikulua araberak, eta, bestetik, segurtasun nazionaleko jarduerak izaera berezia eta beharizan operatibo zehatzak dituztelako eta jarduera horiei arau nazional jakinak aplikatzen zaizkielako. Dena dela, helburu militar edo defentsakoekin edo segurtasun nazionaleko helburuekin merkatuan jarri, zerbitzuan ipini eta erabiltzeko AA-sistema bat denbora batez edo etengabe beste helburu batzuekin erabiltzen bada (adibidez, helburu zibil edo humanitarioekin edo zuzenbidea betearazteko edo segurtasun publikoa bermatzeko helburuekin), sistema hori erregelamendu honen aplikazio-eremuan sartuko da. Halakoetan, entitate batek militarrek, defentsakoak edo segurtasun nazionalekoak ez diren helburuekin erabiltzen badu AA-sistema hori, entitateak berak bermatu beharko du AA-sistemak erregelamendu honetan xedatzen dena betetzen duela, baldin eta sistemak berak jada bermatzen ez badu. Merkatuan jarri, zerbitzuan ipini eta erabiltzen den AA-sistema batek bietariko helburuak baditu, hau da, erregelamendu honetatik kanpo geratutako helburuetako bat (helburu militar, defentsakoa edo segurtasun nazionalekoa) eta erregelamenduari dagokion helbururen bat (hala nola helburu zibilak edo zuzenbidea betearaztekoak), orduan, sistema hori erregelamendu honen aplikazio-eremuan sartuko da, eta sistema horren hornitzaileek



cumplimiento del presente Reglamento. En esos casos, el hecho de que un sistema de IA pueda entrar en el ámbito de aplicación del presente Reglamento no debe afectar a la posibilidad de que las entidades que llevan a cabo actividades militares, de defensa y de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades, utilicen sistemas de IA con fines de seguridad nacional, militares y de defensa, cuyo uso está excluido del ámbito de aplicación del presente Reglamento. Un sistema de IA introducido en el mercado con fines civiles o de garantía del cumplimiento del Derecho que se utilice, con o sin modificaciones, con fines militares, de defensa o de seguridad nacional no debe entrar en el ámbito de aplicación del presente Reglamento, independientemente del tipo de entidad que lleve a cabo esas actividades.

(25) El presente Reglamento debe apoyar la innovación, respetar la libertad de ciencia y no socavar la actividad de investigación y desarrollo. Por consiguiente, es necesario excluir de su ámbito de aplicación los sistemas y modelos de IA desarrollados específicamente y puestos en servicio únicamente con fines de investigación y desarrollo científicos. Además, es necesario garantizar que el presente Reglamento no afecte de otro modo a la actividad de investigación y desarrollo científicos sobre sistemas o modelos de IA antes de su introducción en el mercado o su puesta en servicio. Por lo que se refiere a la actividad de investigación, prueba y desarrollo orientada a productos en relación con sistemas o modelos de IA, las disposiciones del presente Reglamento tampoco deben aplicarse antes de que dichos sistemas y modelos se pongan en servicio o se introduzcan en el mercado. Esa exclusión se entiende sin perjuicio de la obligación de cumplir el presente Reglamento cuando se introduzca en el mercado o se ponga en servicio como resultado de dicha actividad de investigación y desarrollo un sistema de IA que entre en el ámbito de aplicación del presente Reglamento, así como de la aplicación de disposiciones sobre espacios controlados de pruebas para la IA y pruebas en condiciones reales. Además, sin perjuicio de la exclusión de los sistemas de IA desarrollados específicamente y puestos en servicio únicamente con fines de investigación y desarrollo científicos, cualquier otro sistema de IA que pueda utilizarse para llevar a cabo cualquier actividad de investigación y desarrollo debe seguir estando sujeto a las disposiciones del presente Reglamento. En cualquier caso, toda actividad de investigación y desarrollo debe llevarse a cabo de conformidad con normas éticas y profesionales reconocidas para la investigación científica y con el Derecho aplicable de la Unión.

(26) Con el fin de establecer un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, es preciso aplicar un enfoque basado en los riesgos claramente definido, que adapte el tipo y contenido de

erregelamendu hau betetzen dela bermatu beharko dute. Halakoetan, AA-sistema bat erregelamendu honen aplikazio-eremuan sartzeak ez du oztopo izan behar jarduera militarrek, defentsakoak edo segurtasun nazionalekoak egiten dituzten entitateek, edozein motatakoak direla ere, AA-sistema segurtasun nazionaleko helburuekin edo helburu militar eta defentsakoekin erabili ahal izateko, erabilera hori erregelamendu honen aplikazio-eremutik kanpo egonda. Helburu zibilekin edo zuzenbidea betearazteko helburuekin merkatuan jarritako AA-sistema bat, baldin eta helburu militar edo defentsakoekin edo segurtasun nazionaleko helburuekin erabiltzen bada, moldatuta zein ez, ez da erregelamendu honen aplikazio-eremuan sartu behar, edozein dela ere jarduera horiek egiten dituen entitate mota.

(25) Erregelamendu honek berrikuntza babestu behar du, zientzia-askatasuna errespetatu eta kalterik ez ekarri ikerketa- eta garapen-jarduerari. Horrenbestez, erregelamendu honen aplikazio-eremutik kanpo utzi behar dira ikerketa eta garapen zientifikorako soilik berariaz garatutako eta zerbitzuan ipinitako AA-sistemak eta -ereduak. Gainera, bermatu behar da erregelamendu honek ez diola beste modu batera eragiten AA-sistemen edo -ereduen gaineko ikerketa eta garapen zientifikoari sistema eta eredu horiek merkatuan jarri edo zerbitzuan ipini aurretik. AA-sistemei edo -ereduei lotutako produktuetara bideratutako ikerketa-, proba- eta garapen-jarduerari dagokionez, erregelamendu honetako xedapenak ez dira aplikatu behar sistema eta eredu horiek zerbitzuan ipini edo merkatuan jarri aurretik. Nolanahi ere, salbuespen horrek ez du eragotziko erregelamendu hau bete behar izatea ikerketa-, proba- eta garapen-jarduera horren ondorioz erregelamendu honen aplikazio-eremuan sartzen den AA-sistema bat jartzen denean merkatuan edo ipintzen denean zerbitzuan; era berean, ez du eragotziko AArako proba-ingurune arautuei eta baldintza errealeko probei buruzko xedapenak aplikatzea ere. Gainera, ikerketa eta garapen zientifikoko helburu hutsekin berariaz garatutako eta zerbitzuan ipinitako AA-sistemak erregelamendu honen aplikazio-eremutik kanpo uztekoak badira ere, ikerketa eta garapeneko edozein jarduera egiteko baliatutako beste AA-sistemek erregelamendu honen xedapenei lotuta jarraitu behar dute. Nolanahi ere, ikerketa- eta garapen-jarduerak egiteko orduan, beti bete beharrekoak dira ikerketa zientifikorako aintzatetsitako arau etikoak eta profesionalak, baita aplikatzekoa den Batasuneko zuzenbidea ere.

(26) AA-sistemetarako arau lotesleen multzo proportzionatu eta eraginkorra ezartzeko, beharrezkoa da arriskueta oinarritutako ikuspegia aplikatzea; ikuspegi horrek argi eta garbi definituta egon behar du,



las normas a la intensidad y el alcance de los riesgos que puedan generar los sistemas de IA de que se trate. Por consiguiente, es necesario prohibir determinadas prácticas de IA que no son aceptables, definir los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes, así como imponer obligaciones de transparencia a determinados sistemas de IA.

(27) Si bien el enfoque basado en el riesgo es la base de un conjunto proporcionado y eficaz de normas vinculantes, es importante recordar las Directrices éticas para una IA fiable, de 2019, elaboradas por el Grupo independiente de expertos de alto nivel sobre IA creado por la Comisión. En dichas directrices, el Grupo independiente de expertos de alto nivel sobre IA desarrolló siete principios éticos no vinculantes para la IA que tienen por objeto contribuir a garantizar la fiabilidad y el fundamento ético de la IA. Los siete principios son: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental, y rendición de cuentas. Sin perjuicio de los requisitos jurídicamente vinculantes del presente Reglamento y de cualquier otro acto aplicable del Derecho de la Unión, esas directrices contribuyen al diseño de una IA coherente, fiable y centrada en el ser humano, en consonancia con la Carta y con los valores en los que se fundamenta la Unión. De acuerdo con las directrices del Grupo independiente de expertos de alto nivel sobre IA, por «acción y supervisión humanas» se entiende que los sistemas de IA se desarrollan y utilizan como herramienta al servicio de las personas, que respeta la dignidad humana y la autonomía personal, y que funciona de manera que pueda ser controlada y vigilada adecuadamente por seres humanos. Por «solidez técnica y seguridad» se entiende que los sistemas de IA se desarrollan y utilizan de manera que sean sólidos en caso de problemas y resilientes frente a los intentos de alterar el uso o el funcionamiento del sistema de IA para permitir su uso ilícito por terceros y reducir al mínimo los daños no deseados. Por «gestión de la privacidad y de los datos» se entiende que los sistemas de IA se desarrollan y utilizan de conformidad con normas en materia de protección de la intimidad y de los datos, al tiempo que tratan datos que cumplen normas estrictas en términos de calidad e integridad. Por «transparencia» se entiende que los sistemas de IA se desarrollan y utilizan de un modo que permita una trazabilidad y explicabilidad adecuadas, y que, al mismo tiempo, haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA e informe debidamente a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos. Por «diversidad, no discriminación y equidad» se entiende que los sistemas de IA se desarrollan y utilizan de un

eta egokiro moldatu behar ditu arauen mota eta edukia kasuan kasuko AA-sistemek sor ditzaketen arriskuen intentsitatera eta irismenera. Horrenbestez, beharrezkoa da onargarriak ez diren AA-jardunbideak debekatzea, arrisku handiko AA-sistemek bete beharreko betekizunak zehaztea, operadoreei aplikatzekoak zaizkien betebeharrak finkatzea eta AA-sistema jakin batzuei gardentasun-betebeharrak ezartzea.

(27) Nahiz eta arriskuan funtsatutako ikuspegia oinarri den arau lotesleen multzo proportzionatu eta eraginkor baterako, garrantzitsua da AArako Gidalerro Etikoak gogora ekartzea: Batzordeak AAren arlorako sortutako goi-mailako adituen talde independente batek eratu zituen 2019an, eta, gidalerro horietan, AAri buruzko goi-mailako adituen talde independente horrek AArako zazpi printzipio etiko ez-lotesle garatu zituen, AAren fidagarritasuna eta oinarri etikoa bermatzen laguntzeko. Hona zazpi printzipioak: giza ekintza eta giza ikuskapena; sendotasun teknikoa eta segurtasuna; pribatutasunaren eta datuen kudeaketa; gardentasuna; aniztasuna, diskriminaziorik eza eta ekitatea; gizarte- eta ingurumen-ongizatea, eta kontuak ematea. Erregelamendu honetan jasotako betekizun juridikoki lotesleak gorabehera eta Batasuneko zuzenbidearen arabera aplikatzekoa den beste edozein egintza eragotzi gabe, gidalerro horiek lagungarriak dira gizakian oinarritutako AA koherente eta fidagarri bat diseinatzeko, bat etorrita Batasunaren Gutunarekin eta balioekin, Batasunaren ardatz izanik. AAri buruzko goi-mailako adituen talde independentearen gidalerroen arabera, «giza ekintza eta giza ikuskapenaren» printzipioak adierazten du ezen AA-sistemak gizakion zerbitzura egoteko tresna izateko garatzen eta erabiltzen direla, giza duintasuna eta pertsonen autonomia errespetatuta, eta gizakiok kontrolatu eta behatu ahal izateko moduan funtzionatzen dutela. «Sendotasun teknikoaren eta segurtasunaren» printzipioak, berriz, esan nahi du AA-sistemak egokiro garatzen eta erabiltzen direla arazoan aurrean sendoak izan daitezen eta erresilienteak izan daitezen inor sistema horien erabilera edo funtzionamendua aldatzen saiatuz gero hirugarren batzuek erabilera ez-zilegia emateko, minimora murriztuta nahi gabeko kalteak. «Pribatutasunaren eta datuen kudeaketaren» printzipioak aditzera ematen du AA-sistemak intimitatea eta datuak babesteko arauarekin bat etorrita garatzen eta erabiltzen direla eta, aldi berean, tratatzen diren datuek arau zorrotzak betetzen dituztela kalitateari eta segurtasunari begira. «Gardentasunaren» printzipioak, berriz, esaten du ezen AA-sistemak trazabilitatea eta esplikagarritasuna izateko moduan garatzen eta erabiltzen direla, aldi berean bidea emanda pertsonak ohartu daitezen AA-sistema batekin ari direla komunikatzen eta harremana izaten eta informazio egokia emanda hedapenaren arduradunei AA-sistemak berak dituen gaitasunez eta mugez, eta ukitutako pertsonen, berriz, haien eskubideez. «Dibertsitatearen,



modo que incluya a diversos agentes y promueve la igualdad de acceso, la igualdad de género y la diversidad cultural, al tiempo que se evitan los efectos discriminatorios y los sesgos injustos prohibidos por el Derecho nacional o de la Unión. Por «bienestar social y ambiental» se entiende que los sistemas de IA se desarrollan y utilizan de manera sostenible y respetuosa con el medio ambiente, así como en beneficio de todos los seres humanos, al tiempo que se supervisan y evalúan los efectos a largo plazo en las personas, la sociedad y la democracia. La aplicación de esos principios debe traducirse, cuando sea posible, en el diseño y el uso de modelos de IA. En cualquier caso, deben servir de base para la elaboración de códigos de conducta en virtud del presente Reglamento. Se anima a todas las partes interesadas, incluidos la industria, el mundo académico, la sociedad civil y las organizaciones de normalización, a que tengan en cuenta, según proceda, los principios éticos para el desarrollo de normas y mejores prácticas voluntarias.

(28) Al margen de los múltiples usos beneficiosos de la IA, esta también puede utilizarse indebidamente y proporcionar nuevas y poderosas herramientas para llevar a cabo prácticas de manipulación, explotación y control social. Dichas prácticas son sumamente perjudiciales e incorrectas y deben estar prohibidas, pues van en contra de los valores de la Unión de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho y de los derechos fundamentales consagrados en la Carta, como el derecho a la no discriminación, a la protección de datos y a la intimidad y los derechos del niño.

(29) Las técnicas de manipulación que posibilita la IA pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados o para engañarlas empujándolas a tomar decisiones de una manera que socava y perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente. Son especialmente peligrosos y, por tanto, deben prohibirse la introducción en el mercado, la puesta en servicio o la utilización de determinados sistemas de IA con el objetivo o al efecto de alterar de manera sustancial el comportamiento humano, con la consiguiente probabilidad de que se produzcan perjuicios considerables, en particular perjuicios con efectos adversos suficientemente importantes en la salud física o mental o en los intereses financieros. Esos sistemas de IA utilizan componentes subliminales, como estímulos de audio, imagen o vídeo que las personas no pueden percibir —ya que dichos estímulos trascienden la percepción humana—, u otras técnicas manipulativas o engañosas que socavan o perjudican la autonomía, la toma de decisiones o la capacidad de elegir libremente

diskriminaziorik ezaren eta ekitatearen» printzipioak adierazten du ezen AA-sistemak halako moduan garatzen eta erabiltzen direla non bide ematen duten askotariko eragileak barne hartzeko eta sarbide-berdintasuna, genero-berdintasuna eta kultura-aniztasuna sustatzeko, aldi berean itzuri eginez zuzenbide nazionalean edo Batasuneko zuzenbidean debekatutako eragin diskriminatzaileei eta alborapen bidegabei. «Gizarte- eta ingurumen-ongizatearen» printzipioak, azkenik, aditzera ematen du AA-sistemak modu jasangarrian, ingurumenarekiko errespetuz eta gizaki guztiei onura egiteko moduan garatzen eta erabiltzen direla, aldi berean pertsonengan, gizartean eta demokrazian epe luzera izan ditzaketen eraginak aztertuz eta ebaluatuz. Printzipio horien aplikazioa, ahal denean, AA-ereduen diseinuan eta erabileran islatu behar da, eta lagungarriak izan behar dute beti, erregelamendu honen arabera jokabide-kodeak eratzeko. Alderdi interesdun guztiei bultzatzen zaie —barnean direla industria, mundu akademikoa, gizarte zibila eta normalizazio-antolakundeak— kontuan izan ditzaten, dagokien heinean, arauak eratzeko eta borondatezko jardunbide egokienak garatzeko printzipio etikoak.

(28) AArek erabilera onuragarriak ugari izanda ere, bidegabe ere erabil daiteke, eta tresna berri eta boteretsuak eman ditzake gizarte manipulatzeko, ustiatzeko eta kontrolatzeko jardunbideak egiteko. Jardunbide horiek izugarri kaltegarriak eta okerrak dira, eta debekatuta egon behar dute, ez baitituzte errespetatzen Batasunaren balioak —hau da, giza duintasuna, askatasuna, berdintasuna, demokrazia eta zuzenbide-estatua— ez eta Gutunean ezarritako oinarritzko eskubideak ere —hor dira diskriminaziorik ez jasateko eskubidea, datuen babeserako eskubidea eta intimitate-eskubidea eta haurren eskubideak—.

(29) AAk ahalbidetzen dituen manipulazio-teknikek aukera ematen dute pertsonak limurtzeko portaera okerrak edo erabaki galgarriak har ditzaten, eta, hartara, urradura eta kaltea eragin pertsonen autonomiari eta askatasunez aukeratzeko gaitasunari. Bereziki arriskutsuak dira giza portaera erroto aldatzeko helburua duten AA-sistemak, eta, beraz, halako sistemak ezin zaie utzi ez merkatuan jartzen, ez zerbitzuan ipintzen, ez erabiltzen; izan ere, sistema horiek kalte nabarmenak eragin ditzakete, bereziki osasunaren arloan, ondorio galgarri garrantzitsuak utz baititzaizkete pertsonen osasun fisiko zein mentalean, bai, halaber, finantza-interesetan ere. AA-sistema horiek osagai subliminalak erabiltzen dituzte —pertsonak hauteman ezin dituzten audio-, irudi- edo bideo-estimuluak adibidez, estimulu horiek giza pertzepzioa gainditzen baitute— eta beste manipulazio-teknika edo teknika engainagarri batzuk ere bai, kaltetu edo ahuldu egiten dutenak pertsonen autonomiaz jokatzeko, erabakiak hartzeko edo askatasunez aukeratzeko duten gaitasuna; pertsonak, gainera, ez dira egiazki jabetzen teknika



de las personas de maneras de las que estas no son realmente conscientes de dichas técnicas o, cuando lo son, pueden seguir siendo engañadas o no pueden controlarlas u oponerles resistencia. Esto podría facilitarse, por ejemplo, mediante interfaces cerebro-máquina o realidad virtual, dado que permiten un mayor grado de control acerca de qué estímulos se presentan a las personas, en la medida en que pueden alterar sustancialmente su comportamiento de un modo que suponga un perjuicio considerable. Además, los sistemas de IA también pueden explotar de otras maneras las vulnerabilidades de una persona o un colectivo específico de personas derivadas de su edad, su discapacidad en el sentido de lo dispuesto en la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo (16) o de una situación social o económica concreta que probablemente aumente su vulnerabilidad a la explotación, como vivir en condiciones de pobreza extrema o pertenecer a minorías étnicas o religiosas. Estos sistemas de IA pueden introducirse en el mercado, ponerse en servicio o utilizarse con el objetivo de alterar de manera sustancial el comportamiento de una persona, o tener ese efecto, y de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra persona o colectivo de personas, incluidos perjuicios que pueden acumularse a lo largo del tiempo y que, por tanto, deben prohibirse. No puede presuponerse que existe la intención de alterar el comportamiento si la alteración es el resultado de factores externos al sistema de IA que escapan al control del proveedor o del responsable del despliegue, a saber, factores que no es lógico prever y que, por tanto, el proveedor o el responsable del despliegue del sistema de IA no pueden mitigar. En cualquier caso, no es necesario que el proveedor o el responsable del despliegue tengan la intención de causar un perjuicio considerable, siempre que dicho perjuicio se derive de las prácticas de manipulación o explotación que posibilita la IA. La prohibición de tales prácticas de IA complementa lo dispuesto en la Directiva 2005/29/CE del Parlamento Europeo y del Consejo (17), en particular la prohibición, en cualquier circunstancia, de las prácticas comerciales desleales que causan perjuicios económicos o financieros a los consumidores, hayan sido establecidas mediante de sistemas de IA o de otra manera. La prohibición de las prácticas de manipulación y explotación establecida en el presente Reglamento no debe afectar a prácticas lícitas en el contexto de un tratamiento médico, como el tratamiento psicológico de una enfermedad mental o la rehabilitación física, cuando dichas prácticas se lleven a cabo de conformidad con el Derecho y las normas médicas aplicables, por ejemplo, con el consentimiento expreso de las personas o de sus representantes legales. Asimismo, no debe considerarse que las prácticas comerciales comunes y legítimas (por ejemplo, en el campo de la publicidad) que cumplan el Derecho

horien erabileraz, edo, jabetuta ere, teknika horien eraginpean jarraitzen dute, haien eragina kontrolatu ezinik edo kontra egin ezinik. Egoera hori bideratzeko, burmuina-makina interfazeak edo errealtate birtuala erabil daitezke, modua ematen baitute hobeto kontrolatzeko zer-nolako estimuluak eragiten zaizkien pertsoneri, estimulu horiek errotik aldaraz baitezakete pertsonen portaera, eta, ondorioz, kalte handia eragin. AA-sistemek, gainera, beste modu batzuetara ere ustia ditzakete pertsona baten edo kolektibo jakin baten kalteberatasunak, direla adinak eragindakoak, direla desgaitasunek eragindakoak —Europako Parlamentuaren eta Kontseiluaren 2019/882 (EB) Zuzentarauan xedatutakoaren arabera (16)— edo direla egoera sozial edo ekonomikoak eragindakoak; izan ere, egoera horietan, litekeena izaten da pertsona horiek are kalteberago bihurtzea ustiaketaren aurrean, adibidez muturreko pobrezian bizi direnean edo gutxiengo etniko edo erlijiosoetako kide direnean. Gerta liteke pertsona baten portaera errotik aldarazteko jartzea merkatuan, ipintzea zerbitzuan edo erabiltzea AA-sistemak —edo sistemek eragin hori izatea— eta, ondorioz, pertsona horri edo beste pertsona bati edo kolektibo bati kalte nabarmenak eragitea —edo kalte nabarmenak eragiteko probabilitate argia egotea— eta kalte horiek, batzuetan, luzaroan metatzea; halakoetan, bada, sistema horiek debekatu egin behar dira. Ezin da aurrez jo portaera aldarazteko asmoa dagoenik, aldaketa hori AA-sistemetatik kanpoko faktoreen emaitza bada eta faktore horiek ez badaude hornitzailearen edo hedapenaren arduradunaren kontrolpean; adibidez, senez aurreikusteko moduko faktoreak ez direnean eta, beraz, AA-sistemaren hornitzaileak edo hedapenaren arduradunak ezin dituenean leundu. Nolanahi ere, ez da beharrezkoa hornitzaileak edo hedapenaren arduradunak kalte nabarmena eragiteko asmoa izatea, baldin eta AAK ahalbidetzen dituen manipulazio- edo ustiapen-jardunbideetatik eratoritzen bada kalte hori. AA-jardunbide horiek debekatzeko osatu egiten du Europako Parlamentuaren eta Kontseiluaren 2005/29/EE Zuzentarauan xedatutakoa (17). Debeku hau aipatzekoa da, bereziki: AA-sistemen bidez edo bestelako moduren batean, jardunbide komertzial desleialak egitea, egoera edozein dela ere, kalte ekonomiko eta finantzarioak eragiten dizkieten heinean kontsumitzaileei. Erregelamendu honetan ezarritako manipulazio- edo ustiapen-jardunbideak debekatzeko ez du eraginik izan behar tratamendu medikoetako bidezko jardunbideetan, hala nola gaixotasun mental baterako tratamendu psikologikoan edo errehabilitazio fisikoan, baldin eta jardunbide horiek garatzeko egokiro betetzen badira bai zuzenbidean ezarritako xedapenak, bai aplikatzekoak diren arau medikoak, hala nola pertsonen edo haien legezko ordezkarien berariazko adostasuna izanda. Era berean, ezin da jo zuzenbidea betetzen duten ohiko eta bidezko jardunbide komertzialak (adibidez, publizitatearen esparrukoak), berez, AAK



aplicable son, en sí mismas, prácticas de manipulación perjudiciales que posibilita la IA.

(30) Deben prohibirse los sistemas de categorización biométrica basados en datos biométricos de las personas físicas, como la cara o las impresiones dactilares de una persona física, para deducir o inferir las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona física. Dicha prohibición no debe aplicarse al etiquetado, al filtrado ni a la categorización lícitos de conjuntos de datos biométricos adquiridos de conformidad con el Derecho nacional o de la Unión en función de datos biométricos, como la clasificación de imágenes en función del color del pelo o del color de ojos, que pueden utilizarse, por ejemplo, en el ámbito de la garantía del cumplimiento del Derecho.

(31) Los sistemas de IA que permiten a agentes públicos o privados llevar a cabo una puntuación ciudadana de las personas físicas pueden tener resultados discriminatorios y abocar a la exclusión a determinados colectivos. Pueden menoscabar el derecho a la dignidad y a la no discriminación y los valores de igualdad y justicia. Dichos sistemas de IA evalúan o clasifican a las personas físicas o a grupos de estas sobre la base de varios puntos de datos relacionados con su comportamiento social en múltiples contextos o de características personales o de su personalidad conocidas, inferidas o predichas durante determinados períodos de tiempo. La puntuación ciudadana resultante de dichos sistemas de IA puede dar lugar a un trato perjudicial o desfavorable de determinadas personas físicas o colectivos enteros en contextos sociales que no guardan relación con el contexto donde se generaron o recabaron los datos originalmente, o a un trato perjudicial desproporcionado o injustificado en relación con la gravedad de su comportamiento social. Por lo tanto, deben prohibirse los sistemas de IA que impliquen esas prácticas inaceptables de puntuación y den lugar a esos resultados perjudiciales o desfavorables. Esa prohibición no debe afectar a prácticas lícitas de evaluación de las personas físicas que se efectúen para un fin específico de conformidad con el Derecho de la Unión y nacional.

(32) El uso de sistemas de IA para la identificación biométrica remota «en tiempo real» de personas físicas en espacios de acceso público con fines de garantía del cumplimiento del Derecho invade de forma especialmente grave los derechos y las libertades de las personas afectadas, en la medida en que puede afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia

bideratutako manipulazioko jardunbide kaltegarriak direnik.

(30) Kategorizazio biometrikoko sistemak debekatzekoak dira, pertsona fisikoen datu biometrikotan oinarritzen badira —hala nola pertsona fisiko baten aurpegian edo hatz-marketan— pertsona fisiko baten iritzi politikoa, afiliazio sindikala, sinesmen erlijioso edo filosofikoa, arraza, bizitza sexuala edo orientazio sexuala ondorioztatzeko edo inferitzeko. Debeku hori ez da aplikatzekoa zuzenbide nazionalaren edo Batasuneko zuzenbidearen arabera eskuratutako datu biometrikoen multzoak bidezkoa den moduan etiketatzen, iragazten eta kategorizatzen direnean datu biometrikoen arabera; adibidez, irudiak ilearen kolorearen edo begien kolorearen arabera sailkatzen direnean zuzenbidea betearazteko eremuan.

(31) Eragile publiko edo pribatuei pertsona fisikoen puntuatze soziala egiteko aukera ematen dieten AA-sistemek diskriminazioa eragin dezakete eta zenbait kolektibo bazterrarazi. Era berean, duintasunerako eta diskriminaziorik ezerako eskubidea kaltetu dezakete eta berdintasun- eta justizia-balioak andeatu. AA-sistema horiek pertsona fisikoak edo pertsona taldeak ebaluatzen edo sailkatzen dituzte, zenbait datu-puntu oinarritzat hartuta. Datu-puntu horiek lotuta daude pertsonak askotariko testuinguruetan hartzen duten portaera sozialarekin, ezaugarri pertsonalekin edo izaeraren ezaugarriekin, denboraldi zehatz batean hauteman, ondorioztatu edo aurreikusitakoaren arabera. AA-sistema horien bidez lortzen den puntuatze sozialak bide eman dezake pertsona fisiko jakin batzuek edo kolektibo osoek trataera kaltegarria eta okerra jasotzeko gizarte-testuinguru batzuetan, testuinguru horiek inolako harremanik izan gabe ere hasieran datuak jasotzeko edo sortzeko baliatutako testuinguruarekin; edo gerta daiteke, halaber, jasotako tratua kaltegarria neurritz kanpokoa edo bidegabea izatea, pertsona edo kolektibo horren portaera sozialaren larritasun-maila kontuan izanda. Horregatik, bada, AA-sistema horiek debekatu beharrekoak dira, puntuazio-jardunbide onartezinak dituzten heinean eta ondorio kaltegarri eta okerrak eragiten dituzten heinean. Debeku horrek ez du eraginik izan behar pertsona fisikoak ebaluatzeko bidezko jardunbideetan, Batasuneko zuzenbidearekin eta zuzenbide nazionalarekin bat datorren helburu jakin batekin egiten diren heinean.

(32) Zuzenbidea betearazteko helburuz AA-sistemak erabiltzen direnean sarbide publikoko eremuetan pertsona fisikoen «denbora errealean egiten den» urruneko identifikazio biometrikoa egiteko, larriki urratzen dira ukitutako pertsonen eskubideak eta askatasunak; izan ere, jardunbide horrek biztanleriaren zati handi baten bizitza pribatuari eragin diezaioke eta etengabe zaintzapean daudelako sentsazioa sortu, eta



constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales. Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica remota de las personas físicas pueden dar lugar a resultados sesgados y tener efectos discriminatorios. Tales posibles resultados sesgados y efectos discriminatorios son especialmente pertinentes por lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. Además, la inmediatez de las consecuencias y las escasas oportunidades para realizar comprobaciones o correcciones adicionales en relación con el uso de sistemas que operan «en tiempo real» acrecientan el riesgo que estos conllevan para los derechos y las libertades de las personas afectadas en el contexto de actividades de garantía del cumplimiento del Derecho, o afectadas por estas.

(33) En consecuencia, debe prohibirse el uso de dichos sistemas con fines de garantía del cumplimiento del Derecho, salvo en situaciones enumeradas de manera limitativa y definidas con precisión en las que su utilización sea estrictamente necesaria para lograr un interés público esencial cuya importancia compense los riesgos. Esas situaciones son la búsqueda de determinadas víctimas de un delito, incluidas personas desaparecidas; determinadas amenazas para la vida o para la seguridad física de las personas físicas o amenazas de atentado terrorista; y la localización o identificación de los autores o sospechosos de los delitos enumerados en un anexo del presente Reglamento, cuando dichas infracciones se castiguen en el Estado miembro de que se trate con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años, y como se definan en el Derecho de dicho Estado miembro. Fijar ese umbral para la pena o la medida de seguridad privativas de libertad con arreglo al Derecho nacional contribuye a garantizar que la infracción sea lo suficientemente grave como para llegar a justificar el uso de sistemas de identificación biométrica remota «en tiempo real». Por otro lado, la lista de delitos proporcionada en un anexo del presente Reglamento se basa en los treinta y dos delitos enumerados en la Decisión Marco 2002/584/JAI del Consejo (18), si bien es preciso tener en cuenta que, en la práctica, es probable que algunas sean más relevantes que otras en el sentido de que es previsible que recurrir a la identificación biométrica remota «en tiempo real» podría ser necesario y proporcionado en grados muy distintos para llevar a cabo la localización o la identificación de los autores o sospechosos de las distintas infracciones enumeradas, y que es probable que haya diferencias en la gravedad, la probabilidad y la magnitud de los perjuicios o las posibles consecuencias negativas. Una amenaza inminente para la vida o la seguridad física de las personas físicas también podría derivarse de una perturbación grave de infraestructuras críticas, tal como

biltzeko askatasuna eta beste oinarritzko eskubide batzuk baliatzetik gibelatu ditzake herritarrak zeharka. Pertsona fisikoen urruneko identifikazio biometrikorako AA-sistemen zehaztugabetasun teknikoek emaitza alboratuak eragin ditzakete eta ondorio diskriminatzaileak ekarri. Gerta daitezkeen emaitza alboratu eta diskriminazio-ondorio horiek bereziki eragiten diete adinari, etniari, arrazari, sexuari edo desgaitasunari. «Denbora errealean» jarduten duten sistemen kasuan, ondorioak berehalakoak izanda eta aukera gutxi egonda erabilerari buruzko egiaztapenak egiteko edo zuzenketak gehitzeko, sistema hauek are arriskutsuagoak dira zuzenbidea betearazteko jardueren eremuan ukitutako pertsonen edo haien eraginpeko pertsonen eskubide eta askatasunei begira.

(33) Ondorioz, debekatu egin behar da sistema horiek zuzenbidea betearazteko erabiltzea, salbu eta zehatz-mehatz mugatutako eta doitasun handiz zehaztutako egoeretan, sistema horiek erabiltzea guztiz beharrezkoa delako funtsezko interes publiko bat lortze aldera eta helburu horren garrantziak arriskua hartzea merezi duelako. Hauek dira salbuespeneko egoerak: delitu baten biktima jakin batzuk bilatzea —desagertutako pertsonak barne—; pertsona fisikoen segurtasun fisikorako edo bizitzarako mehatxu jakin batzuk edo atentatu terroristen mehatxuak hautematea, eta erregelamendu honen eranskin batean zerrendatutako delituen egileak edo susmagarriak lokalizatzea eta identifikatzea, arau-hauste horiek gutxienez lau urteko gehieneko denboraz askatasunaz gabetzeko zigor edo segurtasun-neurri batekin zigortzen badira dagokion estatu kidean, estatu horretako zuzenbidean zehaztutako eran. Zuzenbide nazionalaren arabera askatasunaz gabetzeko zigor edo segurtasun-neurrian denbora-muga jakin hori finkatuta zera bermatu nahi da: arau-haustea behar besteko larritasuna izan dezala, justifikatuta egon dadin «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak erabiltzea. Bestalde, erregelamendu honen eranskin batean jasotako delituen zerrenda Kontseiluaren 2002/584/JAI Esparru Erabakian (18) zerrendatutako hogeita hamabi delituetan oinarritzen da; nolanahi ere, praktikan, litekeena da delitu horietako batzuk beste batzuk baino esanguratsuagoak izatea, eta, horrenbestez, pentsatzekoa da «denbora errealean egiten den» urruneko identifikazio biometrikora jotzea ez litzatekeela beti modu berean beharrezkoa eta neurrikoa zerrendatutako arau-hausteen egileak edo susmagarriak lokalizatzeo eta identifikatzeko, eta balitekeela aldeak egotea kalteen edo ondorio kaltegarrien larritasunean, probabilitatean eta muntan. Pertsona fisikoen bizitza edo segurtasun fisikoa bat-batean mehatxatuta gerta daitezke, larriki asaldatu direlako azpiegitura kritikoak, Europako Parlamentuaren eta Kontseiluaren (EB) 2022/2557 Zuzentarauaren 2. artikulua 4. puntuan



se definen en el artículo 2, punto 4, de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo (19), cuando la perturbación o destrucción de dichas infraestructuras críticas suponga una amenaza inminente para la vida o la seguridad física de una persona, también al perjudicar gravemente el suministro de productos básicos a la población o el ejercicio de la función esencial del Estado. Además, el presente Reglamento debe preservar la capacidad de las autoridades garantes del cumplimiento del Derecho, de control fronterizo, de la inmigración o del asilo para llevar a cabo controles de identidad en presencia de la persona afectada, de conformidad con las condiciones establecidas en el Derecho de la Unión y en el Derecho nacional para estos controles. En particular, las autoridades garantes del cumplimiento del Derecho, del control fronterizo, de la inmigración o del asilo deben poder utilizar sistemas de información, de conformidad con el Derecho de la Unión o el Derecho nacional, para identificar a las personas que, durante un control de identidad, se nieguen a ser identificadas o no puedan declarar o demostrar su identidad, sin que el presente Reglamento exija que se obtenga una autorización previa. Puede tratarse, por ejemplo, de una persona implicada en un delito que no quiera revelar su identidad a las autoridades garantes del cumplimiento del Derecho, o que no pueda hacerlo debido a un accidente o a una afección médica.

(34) Para velar por que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en esas situaciones enumeradas de manera limitativa y definidas con precisión, se tengan en cuenta determinados elementos, en particular en lo que se refiere a la naturaleza de la situación que dé lugar a la solicitud, a las consecuencias que su uso puede tener sobre los derechos y las libertades de todas las personas implicadas, y a las garantías y condiciones que acompañen a su uso. Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho debe llevarse a cabo únicamente para confirmar la identidad de la persona que constituya el objetivo específico y limitarse a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal, teniendo en cuenta, en particular, las pruebas o indicios relativos a las amenazas, las víctimas o los autores. El uso del sistema de identificación biométrica remota en tiempo real en espacios de acceso público solo debe autorizarse si la correspondiente autoridad garante del cumplimiento del Derecho ha llevado a cabo una evaluación de impacto relativa a los derechos fundamentales y, salvo que se disponga otra cosa en el presente Reglamento, si ha registrado el sistema en la base de datos establecida en el presente Reglamento. La base de datos de personas

definitutako moduan (19), azpiegitura kritiko horiek asaldatzeak edo suntsitzeak berehalako mehatxua dakarrenean pertsona baten bizitza edo segurtasun fisikorako, edo asaldura horrek larriki kaltetzen dituenean biztanleriarentzako oinarritzko produktuen hornidura edo Estatuaren funtsezko eginkizuna. Gainera, erregelamendu honek zaindu egin behar du zuzenbidea betearazteaz, muga-kontrolaz, immigrazioaz edo asiloaz arduratzen diren agintaritzek gaitasuna dutela identitate-kontrolak egiteko ukitutako pertsonaren aurrean, Batasuneko zuzenbidean eta zuzenbide nazionalan kontrol horietarako ezarritako baldintzekin bat etorritz. Zuzenbidea betearazteaz, muga-kontrolaz, immigrazioaz edo asiloaz arduratzen diren agintaritzek, zehazki, pertsonak identifikatzeko informazio-sistemak erabiltzeko modua izan behar dute, Batasuneko zuzenbidea eta zuzenbide nazionala beteta beti, baldin eta identitate-kontrol batean uko egiten badiote identifikatzeari edo ezin badute beren identitatea azaldu edo demostratu. Erregelamendu honek ez du eskatuko identifikazio horretarako alde aurreko baimena edukitzeko beharra izatea. Esate baterako, gerta liteke delitu batean inplikaturako pertsona batek bere burua identifikatu nahi ez izatea zuzenbidea betearazteko agintaritzaren aurrean; edo gerta liteke pertsona horrek bere burua ezin identifikatu ahal izatea, istripua izan duelako edo gaitzen bat duelako.

(34) Sistema horiek modu arduratsuan eta proportzionatuan erabiltzen direla zaintzeko, garrantzitsua da, halaber, xeheki zerrendatutako eta zorrotz zehaztutako egoeren zerrenda horretan elementu jakin batzuk kontuan hartzea, bereziki arlo hauei dagokienez: eskaera eragin duen egoera zein den, baliabide hori erabiltzeak zer ondorio izan ditzakeen inplikaturako pertsona guztien eskubide eta askatasunetan eta baliabide hori zer berme eta baldintzapean erabiltzen den. Gainera, zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak erabiltzen direnean, xede zehatza den pertsonaren identitatea konfirmatzeko soilik erabili behar dira, eta behar-beharrezko denborara eta eremu geografiko zein pertsonalera mugatu, zorrotz kontuan hartuta mehatxuen, biktimen edo egileen gaineko frogak eta zantzuak. Sarbide publikoko eremuetan denbora errealean egiten den urruneko identifikazio biometrikoko sistemak erabiltzeko baimena emateko, ezinbestekoa izango da zuzenbidea betearazteko agintaritzak aurrez ebaluatzea zer inpaktu izango duen baliabide horrek oinarritzko eskubideetan; era berean, beharrezkoa izango da sistema erregelamendu honetan ezarritako datu-basean erregistratzea, salbu eta erregelamendu honek beste zeozer xedatzen badu. Pertsonen erreferentziarako datu-baseak egokia izan behar du arestian aipatutako egoera bakoitzerako erabilera-kasu bakoitzerako.



de referencia debe ser adecuada para cada supuesto de uso en cada una de las situaciones antes mencionadas.

(35) Todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho debe haber sido autorizado de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro y cuya decisión sea vinculante. En principio, dicha autorización debe obtenerse antes de utilizar el sistema de IA con el fin de identificar a una o varias personas. Deben permitirse excepciones a esa norma en situaciones debidamente justificadas por motivos de urgencia, a saber, en aquellas en las que la necesidad de utilizar los sistemas de que se trate sea tan imperiosa que resulte efectiva y objetivamente imposible obtener una autorización antes de iniciar el uso del sistema de IA. En tales situaciones de urgencia, el uso debe limitarse al mínimo imprescindible y satisfacer las garantías y condiciones oportunas, conforme a lo dispuesto en el Derecho nacional y según corresponda en cada supuesto concreto de uso urgente por parte de la propia autoridad garante del cumplimiento del Derecho. Además, en esas situaciones las autoridades garantes del cumplimiento del Derecho deben solicitar dicha autorización e indicar los motivos por los que no han podido hacerlo antes, sin demora indebida y, como máximo, en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso de sistemas de identificación biométrica en tiempo real vinculados a la autorización debe interrumpirse con efecto inmediato y todos los datos relacionados con dicho uso deben desecharse y suprimirse. Entre esos datos se incluyen los datos de entrada directamente adquiridos por un sistema de IA durante el uso de dicho sistema, así como los resultados y la información de salida del uso vinculados a dicha autorización. No debe incluir la información de entrada adquirida legalmente de conformidad con otro acto del Derecho nacional o de la Unión. En cualquier caso, no debe adoptarse ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota.

(36) A fin de desempeñar sus funciones de conformidad con los requisitos establecidos en el presente Reglamento, así como en las normas nacionales, debe notificarse a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos cada uso del sistema de identificación biométrica en tiempo real. Las autoridades de vigilancia del mercado y las autoridades nacionales de protección de datos que hayan recibido una notificación deben presentar a la Comisión un informe anual sobre el uso de sistemas de identificación biométrica en tiempo real.

(35) Zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak erabiltzeko, agintaritza judizial batek edo estatu kide bateko administrazio-agintaritza independente batek berariaz eta espezifikoki baimendu beharko du aurrez erabilera hori, eta agintaritza horren erabakia loteslea izango da. Pertsona bat edo batzuk identifikatzeko baimen hori, printzipioz, AA-sistema erabili aurretik lortu behar da. Arau horrek salbuespenak eduki ahal izango ditu behar bezala justifikatutako urgentziatzko arrazoiengatik: adibidez, sistema horiek erabiltzea hain premiazkoa denean non eta guztiz ezinezkoa baita baimena lortzea AA-sistema erabiltzen hasi aurretik. Urgentziatzko egoera horietan, ezinbesteko gutxienezko kasuetara murriztu behar da erabilera hori eta betiere egoki diren bermeak eta baldintzak bete, zuzenbide nazionalaren arabera eta zuzenbidea betearazteko agintaritza bakoitzari urgentziatzko kasu zehatz horietako bakoitzean dagokion moduan. Gainera, egoera horietan, zuzenbidea betearazteko agintaritzek baimen hori eskatu behar dute eta azaldu zergatik ezin izan duten lehenago eskatu. Eskatera hori bidegabeko atzerapenik gabe egin behar dute eta, gehienez ere, hogeita lau orduko epean. Baimena ukatzen bada, berehala utzi behar zaio baimen horri lotutako denbora errealean egiten den identifikazio biometrikoko sistema erabiltzeari, eta erabilera horri dagozkion datu guztiak bota eta ezabatu behar dira. Datu horien barruan daude AA-sistemaren erabileraren bidez zuzenean lortutako sarrera-datuak, baita baimen horri lotuta erabileran lortutako irteera-emaizak eta -informazioa ere. Kanpoan geratzen da zuzenbide nazionalaren edo Batasuneko zuzenbidearen beste egintza bati lortuta legezt lortutako sarrera-informazioa. Zernahi gisaz, ez da sekula hartu behar pertsona bati ondorio juridiko kaltegarriak eragingo dizkion erabakirik urruneko identifikazio biometrikoko sistemaren irteera-emaizetan soilik oinarrituta.

(36) Eginkizunak erregelamendu honetan eta estatuko arauetan ezarritako betekizunen arabera betetzeko, denbora errealean egiten den identifikazio biometrikoko sistemaren erabilera bakoitza jakinarazi behar zaie bai merkatua zaintzeko agintaritzari, bai datuak babesteko agintaritza nazionalari. Merkatua zaintzeko agintaritzek eta datuak babesteko agintaritza nazionalak, jakinarazpena jasoz gero, denbora errealean egiten den identifikazio biometrikoko sistemen erabilerari buruzko urteko txostena aurkeztu behar diote Batzordeari.



(37) Por otro lado, conviene disponer, en el marco exhaustivo que establece este Reglamento, que dicho uso en el territorio de un Estado miembro conforme a lo dispuesto en el presente Reglamento solo debe ser posible cuando el Estado miembro de que se trate haya decidido contemplar expresamente la posibilidad de autorizarlo en las normas detalladas de su Derecho nacional, y en la medida en que lo haya contemplado. En consecuencia, con arreglo al presente Reglamento los Estados miembros siguen teniendo la libertad de no ofrecer esta posibilidad en absoluto o de ofrecerla únicamente en relación con algunos de los objetivos que pueden justificar un uso autorizado conforme al presente Reglamento. Dichas normas nacionales deben notificarse a la Comisión en un plazo de treinta días a partir de su adopción.

(38) La utilización de sistemas de IA para la identificación biométrica remota en tiempo real de personas físicas en espacios de acceso público con fines de garantía del cumplimiento del Derecho implica, necesariamente, el tratamiento de datos biométricos. Las normas del presente Reglamento que prohíben, con algunas excepciones, ese uso, basadas en el artículo 16 del TFUE, deben aplicarse como *lex specialis* con respecto a las normas sobre el tratamiento de datos biométricos que figuran en el artículo 10 de la Directiva (UE) 2016/680, con lo que se regula de manera exhaustiva dicho uso y el tratamiento de los correspondientes datos biométricos. Por lo tanto, ese uso y tratamiento deben ser posibles únicamente en la medida en que sean compatibles con el marco establecido por el presente Reglamento, sin que haya margen, fuera de dicho marco, para que las autoridades competentes, cuando actúen con fines de garantía del cumplimiento del Derecho, utilicen tales sistemas y traten dichos datos en los supuestos previstos en el artículo 10 de la Directiva (UE) 2016/680. En ese sentido, el presente Reglamento no tiene por objeto proporcionar la base jurídica para el tratamiento de datos personales en virtud del artículo 8 de la Directiva (UE) 2016/680. Sin embargo, el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines distintos de la garantía del cumplimiento del Derecho, también por parte de las autoridades competentes, no debe estar sujeto al marco específico establecido por el presente Reglamento en lo que respecta al uso de dichos sistemas con fines de garantía del cumplimiento del Derecho. Por consiguiente, su uso con fines distintos de la garantía del cumplimiento del Derecho no debe estar sujeto al requisito de obtener una autorización previsto en el presente Reglamento ni a las normas de desarrollo aplicables del Derecho nacional que puedan hacer efectiva dicha autorización.

(39) Todo tratamiento de datos biométricos y de datos personales de otra índole asociado al uso de sistemas de IA para la identificación biométrica, salvo el asociado al uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines

(37) Bestalde, erregelamendu honek ezartzen duen esparru zehatzean, Erregelamenduan xedatutakoaren arabera denbora errealean egiten den identifikazio biometrikoko sistema estatu kide baten lurraldean erabiltzeko, ezinbestekoa izango da estatu horrek bere zuzenbide nazionalen zehaztutako arauetan berariaz jasota edukitzea erabilera hori baimentzen duela, eta arau horietan aurreikusitako neurri horretantxe erabili ahal izango da. Ondorioz, erregelamendu honen arabera, estatu kideek askatasuna dute erabilera hori inolaz ere ez baimentzeko, edo bakar-bakarrik erregelamendu honen arabera baimendutako erabilera justifikatu dezaketen helburu jakin batzuetarako onesteko. Estatuko arau horiek Batzordeari jakinarazi behar zaizkio arauak hartu eta hogeita hamar eguneko epean.

(38) Zuzenbidea betearazteko helburuz AA-sistemak erabiltzen direnean sarbide publikoko eremuetan pertsona fisikoen denbora errealean egiten den urruneko identifikazio biometrikoa egiteko, datu biometrikokoak tratatu egin behar dira ezinbestean. Erregelamendu honetan erabilera hori —salbuespen batzuekin— debekatzen duten arauak, EBFTren 16. artikuluan oinarrituak, *lex specialis* gisa aplikatu behar dira, (EB) 2016/680 Zuzentarauaren 10. artikuluan jasotako datu biometrikoen tratamenduari buruzko arauei dagokienez, hartara zehatz-mehatz araututa datu biometrikoen erabilera eta tratamendua. Hortaz, erabilera eta tratamendu horiek erregelamendu honetan ezarritako esparruarekin bateragarri diren heinean bakarrik izan behar dute posible, eta esparru horretatik at ez da aukerarik egon behar agintaritza eskudunek zuzenbidea betearazteko helburuarekin dihardutela sistema horiek erabili edo datu horiek trata ditzaten (EB) 2016/680 Zuzentarauaren 10. artikuluan aurreikusitako kasuetan. Hala, bada, ez da erregelamendu honen helburua oinarri juridikoa ematea datu pertsonalak (EB) 2016/680 Zuzentarauaren 8. artikuluan arabera tratatzeko. Ordea, sarbide publikoko eremuetan denbora errealean egiten den urruneko identifikazio biometrikoko sistemak zuzenbidea betearazteaz bestelako helburuekin erabiltzen badira —erabiltzaileak agintaritza eskudunak izanda ere—, erabilera hori ez da sartu behar erregelamendu honetan sistema horiek zuzenbidea betearazteko erabiltzeari buruz ezarritako esparru espezifikoan. Ondorioz, sistema horiek zuzenbidea betearazteaz bestelako helburuekin erabili ahal izatea ez dago lotuta baimen bat lortzeko betekizunarekin —erregelamendu honetan aurreikusitako betekizuna—, ez eta baimen hori gauzatu ditzaketen zuzenbide nazionalaren garapen-arauekin ere.

(39) Urruneko identifikazio biometrikoko AA-sistemen erabilerari lotutako datu biometrikoen eta bestelako datu pertsonalen tratamendu orok —salbuespen dela zuzenbidea betearazteko sarbide publikoko eremuetan denbora errealean egiten den urruneko identifikazio



de garantía del cumplimiento del Derecho regulado por el presente Reglamento, debe seguir cumpliendo todos los requisitos derivados del artículo 10 de la Directiva (UE) 2016/680. El artículo 9, apartado 1, del Reglamento (UE) 2016/679 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725 prohíben el tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho, con las excepciones limitadas previstas en dichos artículos. En la aplicación del artículo 9, apartado 1, del Reglamento (UE) 2016/679, el uso de la identificación biométrica remota para fines distintos de la garantía del cumplimiento del Derecho ya ha sido objeto de decisiones de prohibición por parte de las autoridades nacionales de protección de datos.

(40) De conformidad con el artículo 6 bis del Protocolo n.º 21 sobre la Posición del Reino Unido y de Irlanda respecto del Espacio de Libertad, Seguridad y Justicia, anejo al TUE y al TFUE, las normas establecidas en el artículo 5, apartado 1, párrafo primero, letra g), en la medida en que se aplica al uso de sistemas de categorización biométrica para actividades en el ámbito de la cooperación policial y la cooperación judicial en materia penal, el artículo 5, apartado 1, párrafo primero, letra d), en la medida en que se aplica al uso de sistemas de IA comprendidos en el ámbito de aplicación de dicho artículo, el artículo 5, apartado 1, párrafo primero, letra h), y apartados 2 a 6, y el artículo 26, apartado 10, del presente Reglamento, adoptadas basándose en el artículo 16 del TFUE que se refieran al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, de dicho Tratado solo serán vinculantes para Irlanda en la medida en que sean vinculantes para este Estado normas de la Unión que regulen formas de cooperación judicial en materia penal y de cooperación policial en cuyo marco deban respetarse las disposiciones establecidas basándose en el artículo 16 del TFUE.

(41) De conformidad con lo dispuesto en los artículos 2 y 2 bis del Protocolo n.º 22 sobre la Posición de Dinamarca, anejo al TUE y al TFUE, las normas establecidas en el artículo 5, apartado 1, párrafo primero, letra g), en la medida en que se aplica al uso de sistemas de categorización biométrica para actividades en el ámbito de la cooperación policial y la cooperación judicial en materia penal, el artículo 5, apartado 1, párrafo primero, letra d), en la medida en que se aplican al uso de sistemas de IA comprendidos en el ámbito de aplicación de dicho artículo, el artículo 5, apartado 1, párrafo primero, letra h), y apartados 2 a 6, y el artículo 26, apartado 10, del presente Reglamento, adoptadas sobre la base del artículo 16 del TFUE que se refieran al tratamiento de datos de carácter personal por los Estados miembros en el

biometrikoko sistemak erabiltzearekin lotutako tratamendua, erregelamendu honetan arautua— (EB) 2016/680 Zuzentarauaren 10. artikulutik eratorritako betekizun guztiak betetzen jarraitu behar du. (EB) 2016/679 Erregelamenduaren 9.1 artikulua eta (EB) 2018/1725 Erregelamenduaren 10.1 artikulua debekatu egiten dute datu biometrikoak bestelako helburu batzuetarako erabiltzea zuzenbidea betearaztetik at — salbuespen dira artikulua horietan aurreikusitako egoera mugatuak—. (EB) 2016/679 Erregelamenduaren 9.1 artikulua aplikatuz, datuen babeserako agintaritzak nazionalak, honezkero, debekua ezarri izan diote urruneko identifikazio biometrika zuzenbidea betearaztetik at bestelako helburu batzuetarako erabiltzeari.

(40) Aintzat hartuta Erresuma Batuak eta Irlandak askatasun-, segurtasun- eta justizia-esparruari buruz duten Jarreraren gaineko 21. Protokoloaren 6 bis artikulua (EBTren eta EBFTren eranskina), Irlandarentzat lotesleak diren heinean EBFTren 16. artikuluan oinarrituta ezarritako xedapenak errespetatu beharrekotzat dituzten zigor-arloko lankidetzak judizialerako eta polizia-lankidetzarako moduak arautzen dituzten Batasuneko arauak, hein horretan bakarrik izango dira lotesleak Irlandarentzat honako arau hauek: erregelamendu honen 5.1 artikuluko lehenengo paragrafoko g) letran ezarritako arauak —polizia-lankidetzaren eta zigor-arloko lankidetzak judizialaren eremuko jardueretarako kategorizazio biometrikoko sistemen erabilerari aplikatzen zaizkion heinean—, 5.1 artikuluko lehenengo paragrafoko d) letran ezarritakoak —artikulu horren aplikazio-eremuan sartzen diren AA-sistemen erabilerari aplikatzen zaion heinean—, erregelamendu honen 5.1 artikuluko lehenengo paragrafoko h) letra eta 26.10 artikuluko 2. apartatutik 6.era bitartean ezarritakoak, guztiak ere EBFTren 16. artikuluan oinarrituta hartutakoak, tratatu horren hirugarren ataleko V. tituluko 4. edo 5. kapituluak jasotako jardueretan estatu kideek datu pertsonalak tratatzeari buruzkoak diren heinean.

(41) Aintzat hartuta Danimarkak askatasun-, segurtasun- eta justizia-esparruari buruz duen Jarreraren gaineko 22. Protokoloaren 2. eta 2 bis artikulua (EBTren eta EBFTren eranskina), arau hauek ez dira lotesleak eta aplikagarriak izango Danimarkarentzat: erregelamendu honen 5.1 artikuluko lehenengo paragrafoko g) letran ezarritako arauak —polizia-lankidetzaren eta zigor-arloko lankidetzak judizialaren eremuko jardueretarako kategorizazio biometrikoko sistemen erabilerari aplikatzen zaizkion heinean—, 5.1 artikuluko lehenengo paragrafoko d) letran ezarritakoak —artikulu horren aplikazio-eremuan sartzen diren AA-sistemen erabilerari aplikatzen zaion heinean—, erregelamendu honen 5.1 artikuluko lehenengo paragrafoko h) letra eta 26.10 artikuluko 2. apartatutik 6.era bitartean ezarritakoak, guztiak ere



ejercicio de las actividades comprendidas en el ámbito de aplicación de la tercera parte, título V, capítulos 4 o 5, de dicho Tratado, no vincularán a Dinamarca ni le serán aplicables.

(42) En consonancia con la presunción de inocencia, las personas físicas de la Unión siempre deben ser juzgadas basándose en su comportamiento real. Las personas físicas nunca deben ser juzgadas a partir de comportamientos predichos por una IA basados únicamente en la elaboración de sus perfiles, en los rasgos o características de su personalidad, como la nacionalidad, el lugar de nacimiento, el lugar de residencia, el número de hijos, el nivel de endeudamiento o el tipo de vehículo, sin una valoración humana y sin que exista una sospecha razonable, basada en hechos objetivos comprobables, de que dicha persona está implicada en una actividad delictiva. Por lo tanto, deben prohibirse las evaluaciones de riesgos realizadas con respecto a personas físicas para evaluar la probabilidad de que cometan un delito o para predecir la comisión de un delito real o potencial basándose únicamente en la elaboración de perfiles de esas personas físicas o la evaluación de los rasgos y características de su personalidad. En cualquier caso, dicha prohibición no se refiere o atañe a los análisis de riesgos que no estén basados en la elaboración de perfiles de personas o en los rasgos y características de la personalidad de las personas, como los sistemas de IA que utilizan los análisis de riesgos para evaluar la probabilidad de fraude financiero por parte de empresas sobre la base de transacciones sospechosas o las herramientas de análisis de riesgo para predecir la probabilidad de localización de estupefacientes y mercancías ilícitas por parte de las autoridades aduaneras, por ejemplo basándose en las rutas de tráfico conocidas.

(43) La introducción en el mercado, la puesta en servicio para ese fin concreto o la utilización de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales a partir de internet o de imágenes de circuito cerrado de televisión deben estar prohibidas, pues esas prácticas agravan el sentimiento de vigilancia masiva y pueden dar lugar a graves violaciones de los derechos fundamentales, incluido el derecho a la intimidad.

(44) Existe una gran preocupación respecto a la base científica de los sistemas de IA que procuran detectar o deducir las emociones, especialmente porque la expresión de las emociones varía de forma considerable entre culturas y situaciones, e incluso en una misma persona. Algunas de las deficiencias principales de estos sistemas son la fiabilidad limitada, la falta de especificidad y la limitada posibilidad de generalizar. Por consiguiente, los sistemas de IA que detectan o

EBFTren 16. artikuluan oinarrituta hartutakoak, tratatu horren hirugarren ataleko V. tituluko 4. edo 5. kapituluari jasotako jardueretan estatu kideek datu pertsonalak tratatzeari buruzkoak diren heinean.

(42) Errugabetasun-presuntzioarekin bat etorritik, Batasuneko pertsona fisikoak haien benetako portaeran oinarrituta epaitu behar dira beti. Pertsona fisikoak ez dira inoiz epaitu behar AA batek aurreikusitako portaeretan funtsatuta; izan ere, AA-sistemek, portaerak aurreikusteko, pertsonen profilak egiten dituzte, nortasunaren bereizgarri edo ezaugarri jakinak hartuta, hala nola nazionalitatea, jaiotzea, bizilekua, seme-alaben kopurua, zorpetze-maila edota ibilgailu mota, gizakia bera balioetsi gabe edo arrazoizko susmorik egon gabe gertaera objektibo egiaztagarrietan oinarrituta pertsona hori delitu-jarduera batean inplikaturik dagoela pentsatzeko. Hortaz, debekatu egin behar dira pertsona fisikoaren gaineko arrisku-ebaluazioak, ebaluazio horien helburua denean neurtzea ea pertsona horiek zer probabilitate duten delitu bat egiteko edo aurreikustea delitu erreala bat edo potentzial bat egingo ote duten, oinarri bakartzat hartuta pertsona fisikoaren gaineko profilaketa edo haien nortasunaren bereizgarrien eta ezaugarrien ebaluazioa. Pertsonen profilaketan edo pertsonen nortasunaren bereizgarrietan eta ezaugarrietan oinarrituta ez dauden arriskuen analisiak ez daude debeku horren barruan: adibidez, transakzio susmagarrietan oinarrituta, arriskuen analisiak enpresen finantza-iruzurraren probabilitatea ebaluatzeko erabiltzen dituzten AA-sistemak, edo aduana-agintaritzek estupefaziak eta lege kanpoko salgaiak aurkitzeko probabilitatea aurreikusteko erabiltzen dituzten tresnak, zeinak arriskuaren analisia egiten baitute ezagutzen diren trafiko-ibilbideetan oinarrituta, esate baterako.

(43) Debekatuta egon behar da AA-sistemak merkatuan jartzea, helburu zehatz horretarako zerbitzuan ipintzea edo erabiltzea, baldin eta sistema horien xedea bada Internetetik aurpegiko irudiak edo telebista-zirkuitu itxiko irudiak hautaketarik gabe erauztea aurpegia ezagutzeko datu-baseak sortzeko edo zabaltzeko; izan ere, jardunbide horiek masiboki zaintzapean gaudelako sentimendua areagotzen dute, eta oinarritzko eskubideen urraketa larriak eragin ditzakete, intimitaterako eskubidearena barne.

(44) Kezka handia dago emozioak ezagutzen edo ondorioztatzen saiatzen diren AA-sistemen oinarri zientifikoa dela-eta, batez ere emozioen adierazpena asko aldatzen delako kultura batzuetatik beste batzuetara eta egoera batetik bestera, baita pertsona berarengan ere. Hona sistema horien gabezia nagusietako batzuk: fidagarritasun mugatua, espezifikotasunik eza eta orokortzeko aukera mugatua. Ondorioz, pertsonen emozioak eta asmoak haien datu



deducen las emociones o las intenciones de las personas físicas a partir de sus datos biométricos pueden tener resultados discriminatorios y pueden invadir los derechos y las libertades de las personas afectadas. Teniendo en cuenta el desequilibrio de poder en el contexto laboral o educativo, unido al carácter intrusivo de estos sistemas, dichos sistemas podrían dar lugar a un trato perjudicial o desfavorable de determinadas personas físicas o colectivos enteros. Por tanto, debe prohibirse la introducción en el mercado, la puesta en servicio y el uso de sistemas de IA destinados a ser utilizados para detectar el estado emocional de las personas en situaciones relacionadas con el lugar de trabajo y el ámbito educativo. Dicha prohibición no debe aplicarse a los sistemas de IA introducidos en el mercado estrictamente con fines médicos o de seguridad, como los sistemas destinados a un uso terapéutico.

(45) El presente Reglamento no debe afectar a las prácticas prohibidas por el Derecho de la Unión, incluido el Derecho de la Unión en materia de protección de datos, de no discriminación, de protección de los consumidores y sobre competencia.

(46) La introducción en el mercado de la Unión, la puesta en servicio o la utilización de sistemas de IA de alto riesgo debe supeditarse al cumplimiento por su parte de determinados requisitos obligatorios, los cuales deben garantizar que los sistemas de IA de alto riesgo disponibles en la Unión o cuyos resultados de salida se utilicen en la Unión no planteen riesgos inaceptables para intereses públicos importantes de la Unión, reconocidos y protegidos por el Derecho de la Unión. Sobre la base del nuevo marco legislativo, tal como se aclara en la Comunicación de la Comisión titulada «“Guía azul” sobre la aplicación de la normativa europea relativa a los productos, de 2022» (20), la norma general es que más de un acto jurídico de la legislación de armonización de la Unión, como los Reglamentos (UE) 2017/745 (21) y (UE) 2017/746 (22) del Parlamento Europeo y del Consejo o la Directiva 2006/42/CE del Parlamento Europeo y del Consejo (23) puedan aplicarse a un producto, dado que la introducción en el mercado o la puesta en servicio solo pueden tener lugar cuando el producto cumple toda la legislación de armonización de la Unión aplicable. A fin de garantizar la coherencia y evitar cargas administrativas o costes innecesarios, los proveedores de un producto que contenga uno o varios sistemas de IA de alto riesgo, a los que se apliquen los requisitos del presente Reglamento y de la legislación de armonización de la Unión incluida en una lista de un anexo del presente Reglamento, deben ser flexibles en lo que respecta a las decisiones operativas relativas a la manera de garantizar la conformidad de un producto que contenga uno o varios sistemas de IA con todos los requisitos

biométricos arabera hautematen edo ondorioztatzen dituzten AA-sistemak diskriminatzaileak izan daitezke eta gaina hartu ukitutako pertsonen eskubide eta askatasunei. Sistema hauek intrusiorako duten joerari gehituta lan-eremuan zein hezkuntzarenean egoten den botere-desoreka, gerta daiteke sistema hauek trataera kaltegarria edo okerra ematea pertsona fisiko batzuei edo kolektibo osoei. Horregatik, debekatu egin behar da AA-sistema hauek merkatuan jartzea, zerbitzuan ipintzea eta erabiltzea, lantokiko edo hezkuntzaren eremuko testuinguruetan pertsonen egoera emozionala hautemateko erabiltzen diren heinean. Debeku hori ez da aplikatu behar AA-sistemak zehatz-mehatz medikuntzaren edo segurtasunaren arloko helburuak bakarrik betetzeko jartzen direnean merkatuan; adibidez, erabilera terapeutikora bideratuko sistemen kasuan.

(45) Erregelamendu honek ez ditu barne hartzen Batasuneko zuzenbidean debekatutako jardunbideak, barruan direla Batasuneko zuzenbideak ezarritakoa datuen babesaren gainean, diskriminaziorik ezaren gainean, kontsumitzaileak babestearen gainean eta lehiaren gainean.

(46) Arrisku handiko AA-sistemak Batasunean merkatuan jartzeko, zerbitzuan ipintzeko edo erabiltzeko ezinbestekoa da sistemak nahitaezko zenbait betekizun betetzea, haien bidez bermatuta gera dadin Batasunean erabilgarri dauden arrisku handiko AA-sistema horiek edo Batasunean erabiliko diren haien irteera-emaitzek ez dutela arrisku onartezinik eragingo Batasunaren interes publiko garrantzitsuetan, zeinak berariaz aintzatetsita eta babestuta baitaude Batasuneko zuzenbidean. Legegintza-esparru berria oinarri hartuta, Batzordearen 2022ko «Produktuei buruzko Europako araudiaren aplikazioari buruzko “Gida urdina”» izeneko Komunikazioan argitzen den bezala (20), arau orokorra da produktu berari Batasunaren harmonizazioko legeriako egintza juridiko bat baino gehiago aplikatu ahal izatea, hala nola Europako Parlamentuaren eta Kontseiluaren (EB) 2017/745 Erregelamendua (21) eta (EB) 2017/746 Erregelamendua (22) edo Europako Parlamentuaren eta Kontseiluaren 2006/42/EE Zuzentaraua (23); izan ere, produktu bat merkatuan jarri edo zerbitzuan ipini ahal izateko, ezinbestekoa da produktuak guztiz betetzea aplikatzekoa zaion Batasunaren harmonizazioko legeria. Koherentzia bermatzeko eta beharrezkoak ez diren administrazio-kargak edo kostuak saihesteko, arrisku handiko AA-sistema bat edo gehiago dituzten produktuen kasuan — sistema horiei erregelamendu honetan eta Batasunaren harmonizazioko legerian (erregelamendu honen eranskin batean jaso) ezarritako betekizunak aplikatzen zaizkien heinean—, hornitzaileek malguak izan behar dute erabaki operatiboak hartzeko orduan AA-sistema bat edo gehiago dituen produktu bat



aplicables de la legislación de armonización de la Unión de manera óptima. La clasificación de un sistema de IA como «de alto riesgo» debe limitarse a aquellos sistemas de IA que tengan un efecto perjudicial considerable en la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación debe reducir al mínimo cualquier posible restricción del comercio internacional.

(47) Los sistemas de IA pueden tener un efecto adverso para la salud y la seguridad de las personas, en particular cuando funcionan como componentes de seguridad de productos. En consonancia con los objetivos de la legislación de armonización de la Unión de facilitar la libre circulación de productos en el mercado interior y de velar por que solo lleguen al mercado aquellos productos que sean seguros y conformes, es importante prevenir y mitigar debidamente los riesgos de seguridad que pueda generar un producto en su conjunto debido a sus componentes digitales, entre los que pueden figurar los sistemas de IA. Por ejemplo, los robots cada vez más autónomos que se utilizan en las fábricas o con fines de asistencia y atención personal deben poder funcionar y desempeñar sus funciones de manera segura en entornos complejos. Del mismo modo, en el sector sanitario, donde puede haber repercusiones especialmente importantes en la vida y la salud, los sistemas de diagnóstico y de apoyo a las decisiones humanas, cuya sofisticación es cada vez mayor, deben ser fiables y precisos.

(48) La magnitud de las consecuencias adversas de un sistema de IA para los derechos fundamentales protegidos por la Carta es especialmente importante a la hora de clasificar un sistema de IA como de alto riesgo. Entre dichos derechos se incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, el derecho a la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, la igualdad entre hombres y mujeres, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración. Además de esos derechos, conviene poner de relieve el hecho de que los menores poseen unos derechos específicos consagrados en el artículo 24 de la Carta y en la Convención sobre los Derechos del Niño de las Naciones Unidas, que se desarrollan con más detalle en la observación general n.º 25 de la Convención sobre los Derechos del Niño de Naciones Unidas relativa a los derechos de los niños en relación con el entorno digital. Ambos instrumentos exigen que se tengan en consideración las vulnerabilidades de los menores y que se les brinde la

Batasunaren harmonizazioko legeriako betekizun aplikagarri guztiekin bat datorrela bermatzeko moduari dagokionez. AA-sistema bat «arrisku handikotzat» sailkatuko da, bakarrik baldin eta eragin kaltegarri nabarmena badu Batasuneko pertsonen osasunean, segurtasunean eta oinarritzko eskubideetan, eta muga horrek ahalik eta gehien murriztu behar du nazioarteko merkataritzaren murrizketa posible oro.

(47) AA-sistemek ondorio kaltegarriak izan ditzakete pertsonen osasunean eta segurtasunean, bereziki produktuen segurtasun-osagai gisa funtzionatzen dutenean. Batasunaren harmonizazioko legeriaren helburuekin bat etorritik (barne-merkatuan produktuen zirkulazio askea erraztekoa eta produktu seguru eta egokiak soilik irits daitezen zaintzekoa), garrantzitsua da behar bezala prebenitzea eta arintzea produktu batek, bere osagai digitalak direla-eta, oro har sor ditzakeen segurtasun-arriskuak, eta osagai digital horien artean egon daitezke AA-sistemak. Adibidez, gero eta robot autonomoagoak erabiltzen dira, dela ekoizpenerako, dela laguntza eta arreta pertsonalerako; bada, robot horiek ingurune konplexuetan modu seguruan funtzionatu eta modu seguruan bete behar dituzte beren eginbeharrak. Era berean, osasun-sektorean ondorio bereziki garrantzitsuak egon daitezke pertsonen bizitzarako eta osasunerako, eta diagnostikoak egiteko eta giza erabakiak babesteko sistemek —gero eta sofistikatuagoak— fidagarriak eta zehatzak izan behar dute.

(48) AA-sistema batek Gutunean babestutako oinarritzko eskubideei dakarkien ondorio kaltegarrien munta bereziki kontuan hartzekoa da AA-sistema bat arrisku handikotzat sailkatzeko. Eskubide horien artean dira giza duintasunerako eskubidea, bizitza pribaturako eta familia-bizitzarako errespetua, datu pertsonalen babesa, adierazpen- eta informazio-askatasuna, biltzeko eta elkartzeko askatasuna, diskriminaziorik ez jasateko eskubidea, hezkuntzarako eskubidea, kontsumitzaileen babesa, langileen eskubideak, desgaitasuna duten pertsonen eskubideak, gizonen eta emakumeen arteko berdintasuna, jabetza intelektualeko eskubideak, benetako babes judizialerako eta epaile inpartziala izateko eskubidea, defentsarako eta errugabetasun-presuntziorako eskubideak eta administrazio onerako eskubidea. Eskubide horiez gain, nabarmendu behar da adingabeek eskubide espezifiko batzuk dituztela, Gutunaren 24. artikuluan eta Haurren Eskubideei buruzko Nazio Batuen Konbentzioan jasotakoak. Eskubide horiek zehatzago garatzen dira Haurren Eskubideei buruzko Nazio Batuen Konbentzioaren 25. ohar orokorrean, haurrek ingurune digitalean dituzten eskubideei buruzkoa berau. Adingabeen kalteberatasunak kontuan hartzea eta haien ongizaterako beharrezkoak diren babesa eta laguntza ematea exijitzen dute bi tresna horiek. AA-sistema batek eragin dezakeen kaltearen larritasuna ebaluatzen



protección y la asistencia necesarias para su bienestar. Cuando se evalúe la gravedad del perjuicio que puede ocasionar un sistema de IA, también en lo que respecta a la salud y la seguridad de las personas, también se debe tener en cuenta el derecho fundamental a un nivel elevado de protección del medio ambiente consagrado en la Carta y aplicado en las políticas de la Unión.

(49) En relación con los sistemas de IA de alto riesgo que son componentes de seguridad de productos o sistemas, o que son en sí mismos productos o sistemas que entran en el ámbito de aplicación del Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo (24), el Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo (25), el Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo (26), la Directiva 2014/90/UE del Parlamento Europeo y del Consejo (27), la Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo (28), el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo (29), el Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo (30), y el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo (31), procede modificar dichos actos para garantizar que, cuando la Comisión adopte actos delegados o de ejecución pertinentes basados en ellos, tenga en cuenta los requisitos obligatorios para los sistemas de IA de alto riesgo previstos en el presente Reglamento, atendiendo a las particularidades técnicas y reglamentarias de los distintos sectores y sin interferir con los mecanismos y las autoridades de gobernanza, evaluación de la conformidad y control del cumplimiento vigentes establecidos en dichos actos.

(50) En cuanto a los sistemas de IA que son componentes de seguridad de productos, o que son productos en sí mismos, y entran dentro del ámbito de aplicación de determinados actos legislativos de armonización de la Unión enumerados en un anexo del presente Reglamento, procede clasificarlos como de alto riesgo en virtud del presente Reglamento si el producto de que se trate es sometido a un procedimiento de evaluación de la conformidad con un organismo de evaluación de la conformidad de terceros de acuerdo con dichos actos legislativos de armonización de la Unión. Esos productos son, en concreto, máquinas, juguetes, ascensores, equipo y sistemas de protección para uso en atmósferas potencialmente explosivas, equipos radioeléctricos, equipos a presión, equipos de embarcaciones de recreo, instalaciones de transporte por cable, aparatos que queman combustibles gaseosos, productos sanitarios, productos sanitarios para diagnóstico in vitro, automoción y aviación.

denean, barnean direla pertsonen osasuna eta segurtasuna, kontuan hartu behar da, halaber, ingurumen-babeseko maila handia izateko oinarritzko eskubidea, Gutunean ezarritako eta Batasunaren politiketan aplikatutako moduan.

(49) Aipagai hartuta produktuen edo sistemen segurtasun-osagai diren arrisku handiko AA-sistemak eta beren kabuz produktu edo sistemak direnak, Batasunaren araudi jakinen aplikazio-eremuan sartzen diren heinean [Europako Parlamentuaren eta Kontseiluaren (EE) 300/2008 Erregelamendua (24), Europako Parlamentuaren eta Kontseiluaren (EB) 167/2013 Erregelamendua (25), Europako Parlamentuaren eta Kontseiluaren (EB) 168/2013 Erregelamendua (26), Europako Parlamentuaren eta Kontseiluaren 2014/90/EB Zuzentaraua (27), Europako Parlamentuaren eta Kontseiluaren (EB) 2016/797 Zuzentaraua (28), Europako Parlamentuaren eta Kontseiluaren (EB) 2018/858 Erregelamendua (29), Europako Parlamentuaren eta Kontseiluaren (EB) 2018/1139 Erregelamendua (30), Europako Parlamentuaren eta Kontseiluaren (EB) 2019/2144 Erregelamendua (31)], beharrezkoa da egintza horiek aldatzea, hartara bermatzeko ezen Batzordeak, egoki diren egintza eskuordetuak edo betearazpen-egintzak onartzen dituen egintza horietan oinarrituta, kontuan hartuko dituela erregelamendu honetan arrisku handiko AA-sistematarako aurreikusitako nahitaezko betekizunak, sektoreen berezitasun teknikoak eta erregelamenduzkoen arabera eta oztoporik eragin gabe egintza horietan ezarri diren eta indarrean dauden gobernantzako, adostasunaren ebaluazioko eta betetze-kontrolko mekanismoei eta agintaritzei.

(50) Produktuen segurtasun-osagai diren edo beren kabuz produktu diren AA-sistemak, Batasunaren harmonizazioko lege-egintza jakin batzuen aplikazio-eremuan sartzen diren heinean (erregelamendu honen eranskin batean daude zerrendatuta), egoki da arrisku handikotzat sailkatzea erregelamendu honen arabera, baldin eta dena delako produktua hirugarrenen adostasuna ebaluatzeko organismo baten adostasunaren ebaluazio-prozedura baten mende jartzen bada, Batasunaren harmonizazioko lege-egintza horien arabera. Hona zehazki zein diren produktu horiek: makinak, jostailuak, igogailuak, leherkorrak izan daitezkeen atmosferetan erabiltzeko ekipamenduak eta babes-sistemak, ekipamendu erradioelektrikoak, presio-ekipamenduak, aisiako ontzien ekipamenduak, kable bidezko garraioaren instalazioak, gas-erregaiak erretzen dituzten aparatuak, osasun-produktuak, in vitro diagnostikorako osasun-produktuak eta automozio- eta abiazio-produktuak.



(51) Que un sistema de IA se clasifique como de alto riesgo en virtud del presente Reglamento no significa necesariamente que el producto del que sea componente de seguridad, o el propio sistema de IA como producto, se considere de «alto riesgo» conforme a los criterios establecidos en la correspondiente legislación de armonización de la Unión que se aplique al producto. Tal es el caso, en particular, de los Reglamentos (UE) 2017/745 y (UE) 2017/746, que prevén una evaluación de la conformidad de terceros de los productos de riesgo medio y alto.

(52) En cuanto a los sistemas de IA independientes, a saber, aquellos sistemas de IA de alto riesgo que no son componentes de seguridad de productos, o que son productos en sí mismos, deben clasificarse como de alto riesgo si, a la luz de su finalidad prevista, presentan un alto riesgo de ser perjudiciales para la salud y la seguridad o los derechos fundamentales de las personas, teniendo en cuenta tanto la gravedad del posible perjuicio como la probabilidad de que se produzca, y se utilizan en varios ámbitos predefinidos especificados en el presente Reglamento. Para identificar dichos sistemas, se emplean la misma metodología y los mismos criterios previstos para la posible modificación futura de la lista de sistemas de IA de alto riesgo, que la Comisión debe estar facultada para adoptar, mediante actos delegados, a fin de tener en cuenta el rápido ritmo del desarrollo tecnológico, así como los posibles cambios en el uso de los sistemas de IA.

(53) También es importante aclarar que pueden existir casos específicos en los que los sistemas de IA referidos en ámbitos predefinidos especificados en el presente Reglamento no entrañen un riesgo considerable de causar un perjuicio a los intereses jurídicos amparados por dichos ámbitos, dado que no influyen sustancialmente en la toma de decisiones o no perjudican dichos intereses sustancialmente. A efectos del presente Reglamento, por sistema de IA que no influye sustancialmente en el resultado de la toma de decisiones debe entenderse un sistema de IA que no afecta al fondo, ni por consiguiente al resultado, de la toma de decisiones, ya sea humana o automatizada. Un sistema de IA que no influye sustancialmente en el resultado de la toma de decisiones podría incluir situaciones en las que se cumplen una o varias de las siguientes condiciones. La primera de dichas condiciones debe ser que el sistema de IA esté destinado a realizar una tarea de procedimiento delimitada, como un sistema de IA que transforme datos no estructurados en datos estructurados, un sistema de IA que clasifique en categorías los documentos recibidos o un sistema de IA que se utilice para detectar duplicados entre un gran número de aplicaciones. La naturaleza de esas tareas es tan restringida y limitada que solo presentan riesgos limitados que no aumentan por la utilización de un sistema de IA en un contexto que un anexo al presente Reglamento recoja como uso de alto riesgo. La segunda condición debe ser que la tarea realizada por el sistema de IA esté destinada a mejorar el resultado de una actividad previa llevada a cabo por un ser humano, que pudiera ser

(51) Erregelamendu honen arabera AA-sistema bat arrisku handikotzat sailkatzeak ez du nahitaez esan nahi sistema hori —produktu baten segurtasun-osagaia izan, zein bere kabuz produktu izan— «arrisku handikotzat» hartzen denik produktuari aplikatzen zaion Batasunaren harmonizazioko legerian ezarritako irizpideen arabera. Horixe gertatzen da, zehazki, (EB) 2017/745 eta (EB) 2017/746 erregelamenduetan; izan ere, hirugarrenen adostasunaren ebaluazioa aurreikusten dute arrisku ertain eta handiko produktuetan.

(52) AA-sistema independenteak—hau da, produktuen segurtasun-osagai ez diren edo berez produktu diren arrisku handiko AA-sistemak— arrisku handikotzat sailkatu behar dira, baldin eta, helburu aurreikusaren arabera, arrisku handia badute pertsonen osasunerako, segurtasunerako edo oinarritzko eskubideetarako kaltegarriak izateko, balizko kaltearen larritasuna eta kaltea gertatzeko probabilitatea kontuan hartuta, eta erregelamendu honetan aurrez zehaztutako eremu batean baino gehiagotan erabiltzen badira. Sistema horiek identifikatzeko, arrisku handiko AA-sistemen zerrenda etorkizunean aldatu ahal izateko aurreikusitako metodologia eta irizpide berberak erabiltzen dira, eta, Batzordeak ahalmena eduki behar du egintza eskuordetuen bidez bere egiteko, garapen teknologiko azkarrari eta AA-sistemen erabileran egon daitezkeen aldaketei erantzun ahal izateko.

(53) Era berean, gerta daiteke kasu jakin batzuetan erregelamendu honetan aurrez zehaztutako eremuei dagozkien AA-sistemek ez eragitea arrisku nabarmenik eremu horietan jasotako interes juridikoei kalte egiteko, ez dutelako funtsezko eraginik erabakiak hartzeko prozesuan edo ez dietelako funtsezko kalterik egiten interes horiei. Erregelamendu honen ondorioetarako, hauxe ulertu behar da erabakiak hartzeko prozesuaren emaitzan funtsezko eraginik ez duen AA-sistematzat: AA-sistema bat, zeinak ez dion eragiten erabakiak hartzeko funtsari, eta, ondorioz, emaitzari ere ez, giza erabakiak izan zein erabaki automatizatuak izan. Erabakiak hartzeko prozesuaren emaitzan funtsezko eraginik ez duten AA-sistemek egoera bat baino gehiago barne har ditzakete, eta, egoera horietan, baldintza hauetako bat edo batzuk bete daitezke: Baldintza horietako lehena da AA-sistema prozedura-lan mugatu bat egitera bideratuta egotea. Hori gertatzen da, esaterako, egituratu gabeko datuak datu egituratu bihurtzeko erabiltzen denean AA-sistema, edo jasotako dokumentuak kategorietan sailkatzeko erabiltzen denean edo aplikazio kopuru handi baten artean bikoiztuak detektatzeko. Zeregin horien izaera hain da mugatua, arriskuak ere mugatuak baitira. Arrisku horiek, gainera, ez dira handitzen AA-sistema erregelamenduaren eranskin batean arrisku handiko erabileratzat zehaztutako testuinguru batean erabiltza ere. Bigarren baldintza da AA-sistemak betetako zereginaren helburua gizaki batek aurrez egindako



pertinente a efectos de las utilizaciones de alto riesgo enumeradas en un anexo del presente Reglamento. Teniendo en cuenta esas características, el sistema de IA solo añade un nivel adicional a la actividad humana, entrañando por consiguiente un riesgo menor. Esa condición se aplicaría, por ejemplo, a los sistemas de IA destinados a mejorar el lenguaje utilizado en documentos ya redactados, por ejemplo, en lo referente al empleo de un tono profesional o de un registro lingüístico académico o a la adaptación del texto a una determinada comunicación de marca. La tercera condición debe ser que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones respecto de patrones de toma de decisiones anteriores. El riesgo sería menor debido a que el sistema de IA se utiliza tras una valoración humana previamente realizada y no pretende sustituirla o influir en ella sin una revisión adecuada por parte de un ser humano. Por ejemplo, entre los sistemas de IA de este tipo, se incluyen aquellos que pueden utilizarse para comprobar a posteriori si un profesor puede haberse desviado de su patrón de calificación determinado, a fin de llamar la atención sobre posibles incoherencias o anomalías. La cuarta condición debe ser que el sistema de IA esté destinado a realizar una tarea que solo sea preparatoria de cara a una evaluación pertinente a efectos de los sistemas de IA enumerados en el anexo del presente Reglamento, con lo que la posible repercusión de los resultados de salida del sistema sería muy escasa en términos de representar un riesgo para la subsiguiente evaluación. Esa condición comprende, entre otras cosas, soluciones inteligentes para la gestión de archivos, lo que incluye funciones diversas tales como la indexación, la búsqueda, el tratamiento de texto y del habla o la vinculación de datos a otras fuentes de datos, o bien los sistemas de IA utilizados para la traducción de los documentos iniciales. En cualquier caso, debe considerarse que los sistemas de IA utilizados en casos de alto riesgo enumerados en un anexo del presente Reglamento presentan un riesgo significativo de menoscabar la salud y la seguridad o los derechos fundamentales si el sistema de IA conlleva la elaboración de perfiles en el sentido del artículo 4, punto 4, del Reglamento (UE) 2016/679, del artículo 3, punto 4, de la Directiva (UE) 2016/680 o del artículo 3, punto 5, del Reglamento (UE) 2018/1725. Para garantizar la trazabilidad y la transparencia, los proveedores que, basándose en las condiciones antes citadas, consideren que un sistema de IA no es de alto riesgo, deben elaborar la documentación de la evaluación previamente a la introducción en el mercado o la entrada en servicio de dicho sistema de IA y facilitarla a las autoridades nacionales competentes cuando estas lo soliciten. Dichos proveedores deben tener la obligación de registrar el sistema en la base de datos de la UE creada en virtud del presente Reglamento. Con el fin de proporcionar orientaciones adicionales sobre la aplicación práctica de las condiciones con arreglo a las cuales los sistemas de IA enumerados en un anexo del presente Reglamento no se consideran, con carácter excepcional, de alto riesgo, la Comisión debe, previa consulta al Consejo de IA, proporcionar directrices

jarduera baten emaitza hobetzea izatea, zeina erregelamendu honen eranskin batean zerrendatutako arrisku handiko erabileren ondorioetarako egokia izan baitaiteke. Ezaugarri horien arabera, giza jarduerari beste maila bat eranstera mugatzen da AA-sistema, eta, beraz, txikia da arriskua. Baldintza hori legokieke, esaterako, aurrez idatzitako dokumentuetan erabilitako hizkuntza hobetzen duten AA-sistemei, adibidez hizkera profesionala edo hizkuntza-erregistro akademikoa emateko baliatzen direnean edo testu bat marka-komunikazio jakin batera egokitu behar direnean. Hirugarren baldintza da AA-sistemaren helburua izatea erabakiak hartzeko patroiak hautematea edo erabakiak hartzeko aurreko ereduen gaineko desbideraketak hautematea. Arriskua txikiagoa izango litzateke, AA-sistema erabili aurretik giza balioespen bat egin delako eta AA-sistemaren bidez ez delako balioespen hori ordeztu edo hartan eragin nahi, gizaki batek behar den berrikuspena egin gabe. Moltzo horretan daude, adibidez, irakasle bat kalifikazio-patroi jakin batetik aldenitu ote den jakiteko erabiltzen diren AA-sistemak, inkoherentziak edo anomaliaz hautemanez gero haien gainean ohartarazteko. Hona laugarren baldintza: erregelamendu honen eranskin batean zerrendatutako AA-sistemen ondorioetarako ebaluazio egoki bat egiteko prestaketa-lan bat egitera mugatuta erabiltzea AA-sistema. Izan ere, halakoetan, irteera-emaitzen eragina nekez izan daiteke arriskutsua hurrengo ebaluaziorako. Halakoak dira, adibidez, fitxategiak kudeatzeko soluzio adimendunak, zeinek askotariko eginkizunak barne hartzen baitituzte, hala nola indexazioa, bilaketa, testuaren eta hizketaren tratamendua eta datuak beste datu-iturri batzuekin lotzeko prozesuak; halakoak dira, orobat, hasierako dokumentuak itzultzeko erabiltzen diren AA-sistemak. Edonola ere, erregelamendu honen eranskin batean zerrendatutako arrisku handiko kasuetan erabilitako AA-sistemak osasuna, segurtasuna edo oinarritzko eskubideak kaltezeko arrisku nabarikotzat jo behar dira, badin eta sistema horien jardunbidean profilaketa sartzen bada (EB) 2016/679 Erregelamenduaren 4.4 artikuluan, (EB) 2016/680 Zuzentarauaren 3.4 artikuluan edo (EB) 2018/1725 Erregelamenduaren 3.5 artikuluan zehaztutako moduan. Trazabilitatea eta gardentasuna bermatzeko, lehen aipatutako baldintzetan oinarrituta AA-sistema bat arrisku handikoa ez dela uste duten hornitzaileek ebaluazioaren dokumentazioa prestatu behar dute AA-sistema hori merkatuan jarri edo zerbitzuan ipini aurretik, eta agintaritzak nazional eskudunei eman behar diete haiek eskatzen dutenean. Hornitzaile horiek erregelamendu honen arabera sortutako EBren datu-basean erregistratu behar dute sistema. Erregelamendu honen eranskin batean zerrendatutako AA-sistemak salbuespen gisa arrisku handikotzat ez hartzeko baldintzak praktikoki nola aplikatu azaltzeko orientabide gehiago emate aldera, Batzordeak, AA-kontseiluari kontsulta egin ondoren, aplikazio praktikoki hori zehazteko gidalerroak eman behar ditu, zerrenda zehatz batean

que especifiquen dicha aplicación práctica, completadas por una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y de casos de uso que no lo sean.

(54) Dado que los datos biométricos constituyen una categoría de datos personales sensibles, procede clasificar como de alto riesgo varios casos de uso críticos de sistemas biométricos, en la medida que su utilización esté permitida con arreglo al Derecho de la Unión y nacional pertinente. Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica remota de las personas físicas pueden dar lugar a resultados sesgados y tener efectos discriminatorios. El riesgo de dichos resultados sesgados y efectos discriminatorios es especialmente pertinente por lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. Por lo tanto, los sistemas de identificación biométrica remota deben clasificarse como de alto riesgo debido a los riesgos que entrañan. Quedan excluidos de dicha clasificación los sistemas de IA destinados a la verificación biométrica, que incluye la autenticación, cuyo único propósito es confirmar que una persona física concreta es quien dicha persona dice ser, así como confirmar la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga un acceso seguro a un local. Además, deben clasificarse como de alto riesgo los sistemas de IA destinados a ser utilizados para la categorización biométrica conforme a atributos o características sensibles protegidos en virtud del artículo 9, apartado 1, del Reglamento (UE) 2016/679 sobre la base de datos biométricos, en la medida en que no estén prohibidos en virtud del presente Reglamento, así como los sistemas de reconocimiento de emociones que no estén prohibidos con arreglo al presente Reglamento. Los sistemas biométricos destinados a ser utilizados exclusivamente a efectos de posibilitar la ciberseguridad y las medidas de protección de los datos personales no deben considerarse sistemas de IA de alto riesgo.

(55) Por lo que respecta a la gestión y el funcionamiento de infraestructuras críticas, procede clasificar como de alto riesgo los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas que se enumeran en el anexo, punto 8, de la Directiva (UE) 2022/2557; del tráfico rodado y del suministro de agua, gas, calefacción y electricidad, pues un fallo o un defecto de funcionamiento de estos componentes puede poner en peligro la vida y la salud de las personas a gran escala y alterar de manera considerable el desarrollo habitual de las actividades sociales y económicas. Los componentes de seguridad de las infraestructuras críticas, como las infraestructuras digitales críticas, son sistemas utilizados para proteger directamente la integridad física de las infraestructuras críticas o la salud

jasota arrisku handikoak diren AA-sistemen erabilera-
kasuen eta arrisku handikoak ez diren erabilera-kasuen
adibide praktikoak.

(54) Datu biometrikoen kasuan, bereziki babestutako datu pertsonalen kategoria bat direnez, sistema biometrikoen zenbait erabilera kritiko arrisku handikotzat sailkatu behar dira, betiere erabilera hori baimenduta dagoen heinean Batasuneko zuzenbidearen eta dagokion zuzenbide nazionalaren arabera. Pertsona fisikoek urruneko identifikazio biometrikorako AA-sistemen zehaztugabetasun teknikoek emaitza alboratuak eragin ditzakete eta ondorio diskriminatzaileak ekarri. Emaitza alboratuak eta diskriminazio-ondorioak izateko arrisku horrek bereziki eragiten die adinari, etniari, arrazari, sexuari edo desgaitasunari. Horregatik, urruneko identifikazio biometrikoko sistemak arrisku handikotzat sailkatu behar dira, halako arriskua baitakarte. Egiaztapen biometrikora —autentifikazioa barne hartuta— bideratutako AA-sistemak sailkapen horretatik kanpo geratzen dira, baldin eta haien helburu bakarra bada pertsona fisiko baten identitatea hark esandakoarekin bat datorrela ziurtatzea edo pertsona fisiko baten identitatea egiaztatzea xede jakin baterako, hala nola zerbitzu zehatz baterako sarbidea izateko, gailu bat desblokeatzeko edo lokal baterako sarbide segurua izateko. Orobat, AA-sistemak arrisku handikotzat sailkatu behar dira, baldin eta bereziki babestu beharreko atributu edo ezaugarrien arabera kategorizazio biometrikorako erabili behar badira, bat etorrita (EB) 2016/679 Erregelamenduaren 9.1 artikuluaarekin, datu biometrikoak oinarri hartuta, non eta erregelamendu honen arabera ez dauden debekatuta; arrisku handikotzat sailkatu behar dira, halaber, emozioak ezagutzeko sistemak, erregelamendu honen arabera debekatuta ez dauden heinean.

Zibersegurtasuna eta datu pertsonalak babesteko neurriak ahalbidetzeko soilik erabiliko diren sistema biometrikoak ez dira arrisku handiko AA-sistematzat hartu behar.

(55) Azpiegitura kritikoen kudeaketari eta funtzionamenduari dagokienez, arrisku handikotzat sailkatzeak dira (EB) 2022/2557 Zuzentarauaren 8. puntuan zerrendatzen diren azpiegitura digital kritikoen kudeaketan eta funtzionamenduan segurtasun-osagai gisa erabiltzekoak diren AA-sistemak; bai, halaber, ur-, gas-, berokuntza- edo elektrizitate-horniduraren kudeaketan eta funtzionamenduan segurtasun-osagai gisa erabiliko diren AA-sistemak ere. Izan ere, osagai horien funtzionamendu-hutsegite edo -akats batek pertsonen bizitza eta osasuna arriskuan jar ditzake eskala handian, eta nabarmen alda dezake jarduera sozial eta ekonomikoen ohiko garapena. Azpiegitura kritikoen segurtasun-osagaiak —hala nola azpiegitura digital kritikoak— azpiegitura kritikoen osotasun fisikoa eta pertsonen osasuna eta segurtasuna eta ondasunena



y la seguridad de las personas y los bienes, pero que no son necesarios para el funcionamiento del sistema. El fallo o el defecto de funcionamiento de estos componentes podría dar lugar directamente a riesgos para la integridad física de las infraestructuras críticas y, por tanto, a riesgos para la salud y la seguridad de las personas y los bienes. Los componentes destinados a ser utilizados exclusivamente con fines de ciberseguridad no deben considerarse componentes de seguridad. Entre los componentes de seguridad de esas infraestructuras críticas cabe citar los sistemas de control de la presión del agua o los sistemas de control de las alarmas contra incendios en los centros de computación en la nube.

(56) El despliegue de sistemas de IA en el ámbito educativo es importante para fomentar una educación y formación digitales de alta calidad y para que todos los estudiantes y profesores puedan adquirir y compartir las capacidades y competencias digitales necesarias, incluidos la alfabetización mediática, y el pensamiento crítico, para participar activamente en la economía, la sociedad y los procesos democráticos. No obstante, deben clasificarse como de alto riesgo los sistemas de IA que se utilizan en la educación o la formación profesional, y en particular aquellos que determinan el acceso o la admisión, distribuyen a las personas entre distintas instituciones educativas y de formación profesional o programas de todos los niveles, evalúan los resultados del aprendizaje de las personas, evalúan el nivel apropiado de educación de una persona e influyen sustancialmente en el nivel de educación y formación que las personas recibirán o al que podrán acceder, o supervisan y detectan comportamientos prohibidos de los estudiantes durante las pruebas, ya que pueden decidir la trayectoria formativa y profesional de una persona y, en consecuencia, puede afectar a su capacidad para asegurar su subsistencia. Cuando no se diseñan y utilizan correctamente, estos sistemas pueden invadir especialmente y violar el derecho a la educación y la formación, y el derecho a no sufrir discriminación, además de perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, las personas con discapacidad o las personas de cierto origen racial o étnico o con una determinada orientación sexual.

(57) También deben clasificarse como de alto riesgo los sistemas de IA que se utilizan en los ámbitos del empleo, la gestión de los trabajadores y el acceso al autoempleo, en particular para la contratación y la selección de personal, para la toma de decisiones que afecten a las condiciones de las relaciones de índole laboral, la promoción y la rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales y para la supervisión o evaluación de las personas en el marco de las

zuzenean babesteko erabiltzen dira, baina ez dira beharrezkoak sistemaren funtzionamendurako. Osagai horietan funtzionamendu-hutsegiteak edo -akatsak gertatuz gero, zuzenean gera daiteke arriskuan azpiegitura kritikoen osotasun fisikoa, eta, ondorioz, pertsonen osasuna eta segurtasuna ere bai, baita ondasunena ere. Zibersegurtasun-xedeetarako soilik erabiltzekoak diren osagaiak ez dira segurtasun-osagaitzat hartu behar. Azpiegitura kritiko horien segurtasun-osagaien artean, aipatu beharrezkoak dira hodeiko konputazio-zentroetan uraren presioa eta suteen aurkako alarmak kontrolatzen dituzten sistemak.

(56) Hezkuntzaren eremuan AA-sistemak hedatzea garrantzitsua da kalitate handiko hezkuntza eta prestakuntza digitala sustatzeko eta ikasle eta irakasle guztiek beharrezkoak diren gaitasun eta konpetentzia digitalak eskuratu eta partekatu ahal izateko, barruan direla alfabetatze mediatikoa eta pentsamendu kritikoa, hartara aktiboki parte hartzeko ekonomian, gizartean eta prozesu demokratikoetan. Alabaina, hezkuntzan edo lanbide-heziketan erabiltzen diren AA-sistemak arrisku handikotzat sailkatu behar dira; bereziki, honako hauek: sarbidea edo onarpena zehazten duten sistemak, pertsonak hezkuntza-erakundeen eta lanbide-heziketako erakundeen artean edo maila guztietako programen artean banatzen dituztenak, pertsonen ikaskuntzaren emaitzak ebaluatzen dituztenak, pertsona baten hezkuntza-maila egokia ebaluatzen dutenak eta pertsonak jasoko duten edo eskuratu ahal izango duten hezkuntza- eta prestakuntza-mailan funtsezko eragina dutenak, edo probak egin bitartean ikasleek portaera debekatuak egiten ote dituzten zaintzen eta detektatzen dituztenak; izan ere, horiek denek pertsona baten prestakuntza- eta lanbide-ibilbidea erabaki dezakete eta, ondorioz, eragina izan dezake haren bizibidea ziurtatzeko gaitasunean. Sistema horiek, ez direnean zuzen diseinatzen eta erabiltzen, nabarmen inbaditu eta urratu ditzakete hala hezkuntza- eta prestakuntza-eskubideak, nola diskriminaziorik ez jasatekoa; gainera, betikotu egin ditzakete diskriminazio-patroi historikoak: emakumeen kontrakoak, adin-talde jakin batzuen kontrakoak, desgaitasuna duten pertsonen kontrakoak zein arraza- edo etnia-jatorri jakineko edo sexu-orientazio jakineko pertsonen kontrakoak, adibidez.

(57) Arrisku handikotzat sailkatu behar dira, halaber, enpleguaren, langileen kudeaketaren eta autoenplegurako sarbidearen eremuetan erabiltzen diren AA-sistemak, bereziki eginkizun hauetarako erabiltzen direnak: langileak kontratatze eta hautatzeko, lan-harremanen baldintzei eragiten dieten erabakiak hartzeko, lan-izaerako kontratu-harremanak sustatzeko eta hutsaltzeko, zereginak esleitzeko portaera indibidualetatik edo bereizgarri edo ezaugarri pertsonaletatik abiatuta, eta lan-izaerako kontratu-harremanen esparruan pertsonak gainbegiratzeko edo



relaciones contractuales de índole laboral, dado que pueden afectar de un modo considerable a las futuras perspectivas laborales, a los medios de subsistencia de dichas personas y a los derechos de los trabajadores. Las relaciones contractuales de índole laboral deben incluir, de manera significativa, a los empleados y las personas que prestan servicios a través de plataformas, como indica el programa de trabajo de la Comisión para 2021. Dichos sistemas pueden perpetuar patrones históricos de discriminación, por ejemplo contra las mujeres, determinados grupos de edad, las personas con discapacidad o las personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante todo el proceso de contratación y en la evaluación, promoción o retención de personas en las relaciones contractuales de índole laboral. Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden socavar sus derechos fundamentales a la protección de los datos personales y a la intimidad.

(58) El acceso a determinados servicios y prestaciones esenciales, de carácter público y privado, necesarios para que las personas puedan participar plenamente en la sociedad o mejorar su nivel de vida, y el disfrute de dichos servicios y prestaciones, es otro ámbito en el que conviene prestar especial atención a la utilización de sistemas de IA. En particular, las personas físicas que solicitan a las autoridades públicas o reciben de estas prestaciones y servicios esenciales de asistencia pública, a saber, servicios de asistencia sanitaria, prestaciones de seguridad social, servicios sociales que garantizan una protección en casos como la maternidad, la enfermedad, los accidentes laborales, la dependencia o la vejez y la pérdida de empleo, asistencia social y ayudas a la vivienda, suelen depender de dichas prestaciones y servicios y, por lo general, se encuentran en una posición de vulnerabilidad respecto de las autoridades responsables. La utilización de sistemas de IA para decidir si las autoridades deben conceder, denegar, reducir o revocar dichas prestaciones y servicios o reclamar su devolución, lo que incluye decidir, por ejemplo, si los beneficiarios tienen legítimamente derecho a dichas prestaciones y servicios, podría tener un efecto considerable en los medios de subsistencia de las personas y vulnerar sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a la tutela judicial efectiva y, por lo tanto, deben clasificarse como de alto riesgo. No obstante, el presente Reglamento no debe obstaculizar el desarrollo y el uso de enfoques innovadores en la Administración, que podrían beneficiarse de una mayor utilización de sistemas de IA conformes y seguros, siempre y cuando dichos sistemas no supongan un alto riesgo para las personas jurídicas y físicas. Además, deben clasificarse como de alto riesgo los sistemas de IA usados para evaluar la calificación crediticia o solvencia de las personas físicas, ya que deciden si dichas personas

ebaluatzeko; izan ere, sistema horien erabilerak eragin nabarmena eduki dezake etorkizuneko lan-aurreikuspenetan, pertsona horien bizibide-bitartekoetan eta langileen eskubideetan. Lan-izaerako kontratu-harremanek barnean hartu behar dituzte, modu esanguratsuan, plataformen bidez zerbitzuak ematen dituzten langileak eta pertsonak, Batzordearen 2021erako lan-programak adierazten duen bezala. Sistema horiek betikotu egin ditzakete diskriminazio-patroi historikoak lan-izaerako kontratazio-harremanetan, dela emakumeen kontra, dela adin-talde jakin batzuen kontra, dela desgaitasuna duten pertsonen kontra edo arraza- edo etnia-jatorri jakineko edo sexu-orientazio jakineko pertsonen kontra, bai kontratazio-prozesu osoan, bai pertsonak ebaluatzeko, sustatzeko edo atxikitzeko orduan. Pertsona horien errendimendua eta portaera kontrolatzeko erabiltzen diren AA-sistemek, gainera, kaltea ekar diezaiekete datu pertsonalak eta intimitatea babesteko oinarritzko eskubideei.

(58) AA-sistemak erabiltzeko orduan bada bereziki kontuan hartu beharreko beste arlo bat ere: funtsezko zerbitzu eta prestazio publiko zein pribatu jakin batzuetarako sarbidea izatea —beharrezkoak diren heinean pertsonak gizartearen bete-betean parte hartu edo haien bizi-maila hobetu ahal izan dezaten— eta zerbitzu edo prestazio horiez goatzeko aukera edukitzea. Laguntza publikoko funtsezko prestazio eta zerbitzuen kasuan —egoera jakinetan osasun-laguntzako zerbitzuak, gizarte-segurantzako prestazioak eta babesa bermatzeko gizarte-zerbitzuak ematekoak, hala nola amatasun, gaixotasun, lan-istripu, mendekotasun edo zahartzaroko egoeretan—, pertsona fisikoek agintaritza publikoei laguntza publikoko funtsezko prestazio eta zerbitzu horiek eskatzen dizkietenean edo laguntza horiek jasotzen dituztenean, prestazio eta zerbitzu horien mende egoten dira maiz, eta, askotan, agintaritza horiekiko kalteberatasun-egoeran. Halakoetan, agintaritzek prestazio edo zerbitzu horiek eman, ukatu, murriztu edo errebokatu behar dituztenean edo atzera itzul daitezen eskatu behar dutenean —adibidez, erabaki behar denean ea onuradunek eskubidea duten legez prestazio eta zerbitzu horiek jasotzeko—, AA-sistemak erabiltzen badira halako erabakiak hartzeko, kontuan hartu behar da erabaki horrek eragin nabarmena izan dezakeela pertsonen bizibide-bitartekoetan, eta oinarritzko eskubideak urra ditzakeela, hala nola gizarte-babeserako eskubidea, diskriminaziorik ez jasateko eskubidea, giza duintasunerako eskubidea edo benetako babes judizialerako eskubidea. Beraz, arrisku handikotzat sailkatu behar dira AA-sistema horiek. Dena dela, erregelamendu honek ez du oztopo izan behar Administrazioan ikuspegi berritzaileak garatzeko eta erabiltzeko, eta ikuspegi berritzaile horietarako lagungarria gerta daiteke AA-sistema egoki eta seguruak gehiago erabiltzea, non eta sistema horiek ez dakarten arrisku handirik pertsona juridiko eta



pueden acceder a recursos financieros o servicios esenciales como la vivienda, la electricidad y los servicios de telecomunicaciones. Los sistemas de IA usados con esos fines pueden discriminar a determinadas personas o colectivos y perpetuar patrones históricos de discriminación, como por motivos de origen racial o étnico, género, discapacidad, edad u orientación sexual, o generar nuevas formas de discriminación. No obstante, los sistemas de IA previstos por el Derecho de la Unión con vistas a detectar fraudes en la oferta de servicios financieros y, a efectos prudenciales, para calcular los requisitos de capital de las entidades de crédito y las empresas de seguros no deben considerarse de alto riesgo en virtud del presente Reglamento. Además, los sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud también pueden afectar de un modo considerable a los medios de subsistencia de las personas y, si no se diseñan, desarrollan y utilizan debidamente, pueden vulnerar sus derechos fundamentales y pueden tener graves consecuencias para la vida y la salud de las personas, como la exclusión financiera y la discriminación. Por último, los sistemas de IA empleados para evaluar y clasificar llamadas de emergencia de personas físicas o el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, incluidos policía, bomberos y servicios de asistencia médica, así como sistemas de triaje de pacientes para la asistencia sanitaria de emergencia, también deben considerarse de alto riesgo, dado que adoptan decisiones en situaciones sumamente críticas para la vida y la salud de las personas y de sus bienes.

(59) Dado su papel y su responsabilidad, las actuaciones de las autoridades garantes del cumplimiento del Derecho que implican determinados usos de los sistemas de IA se caracterizan por un importante desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física, así como tener otros efectos negativos sobre los derechos fundamentales consagrados en la Carta. En particular, si el sistema de IA no está entrenado con datos de buena calidad, no cumple los requisitos adecuados en términos de rendimiento, de precisión o de solidez, o no se diseña y prueba debidamente antes de introducirlo en el mercado o ponerlo en servicio, es posible que señale a personas de manera discriminatoria, incorrecta o injusta. Además, podría impedir el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como el derecho a la defensa y a la presunción de inocencia, sobre todo cuando dichos

fisikoentzat. Bestalde, pertsona fisikoen kreditu-kalifikazioa edo kaudimena ebaluatzeko erabiltzen diren AA-sistemak ere arrisku handikotzat sailkatu behar dira; izan ere, sistema horien erabakiaren mende geratzen da ea pertsona horiek finantza-baliabideak edo funtsezko zerbitzuak (etxebizitza, elektrizitatea eta telekomunikazio-zerbitzuak) eskuratzeko modua izango duten. Eta helburu horietarako erabilitako AA-sistemek pertsona edo kolektibo jakin batzuk diskrimina ditzakete eta diskriminazio-patroi historikoak betikotu arrazoitzat hartuta arraza- edo etnia-jatorria, generoa, desgaitasuna, adina edo sexu-orientazioa; era berean, diskriminazio-eredu berriak ere sor ditzakete. Aitzitik, erregelamendu honen arabera, AA-sistemak ez dira arrisku handikotzat jo behar, Batasuneko zuzenbidean aurreikusitakoari jarrikiz finantza-zerbitzuen eskaintzan iruzurrak hautemateko erabiltzekoak badira edo kreditu-entitateen eta aseguru-enpresen kapital-betekizunak kalkulatzeko erabiltzekoak, zuhurtziaz jokatzeko aldera. Bizi-aseguruen eta osasun-aseguruen kasuan, pertsona fisikoen araberrako arriskuak ebaluatzeko eta prezioak finkatzeko erabiltzen diren AA-sistemak ere eragin esanguratsua izan dezakete pertsonen bizibide-bitartekoetan, eta, ez badira behar bezala diseinatzen, garatzen eta erabiltzen, pertsonen oinarritzko eskubideak urra ditzakete eta ondorio larriak eragin pertsona horien bizitzan eta osasunean, finantza-bazterketa eta diskriminazioa eraginda. Azkenik, arrisku handikotzat jo behar dira, halaber, pertsona fisikoen larrialdi-deiak ebaluatzeko eta sailkatzeko erabiltzen diren AA-sistemak edo larrialdi-egoeretan lehen mailako esku-hartzeen zerbitzuak bidaltzeko lehentasunak ezartzeko erabiltzen direnak (polizia, suhiltzaileak eta laguntza medikoko zerbitzuak, esaterako), bai eta larrialdiko osasun-laguntzan pazienteak larritasunaren arabera sailkatzeko sistemak ere; izan ere, halakoetan, pertsonen bizitzarako eta osasunerako eta haien ondasunetarako guztiz kritikoak diren egoeretan hartzen dituzte erabakiak.

(59) Beren zeregina eta erantzukizuna kontuan hartuta, zuzenbidea betearazteko agintaritzen jarduketek, AA-sistemen erabilera jakin batzuk baliatzea dakartzaten heinean, botere-desoreka handia izaten dute ezaugarri, eta ondorio garrantzitsuak eragin ditzakete, hala nola pertsona fisiko bat zaintzapean jartzea, atxilotzea edo askatasunaz gabetzea, bai eta Gutunean jasotako oinarritzko eskubideen gaineko beste ondorio negatibo batzuk ere. Zehazki, AA-sistema kalitate oneko datuekin entrenatuta ez badago, errendimendu-, zehaztasun- edo sendotasun-betekizun egokiak betetzen ez baditu edo merkatuan jarri edo zerbitzuan ipini aurretik behar bezala diseinatzen eta probatzen ez bada, baliteke modu diskriminatzailean, desegokian edo bidegabean seinalatzea pertsonak. Gainera, oinarritzko eskubide prozesal garrantzitsuak eragotzi ditzake, hala nola benetako babes judizialerako eta epaile inpartziala izateko eskubidea; era berean, defentsarako eta



sistemas de IA no sean lo suficientemente transparentes y explicables ni estén suficientemente bien documentados. Por consiguiente, en la medida en que su uso esté permitido conforme al Derecho de la Unión y nacional pertinente, procede clasificar como de alto riesgo varios sistemas de IA destinados a ser utilizados con fines de garantía del cumplimiento del Derecho cuando su precisión, fiabilidad y transparencia sean especialmente importantes para evitar consecuencias adversas, conservar la confianza de la población y garantizar la rendición de cuentas y unas vías de recurso efectivas. En vista de la naturaleza de las actividades y de los riesgos conexos, entre dichos sistemas de IA de alto riesgo deben incluirse, en particular, los sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en nombre de estas, o por las instituciones, órganos u organismos de la Unión en apoyo de las primeras, para evaluar el riesgo de que una persona física sea víctima de delitos, como los polígrafos y otras herramientas similares, para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos y, en la medida en que no esté prohibido conforme al presente Reglamento, para evaluar el riesgo de que una persona física cometa un delito o reincida, no solo sobre la base de la elaboración de perfiles de personas físicas o la evaluación de rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o grupos de personas, o para elaborar perfiles durante la detección, la investigación o el enjuiciamiento de delitos. Los sistemas de IA destinados específicamente a ser utilizados en procesos administrativos por las autoridades fiscales y aduaneras y las unidades de inteligencia financiera que desempeñan tareas administrativas de análisis de información de conformidad con el Derecho de la Unión en materia de lucha contra el blanqueo de capitales no deben clasificarse como sistemas de IA de alto riesgo usados por las autoridades garantes del cumplimiento del Derecho con el fin de prevenir, detectar, investigar y enjuiciar delitos. El uso de herramientas de IA por parte de las autoridades garantes del cumplimiento del Derecho y otras autoridades pertinentes no debe convertirse en un factor de desigualdad o exclusión. No debe ignorarse el impacto del uso de herramientas de IA en los derechos de defensa de los sospechosos, en particular la dificultad para obtener información significativa sobre el funcionamiento de dichos sistemas y la consiguiente dificultad para impugnar sus resultados ante los tribunales, en particular por parte de las personas físicas investigadas.

(60) Los sistemas de IA empleados en la migración, el asilo y la gestión del control fronterizo afectan a personas que con frecuencia se encuentran en una situación especialmente vulnerable y que dependen del resultado de las actuaciones de las autoridades públicas competentes. Por este motivo, es sumamente importante que los sistemas de IA que se utilicen en estos contextos sean precisos, no discriminatorios y

errugabetasun-presuntziorako eskubidea oztopa ditzake, batik bat AA-sistema ez denean behar bezain gardena eta azalgarria eta ez dagoenean behar bezain ondo dokumentatuta. Hala, bada, kontuan hartuta zuzenbidea betearazteko erabiltzekoak diren zenbait AA-sistema —betiere Batasuneko zuzenbideak eta dagokion zuzenbide nazionalak haien erabilera baimentzen duten heinean—bereziki zehatzak, fidagarriak eta gardenak izan behar dutela ondorio kaltegarriak saihesteko, herritarren konfiantzari eusteko eta kontu-ematea eta errekurtsio-bide eraginkorrak bermatzeko, sistema horiek arrisku handikotzat sailkatzekoak dira. Jardueren izaera eta hari lotutako arriskuak ikusita, arrisku handiko AA-sistema horien artean sartu behar dira, bereziki, zuzenbidea betearazteko agintaritzek edo haien izenean dihardutenek edo Batasuneko instituzio, organo edo organismoek agintaritza horiei laguntzeko erabiltzen dituzten AA-sistemak, helburu hauetarako erabiltzen diren heinean: pertsona fisiko batek delituen biktima izateko zer arrisku duen ebaluatzeko —halako sistemak dira poligrafoak eta antzeko beste tresna batzuk—, delituak ikertzen edo epaitzen diren bitartean frogan fidagarritasuna ebaluatzeko, eta, erregelamendu honen arabera debekatuta ez badago, pertsona fisiko batek delitu bat egiteko edo delitu berean berrerortzeko nolako arriskua duen ebaluatzeko —ez bakarrik pertsona fisikoen profilaketan edo pertsona fisikoen edo pertsona-taldearen nortasunaren bereizgarri edo ezaugarrien edo izandako delitu-portaeren ebaluazioan oinarrituta—, baita delituak detektatu, ikertu edo epaitu bitartean profilak egiteko ere. Zuzenbidea betearazteko agintaritzek delituak detektatu, ikertu edo epaitzeko helburuz erabiltzen dituzten arrisku handiko AA-sistemen barruan ez dira sartu behar kapitalak zurriztearen aurkako borrokan Batasuneko zuzenbidearekin bat etorritako informazioa aztertzekeko administrazio-lanak egiten dituzten zerga- eta aduana-agintaritzek eta finantza-inteligentziako unitateek administrazio-prozesuetan berariaz erabiltzekoak diren AA-sistemak. Zuzenbidea betearazteko agintaritzek eta beste agintaritza batzuek AA-tresnak erabiltzea ezin da bilakatu desberdinkerien edo bazterketen iturri. Aintzakotzat hartzekoa da zer-nolako inpaktua duen AA-tresnen erabilerak susmagarrien defentsa-eskubideetan; horren barruan, bereziki kontuan hartzekoa da zelako zailtasuna dagoen —batez ere ikertutako pertsona fisikoen kasuan— sistema horien jardunbideari buruz informazioa eskuratzeko, tresna horien bidez lortutako emaitzak aurkaratu ahal izateko auzitegietan.

(60) Migrazio, asilo eta muga-kontrolaren kudeaketaren eremuetan erabiltzen diren AA-sistemak eragina dute egoera bereziki kalteberan egon ohi diren pertsonengan, zeinak eskumeneko agintaritza publikoen jarduketan emaitzen mende egoten baitira. Horregatik, bada, izugarri garrantzitsua da testuinguru horietan erabiltzen diren AA-sistemak zehatzak, ez-diskriminatzaileak eta gardenak izatea, egokiro bermatzeko ukitutako



transparentes, a fin de garantizar que se respeten los derechos fundamentales de las personas afectadas y, en particular, su derecho a la libre circulación, a la no discriminación, a la intimidad personal y la protección de los datos personales, a la protección internacional y a una buena administración. Por lo tanto, procede clasificar como de alto riesgo, en la medida en que su utilización esté permitida en virtud del Derecho de la Unión y nacional, aquellos sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos u organismos de la Unión que realizan tareas en el ámbito de la migración, el asilo y la gestión del control fronterizo como polígrafos y herramientas similares, para evaluar determinados riesgos que presenten las personas físicas que entren en el territorio de un Estado miembro o que soliciten un visado o asilo, para ayudar a las autoridades públicas competentes a examinar, con inclusión de la evaluación conexa de la fiabilidad de las pruebas, las solicitudes de asilo, visado y permiso de residencia, así como las reclamaciones conexas en relación con el objetivo de determinar si las personas físicas solicitantes reúnen los requisitos necesarios para que se conceda su solicitud, a efectos de detectar, reconocer o identificar a las personas físicas en el contexto de la migración, el asilo y la gestión del control fronterizo, con excepción de la verificación de los documentos de viaje. Los sistemas de IA en el ámbito de la migración, el asilo y la gestión del control fronterizo sujetos al presente Reglamento deben cumplir los requisitos procedimentales pertinentes establecidos por el Reglamento (CE) n.º 810/2009 del Parlamento Europeo y del Consejo (32), la Directiva 2013/32/UE del Parlamento Europeo y del Consejo (33) y otro Derecho de la Unión pertinente. El empleo de los sistemas de IA en la migración, el asilo y la gestión del control fronterizo no debe, en ningún caso, ser utilizado por los Estados miembros o las instituciones, órganos u organismos de la Unión como medio para eludir sus obligaciones internacionales en virtud de la Convención de las Naciones Unidas sobre el Estatuto de los Refugiados, hecha en Ginebra el 28 de julio de 1951, modificada por el Protocolo de 31 de enero de 1967. Tampoco debe ser utilizado para infringir en modo alguno el principio de no devolución, ni para negar unas vías jurídicas seguras y efectivas de acceso al territorio de la Unión, incluido el derecho a la protección internacional.

(61) Deben clasificarse como de alto riesgo determinados sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial. En particular, a fin de hacer frente al riesgo de posibles sesgos, errores y opacidades, procede clasificar como de alto riesgo

pertsonen oinarritzko eskubideak errespetatzen direla, bereziki hauek: zirkulazio aserako eskubidea, diskriminaziorik ez jasatekoa, intimitate pertsonalerako eskubidea eta datu pertsonalen babeserako eskubidea, nazioarteko babeserako eskubidea eta administrazio onerako eskubidea. Ondorioz, honako AA-sistema hauek, beren erabilera Batasuneko zuzenbidearen eta zuzenbide nazionalaren arabera baimenduta dagoen heinean, arrisku handikotzat sailkatu behar dira: agintaritza publiko eskudunek —edo haien izenean dihardutenek— edo Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak, esaterako poligrafoak eta antzeko beste tresna batzuk, helburutzat hartuta estatu kide bateko lurraldean sartzen diren edo bisa edo asilo bat eskatzen duten pertsona fisikoek dakartzaten arrisku jakin batzuk ebaluatzea, eta agintaritza publiko eskudunei laguntzea aztertzen —frogen fidagarritasunari buruzko ebaluazioa barne hartuta— asiloa, bisa eta bizileku-baimena eskuratzeko eskaerak, bai eta horiei lotutako erreklamazioak ere, informazio horren bidez zehaztu ahal izateko ea pertsona fisiko eskatzaileek beren eskaerak onartzeko beharrezkoak diren betekizunak betetzen dituzten, azterketa horren arabera migrazioaren, asiloaren eta muga-kontrolaren kudeaketari begira pertsona fisikoak detektatzeko, ezagutzeko edo identifikatzeko, salbuespen dela bidaia-agirien egiaztapena. Erregelamendu honi lotutako AA-sistemen barruan, migrazioaren, asiloaren eta muga-kontrolaren kudeaketaren esparruan erabiltzekoak diren sistemek prozedura-betekizun zehatzak bete behar dituzte, araudi honen arabera: Europako Parlamentuaren eta Kontseiluaren (EE) 810/2009 Erregelamendua (32), Europako Parlamentuaren eta Kontseiluaren 2013/32/EB Zuzentaraua (33) eta Batasuneko zuzenbidetik dagokien beste araudi guztia. Migrazioaren, asiloaren eta muga-kontrolaren kudeaketaren esparruan erabiltzen diren AA-sistemak ezin dira sekula baliatu estatu kideek edo Batasuneko instituzio, organo eta organismoek itzuri egin diezaieten beren nazioarteko betekizunei, zeinak Errefuxiatuen Estatutuari buruzko Nazio Batuen Konbentzioan ezarrita baitaude (Genevan 1951ko uztailaren 28an egina eta 1967ko urtarrilaren 31ko Protokoloak aldatua). Orobat, AA-sistemak ezin dira inolaz ere erabili ez-itzultzeko printzipioa urratzeko, ezta Batasuneko lurraldera sartzeko bide juridiko seguru eta eraginkorrak ukatzeko ere, barruan dela nazioarteko babeserako eskubidea.

(61) Justizia-administrazioa eta prozesu demokratikoetara bideratutako AA-sistema jakin batzuk arrisku handikotzat sailkatu behar dira; izan ere, eragin potentzialki garrantzitsuak izan ditzakete demokrazian, zuzenbide-estatuan, gizabanakoen askatasunetan eta benetako babes judizialerako eta epaile inpartziala izateko eskubidean. Alborapen-, errore- eta opakutasun-arriskuari aurre egiteko, egoki da AA-sistemak arrisku handikotzat sailkatzea, baldin eta agintaritza judizial



aquellos sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos. También deben considerarse de alto riesgo los sistemas de IA destinados a ser utilizados por los organismos de resolución alternativa de litigios con esos fines, cuando los resultados de los procedimientos de resolución alternativa de litigios surtan efectos jurídicos para las partes. La utilización de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe sustituirlas: la toma de decisiones finales debe seguir siendo una actividad humana. No obstante, la clasificación de los sistemas de IA como de alto riesgo no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la administración de justicia propiamente dicha en casos concretos, como la anonimización o seudonimización de resoluciones judiciales, documentos o datos, la comunicación entre los miembros del personal o las tareas administrativas.

(62) Sin perjuicio de las normas previstas en el Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo (34), y a fin de hacer frente a los riesgos de injerencia externa indebida en el derecho de voto consagrado en el artículo 39 de la Carta, y de efectos adversos sobre la democracia y el Estado de Derecho, deben clasificarse como sistemas de IA de alto riesgo los sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o un referéndum, o en el comportamiento electoral de las personas físicas en el ejercicio de su voto en elecciones o referendos, con excepción de los sistemas de IA a cuyos resultados de salida las personas físicas no están directamente expuestas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico.

(63) El hecho de que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea lícito con arreglo a otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión, por ejemplo, en materia de protección de los datos personales o la utilización de polígrafos y herramientas similares u otros sistemas para detectar el estado emocional de las personas físicas. Todo uso de ese tipo debe seguir realizándose exclusivamente en consonancia con los requisitos oportunos derivados de la Carta y de los actos aplicables del Derecho derivado de la Unión y del Derecho nacional. No debe entenderse que el presente Reglamento constituye un fundamento jurídico para el tratamiento de datos personales, incluidas las categorías especiales de datos personales, en su caso,

batek —edo haren izenean dihardutenek— erabiltzekoak badira agintaritza judizial bati laguntzeko bai egitateak eta zuzenbidea ikertzen eta interpretatzen, bai legea egitate jakin batzuei aplikatzen. Era berean, auziak bide ez-judizialek ebazteko organismoek helburu horretarako erabiltzen dituzten AA-sistemak arrisku handikotzat jo behar dira, auziak bide ez-judizialek ebazteko prozedurek ondorio juridikoak dituztenean aldeentzat. AA-tresnak erabiltzea lagungarri izan daiteke epaileen erabakitze-ahalerako edo independentzia judizialerako, baina ez ditu ordeztu behar: gizakiek jarraitu behar dute azken erabakiak hartzen. Nolanahi ere, osagarriak baizik ez diren administrazio-jarduerak egiteko baliatzen diren AA-sistemak ez dira arrisku handikotzat sailkatu behar, betiere justizia-administrazioari berari eragiten ez dioten kasu jakinetan erabiltzen badira, hala nola ebazpen judizialen, dokumentuen edo datuen anonimizazio edo pseudonimizazioan, langileen arteko komunikazioan edo administrazio-zereginetan.

(62) Europako Parlamentuaren eta Kontseiluaren (EB) 2024/900 Erregelamenduan (34) aurreikusitako arauak alde batera utzi gabe, eta Gutunaren 39. artikuluan jasotako boto-eskubidean kanpoko esku-hartze bidegabea gertatzeko eta demokraziaren eta zuzenbide-estatuaren gaineko ondorio kaltegarrien arriskuei aurre egiteko, arrisku handiko AA-sistema gisa sailkatu behar dira hauteskunde edo erreferendum baten emaitzan edo pertsona fisikoek hauteskundeetan edo erreferendumetan botoa emateko orduan duten hautespen-portaeran eragiteko erabiltzen diren AA-sistemak; alabaina, AA-sistemen irteera-emaitzek pertsona fisikoengan zuzenean eragiten ez badute, sistema horiek sailkapen honetatik kanpo geratzen dira —adibidez, kanpaina politikoak ikuspegi administratibo eta logistikotik antolatze, optimizatzeko eta egituratzeko erabiltzen diren tresnak—.

(63) AA-sistema bat erregelamendu honen arabera arrisku handiko AA-sistematzat kalifikatzeak ez du esan nahi haren erabilera bidezkoa denik Batasuneko zuzenbidearen edo Batasuneko zuzenbidearekin bateragarria den zuzenbide nazionalaren beste egintza batzuen arabera, esaterako datu pertsonalak babesteko arloan, poligrafoak eta antzeko tresnak erabiltzeko orduan, edo pertsona fisikoen egoera emozionala detektatzeko beste sistema batzuk baliatzeko orduan. Gisa horretako erabilerek berariaz betetzen jarraitu behar dute Gutunetik eta Batasuneko zuzenbidetik eta zuzenbide nazionaletik aplikatzekoak zaizkien betekizunak. Ez da ulertu behar erregelamendu honek oinarri juridiko bat osatzen duenik datu pertsonalen tratamendurako —datu pertsonalen kategoria bereziak



salvo que el presente Reglamento disponga específicamente otra cosa.

(64) Con el objetivo de mitigar los riesgos que presentan los sistemas de IA de alto riesgo que se introducen en el mercado o se ponen en servicio, y para garantizar un alto nivel de fiabilidad, deben aplicarse a los sistemas de IA de alto riesgo ciertos requisitos obligatorios que tengan en cuenta la finalidad prevista y el contexto del uso del sistema de IA y estén en consonancia con el sistema de gestión de riesgos que debe establecer el proveedor. Las medidas adoptadas por los proveedores para cumplir los requisitos obligatorios del presente Reglamento deben tener en cuenta el estado actual de la técnica generalmente reconocido en materia de IA, ser proporcionadas y eficaces para alcanzar los objetivos del presente Reglamento. Sobre la base del nuevo marco legislativo, como se aclara en la Comunicación de la Comisión titulada «“Guía azul” sobre la aplicación de la normativa europea relativa a los productos, de 2022», la norma general es que más de un acto jurídico de la legislación de armonización de la Unión puede ser aplicable a un producto, ya que la comercialización o la puesta en servicio solamente puede producirse cuando el producto cumple toda la legislación de armonización de la Unión aplicable. Los peligros de los sistemas de IA cubiertos por los requisitos del presente Reglamento se refieren a aspectos diferentes de los contemplados en la legislación de armonización de la Unión existente y, por consiguiente, los requisitos del presente Reglamento completarían el conjunto existente de legislación de armonización de la Unión. Por ejemplo, las máquinas o los productos sanitarios que incorporan un sistema de IA pueden presentar riesgos de los que no se ocupan los requisitos esenciales de salud y seguridad establecidos en la legislación armonizada de la Unión pertinente, ya que esa legislación sectorial no aborda los riesgos específicos de los sistemas de IA. Esto exige una aplicación simultánea y complementaria de diversos actos legislativos. A fin de garantizar la coherencia y evitar una carga administrativa innecesaria y costes innecesarios, los proveedores de un producto que contenga uno o varios sistemas de IA de alto riesgo, a los que se apliquen los requisitos del presente Reglamento y de los actos legislativos de armonización de la Unión basados en el nuevo marco legislativo y enumerados en un anexo del presente Reglamento, deben ser flexibles en lo que respecta a las decisiones operativas relativas a la manera de garantizar la conformidad de un producto que contenga uno o varios sistemas de IA con todos los requisitos aplicables de la legislación armonizada de la Unión de manera óptima. Esa flexibilidad podría significar, por ejemplo, la decisión del proveedor de integrar una parte de los procesos de prueba y notificación necesarios, así como la información y la documentación exigidas en virtud del presente Reglamento, en la documentación y los

barne, hala badagokio—, salbu eta erregelamendu honek berariaz bestelakorik esaten badu.

(64) Merkatuan jartzen diren edo zerbitzuan ipintzen diren arrisku handiko AA-sistemen arriskuak arintzeko eta fidagarritasun-maila handia bermatzeko, arrisku handiko AA-sistemei nahitaezko betekizun jakin batzuk aplikatu behar zaizkie, kontuan hartzen dituztenak AA-sistemaren helburu aurreikusia eta erabilera-testuingurua, eta bat datozenak hornitzaileak ezarri beharreko arrisku-kudeaketako sistemarekin. Hornitzaileek erregelamendu honetako nahitaezko betekizunak betetzeko hartutako neurriek kontuan izan behar dute zein den AAren arloan oro har aintzatetsitako teknikaren unean uneko egoera, eta proportzionatuak eta eraginkorrak izan behar dute erregelamendu honen helburuak lortzeko. Legegintza-esparru berria oinarri hartuta, Batzordearen 2022ko «Produktuei buruzko Europako araudiaren aplikazioari buruzko “Gida urdina”» izeneko Komunikazioan argitzen den bezala, arau orokorra da produktu berari Batasunaren harmonizazioko legeriako egintza juridiko bat baino gehiago aplikatu ahal izatea; izan ere, produktu bat merkaturatu edo zerbitzuan ipini ahal izateko, ezinbestekoa da produktuak guztiz betetzea aplikatzekoa zaion Batasunaren harmonizazioko legeria. Erregelamendu honetako betekizunak dituzten AA-sistemen arriskuak Batasunaren orain arteko harmonizazioko legerian jasotakoez bestelako arlo batzuk jorratzen dituzte; horrela, bada, erregelamendu honetako betekizunek osatu egiten dute Batasunaren orain arteko harmonizazioko legeria. Esate baterako, gerta daiteke AA-sistemak dituzten makinek edo osasun-produktuek ekar ditzaketen arriskuak ez egotea jasota Batasunaren harmonizazioko legerian ezarritako osasun eta segurtasuneko funtsezko betekizunetan, sektore horretako legeriak ez baititu jorratzen AA-sistemen arrisku espezifikoak. Halakoetan, bada, zenbait lege-egintza aplikatu behar dira, aldi berean eta modu osagarrian. Koherentzia bermatzeko eta beharrezkoak ez diren administrazio-kargak edo kostuak saihesteko, arrisku handiko AA-sistema bat edo gehiago dituzten produktuen kasuan —sistema horiei erregelamendu honetan eta Batasunaren harmonizazioko lege-egintzetan (legegintza-esparru berrian oinarritutakoak eta erregelamendu honen eranskin batean jasotakoak) ezarritako betekizunak aplikatzen zaizkien heinean—, hornitzaileek malguak izan behar dute erabaki operatiboak hartzeko orduan AA-sistema bat edo gehiago dituen produktu bat Batasunaren harmonizazioko legeriako betekizun aplikagarri guztiekin bat datorrela bermatzeko moduari dagokionez. Malgutasun horrek ekar lezake, adibidez, hornitzaileak erabakitzea beharrezkoak diren proba- eta jakinarazpen-prozesuen zati bat eta erregelamendu honen arabera eskatzen den informazioa eta dokumentazioa jasota uztea lehendik dauden dokumentazio eta prozeduretan, betetzekoak diren



procedimientos ya existentes exigidos en virtud de los actos legislativos de armonización de la Unión vigentes basados en el nuevo marco legislativo y enumerados en un anexo del presente Reglamento. Esto no debe socavar en modo alguno la obligación del proveedor de cumplir todos los requisitos aplicables.

(65) El sistema de gestión de riesgos debe consistir en un proceso iterativo continuo que sea planificado y ejecutado durante todo el ciclo de vida del sistema de IA de alto riesgo. Dicho proceso debe tener por objeto detectar y mitigar los riesgos pertinentes de los sistemas de IA para la salud, la seguridad y los derechos fundamentales. El sistema de gestión de riesgos debe revisarse y actualizarse periódicamente para garantizar su eficacia continua, así como la justificación y documentación de cualesquiera decisiones y acciones significativas adoptadas con arreglo al presente Reglamento. Este proceso debe garantizar que el proveedor determine los riesgos o efectos negativos y aplique medidas de mitigación de los riesgos conocidos y razonablemente previsibles de los sistemas de IA para la salud, la seguridad y los derechos fundamentales, habida cuenta de su finalidad prevista y de su uso indebido razonablemente previsible, incluidos los posibles riesgos derivados de la interacción entre el sistema de IA y el entorno en el que opera. El sistema de gestión de riesgos debe adoptar las medidas de gestión de riesgos más adecuadas a la luz del estado actual de la técnica en materia de IA. Al determinar las medidas de gestión de riesgos más adecuadas, el proveedor debe documentar y explicar las elecciones realizadas y, cuando proceda, contar con la participación de expertos y partes interesadas externas. Al determinar el uso indebido razonablemente previsible de los sistemas de IA de alto riesgo, el proveedor debe tener en cuenta los usos de los sistemas de IA que, aunque no estén directamente cubiertos por la finalidad prevista ni establecidos en las instrucciones de uso, cabe esperar razonablemente que se deriven de un comportamiento humano fácilmente previsible en el contexto de las características específicas y del uso de un sistema de IA concreto. Debe incluirse en las instrucciones de uso que sean facilitadas por el proveedor cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales. Con ello se pretende garantizar que el responsable del despliegue sea consciente de estos riesgos y los tenga en cuenta al utilizar el sistema de IA de alto riesgo. La identificación y la aplicación de medidas de reducción del riesgo en caso de uso indebido previsible con arreglo al presente Reglamento no deben suponer la exigencia, para su acometida, de entrenamiento adicional específico para el sistema de IA de alto riesgo por parte del proveedor para hacer frente a usos indebidos previsibles. No obstante, se anima a

heinean indarrean diren Batasunaren harmonizazioko lege-egintzen arabera, zeinak legegintza-esparru berrian oinarrituta baitaude eta erregelamendu honen eranskin batean zerrendatuta. Horrek ez dio inolaz ere kalte egin behar hornitzaileak betekizun aplikagarri guztiak betetzeko duen betebeharrari.

(65) Arriskuak kudeatzeko sistemak iterazio-prozesu jarraitua izan behar du, arrisku handiko AA-sistemaren bizi-ziklo osoan planifikatu eta gauzatuko dena. Prozesuak haxe izan behar du helburu: AA-sistemek osasunean, segurtasunean eta oinarritzko eskubideetan ekar ditzaketen arriskuak hautematea eta leuntzea. Arriskuak kudeatzeko sistema aldian-aldian berrikusi eta eguneratu behar da, etengabe eraginkorra dela bermatzeko eta erregelamendu honen arabera hartutako edozein erabaki eta ekintza garrantzitsuren justifikazioa eta dokumentazioa ziurtatzeko. Prozesu honen bidez bermatu behar da hornitzaileak bere gain hartuko dituela AA-sistemek osasunean, segurtasunean eta oinarritzko eskubideetan izan ditzaketen arrisku edo eragin kaltegarriak zehazteko zeregina, baita ezagunak eta arrazoiz aurreikusgarriak diren arriskuak leuntzeko neurriak ere, kontuan hartuta AA-sistema bakoitzak duen helburu aurreikusia eta arrazoiz aurreikus dakioken erabilera desegokia, barnean daudela AA-sistemaren eta dagokion ingurunearen interakziotik sor daitezkeen arriskuak. Arriskuak kudeatzeko sistemak arriskuak kudeatzeko neurri egokienak hartu behar ditu, AAren arloko teknikak unean-unean duen egoeraren arabera. Arriskuak kudeatzeko neurri egokienak zehaztean, hornitzaileak egindako aukeraketa dokumentatu eta azaldu behar du, eta, behar denean, adituen eta kanpoko alderdi interesdunen parte-hartzea izan. Arrisku handiko AA-sistemetan arrazoiz aurreikus daitekeen erabilera desegokia zehazteko orduan, hornitzaileak kontuan hartu behar du helburu aurreikusian zuzenean jasotako erabileretatik kanpoko eta erabilera-jarraibideetan ezarri gabeko zer erabilera eman dakiekeen hainbatean AA-sistemei, giza portaerari so erraz aurreikusteko moduan AA-sistema bakoitzaren ezaugarri espezifikoak eta erabilera aintzat hartuta. Hornitzaileak ematen dituen erabilera-jarraibideetan, berariaz jaso behar dira arrisku handiko AA-sistemaren gaineko gorabehera ezagun edo aurreikusgarri guztiak, aintzat hartuta hala helburu aurreikusiaren araberrako erabilerak nola arrazoiz aurreikus daitezkeen erabilera desegokiak, erabilera horiek arriskua eragin diezaieketen heinean bai osasunari eta segurtasunari, bai oinarritzko eskubideei. Horren bitartez bermatu nahi da hedapenaren ardura duna arriskuez ohar dadila eta kontuan har ditzala arrisku handiko AA-sistema erabiltzen duenean. Erregelamendu honen arabera aurreikus daitezkeen erabilera desegokiek eragindako arriskua murrizteko neurriak identifikatzeko eta aplikatzeko, ez da beharrezkoa izan behar hornitzaileak arrisku handiko AA-sistemarako entrenamendu osagarri berezia egiterik erabilera desegoki aurreikusgarriei aurre egiteko. Dena dela, bultzatzen da hornitzaileei



los proveedores a considerar dichas medidas de entrenamiento adicionales para mitigar los usos indebidos razonablemente previsibles, cuando resulte necesario y oportuno.

(66) Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a la gestión de riesgos, la calidad y la pertinencia de los conjuntos de datos utilizados, la documentación técnica y la conservación de registros, la transparencia y la comunicación de información a los responsables del despliegue, la supervisión humana, la solidez, la precisión y la ciberseguridad. Dichos requisitos son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad y los derechos fundamentales. Al no disponerse razonablemente de otras medidas menos restrictivas del comercio, dichos requisitos no son restricciones injustificadas al comercio.

(67) Los datos de alta calidad y el acceso a datos de alta calidad desempeñan un papel esencial a la hora de proporcionar una estructura y garantizar el funcionamiento de muchos sistemas de IA, en especial cuando se emplean técnicas que implican el entrenamiento de modelos, con vistas a garantizar que el sistema de IA de alto riesgo funcione del modo previsto y en condiciones de seguridad y no se convierta en una fuente de algún tipo de discriminación prohibida por el Derecho de la Unión. Es preciso instaurar prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos para el entrenamiento, la validación y la prueba sean de alta calidad. Los conjuntos de datos para el entrenamiento, la validación y la prueba, incluidas las etiquetas, deben ser pertinentes, lo suficientemente representativos y, en la mayor medida posible, estar libres de errores y ser completos en vista de la finalidad prevista del sistema. A fin de facilitar el cumplimiento del Derecho de la Unión en materia de protección de datos, como el Reglamento (UE) 2016/679, las prácticas de gestión y gobernanza de datos deben incluir, en el caso de los datos personales, la transparencia sobre el fin original de la recopilación de datos. Los conjuntos de datos deben tener las propiedades estadísticas adecuadas, también en lo que respecta a las personas o los colectivos de personas en relación con los que esté previsto utilizar el sistema de IA de alto riesgo, prestando una atención especial a la mitigación de los posibles sesgos en los conjuntos de datos que puedan afectar a la salud y la seguridad de las personas físicas, tener repercusiones negativas en los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando los datos de salida influyan en la información de entrada de futuras operaciones (bucles de retroalimentación). Los sesgos, por ejemplo, pueden ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos, o generados cuando los sistemas se despliegan en entornos del mundo real. Los resultados de los sistemas de IA

kontuan har ditzaten entrenamendu-neurri osagarri horiek, arrazoiz aurreikus daitezkeen erabilera desegoki horien eragina leundu ahal izan dezaten beharrezkoa eta egokia denean.

(66) Arrisku handiko AA-sistemei alderdi hauei buruzko betekizunak aplikatu behar zaizkie: arriskuen kudeaketa, erabilitako datu multzoen kalitatea eta egokitasuna, dokumentazio tekniko eta erregistroak gordetzea, gardentasuna eta hedapenaren arduradunei informazioa jakinaraztea, giza ikuskapena, sendotasuna, zehaztasuna eta zibersegurtasuna. Betekizun horiek beharrezkoak dira eraginkortasunez leuntzeko halako sistemak osasunean, segurtasunean eta oinarritzko eskubideetan eragin ditzaketen arriskuak. Ez dagoenez merkataritzarako hain murriztailea ez den bestelako arrazoizko neurririk, betekizun horiek ez dira merkataritzarako murrizketa bidegabeak.

(67) Kalitate handiko datuak eta kalitate handiko datuetarako sarbidea izatea funtsezkoa da AA-sistema askoren funtzionamendua bermatzeko eta sistemei hezurdura egokia emateko, batez ere ereduak entrenatzea eskatzen duten teknikak erabiltzen direnean, ziurtatze aldera arrisku handiko AA-sistemak aurreikusitako moduan eta segurtasun-baldintzetan funtzionatzen duela eta ez dela Batasuneko zuzenbideak debekatutako diskriminazioaren baten iturri. Beharrezkoa da datuen kudeaketa eta gobernantza egokia egiteko jardunbideak ezartzea, entrenamendu-, balioztatze- eta proba-datuak kalitate handikoak izan daitezen. Entrenamendu-, balioztatze- eta proba-datuen multzoek —etiketak barne— egokiak eta behar bezain esanguratsuak izan behar dute, eta errorerik gabeak eta ahalik eta osoenak, sistemaren helburu aurreikusia kontuan hartuta. Datuen babesaren arloan Batasunak ezarrita duen zuzenbidea eta (EB) 2016/679 Erregelamendua betetze aldera, datu pertsonalen kasuan, datuak kudeatzeko eta gobernatzeko jardunbideetan, gardentasunez adierazi behar da izatez zer helbururekin jaso diren datuok. Datu multzoek ezaugarri estatistiko egokiak izan behar dituzte —pertsona edo kolektiboek dagokienez ere bai, arrisku handiko AA-sistema haiei loturik erabiltzeko bada—, eta arreta berezia jarriko da datuetako alborapenak murrizteko, pertsona fisikoen osasunean eta segurtasunean eragina izan dezaketen heinean eta ondorio kaltegarriak ekarri oinarritzko eskubideetan edota Batasuneko zuzenbideak debekatutako diskriminazioaren bat sortu, batez ere irteera-datuak eragina dutenean etorkizuneko eragiketarako sarrera-informazioan (atzeraelikatze-begiztak). Gerta daiteke, adibidez, sistemaren barruko datu multzoak berezkoa izatea alborapena, batez ere datu historikoak erabiltzen direnean edo sistemak mundu errealeko inguruneetan hedatzean sortutako datuak erabiltzen direnean. AA-sistemen emaitzak berezko alborapen horien mende daude. Alborapen horiek, gainera, handitzeko joera dute



dependen de dichos sesgos inherentes, que tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente, en particular con respecto a las personas pertenecientes a determinados colectivos vulnerables, incluidos colectivos raciales o étnicos. El requisito de que los conjuntos de datos, en la mayor medida posible, sean completos y estén libres de errores no debe afectar al uso de técnicas de protección de la intimidad en el contexto del desarrollo y la prueba de sistemas de IA. En particular, los conjuntos de datos deben tener en cuenta, en la medida en que lo exija su finalidad prevista, los rasgos, características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que esté previsto que se utilice el sistema de IA. Los requisitos relacionados con la gobernanza de datos pueden cumplirse recurriendo a terceros que ofrezcan servicios certificados de cumplimiento, incluida la verificación de la gobernanza de datos, la integridad del conjunto de datos y las prácticas de entrenamiento, validación y prueba de datos, en la medida en que se garantice el cumplimiento de los requisitos en materia de datos del presente Reglamento.

(68) Para poder desarrollar y evaluar sistemas de IA de alto riesgo, determinados agentes, tales como proveedores, organismos notificados y otras entidades pertinentes, como centros europeos de innovación digital, instalaciones de ensayo y experimentación e investigadores, deben tener acceso a conjuntos de datos de alta calidad en sus campos de actividad relacionados con el presente Reglamento y deben poder utilizarlos. Los espacios comunes europeos de datos establecidos por la Comisión y la facilitación del intercambio de datos entre empresas y con los Gobiernos en favor del interés público serán esenciales para brindar un acceso fiable, responsable y no discriminatorio a datos de alta calidad con los que entrenar, validar y probar los sistemas de IA. Por ejemplo, en el ámbito de la salud, el espacio europeo de datos sanitarios facilitará el acceso no discriminatorio a datos sanitarios y el entrenamiento, a partir de esos conjuntos de datos, de algoritmos de IA de una manera segura, oportuna, transparente, fiable y que respete la intimidad, y contando con la debida gobernanza institucional. Las autoridades competentes pertinentes, incluidas las sectoriales, que proporcionan acceso a datos o lo facilitan también pueden brindar apoyo al suministro de datos de alta calidad con los que entrenar, validar y probar los sistemas de IA.

(69) El derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. Las medidas adoptadas por los proveedores para garantizar

arian-arian, eta, ondorioz, iraunarazi eta zabaldu egiten dute diskriminazioa, bereziki kolektibo kaltebera jakin batzuetako pertsonengan, arraza- edo etnia-kolektiboak ere barnean direla. Datu multzoak ahalik eta osoenak eta zuzenenak —errore gabeak— izateko betekizunak ez du eragotzi behar intimitatea babesteko teknikak erabiltzea AA-sistemak garatzeko eta probatzeko orduan. AA-sistemaren helburu aurreikusiak eskatzen duen neurrian, datu multzoek kontuan hartu behar dute, zehazki, zer bereizgarri, ezaugarri edo osagai berezi dituen AA-sistema aplikatzekoa den ingurune geografiko, kontestual, konduktual eta funtzionalak. Datuak gobernatzearekin lotutako betekizunak betetzeko, betetze-zerbitzu ziurtatuak eskaintzen dituzten hirugarren batzuetara jo daiteke, zerbitzu horien artean daudela datu-gobernantzaren egiaztapena, datu multzoaren integritatea eta datuak entrenatzeko, balioztatze eta probatzeko jardunbideak, betiere erregelamendu honetan datuen arloan zehaztutako betekizunak betetzen direla bermatuta.

(68) Arrisku handiko AA-sistemak garatu eta ebaluatu ahal izateko, eragile batzuek, hala nola hornitzaileek, organismo jakinaraziek eta egoki diren beste entitate batzuek —hor dira berrikuntza digitaleko Europako guneak, saiakuntza- eta esperimentazio-instalazioak eta ikertzaileak— sarbidea izan behar dute kalitate handiko datu multzoetara, erregelamendu honekin lotutako jarduera-eremuetan, eta datu horiek erabiltzeko aukera izan. Batzordeak ezarritako Europako datu-gune komunak zehaztea eta enpresen artean zein gobernuarekin interes publikoaren aldeko datu-trukea bideratzea funtsezko alderdiak izango dira kalitate handiko datuetarako sarbide fidagarria, arduratsua eta ez-diskriminatzailea eskaintzeko, hartara AA-sistemak egokiro entrenatu, balioztatu eta probatu ahal izateko. Esaterako, osasunaren arloan, osasunari buruzko datuen Europako guneak bide emango du osasunari buruzko datuetara diskriminaziorik gabe sarbidea izateko eta datu multzo horien bidez AA-algoritmoak entrenatzeko modu seguru, egoki, garden eta fidagarrian, intimitatea errespetatuta eta behar bezalako gobernantza instituzionalaren babesean. Datuetarako sarbidea ematen edo sarbide hori bideratzen duten agintaritzak eskudunek ere, agintaritzak sektorialak barne, laguntza eman dezakete kalitate handiko datuak emateko, AA-sistemak entrenatze, balioztatze eta probatze aldera.

(69) Intimitaterako eta datu pertsonalen babeserako eskubidea AA-sistemaren bizi-ziklo osoan bermatu behar da. Hala, bada, datu pertsonalen kasuan, datuak minimizatzeko eta datuen babesa diseinutik bertatik eta modu lehenetsian ezartzeko printzipioak dira aplikatzekoak, bi-biak Batasuneko zuzenbideak datuak babesteko arloan ezarritakoak. Printzipio horiek betetzen direla bermatzeko hornitzaileek hartzen



el cumplimiento de estos principios podrán incluir no solo la anonimización y el cifrado, sino también el uso de una tecnología que permita llevar los algoritmos a los datos y el entrenamiento de los sistemas de IA sin que sea necesaria la transmisión entre las partes ni la copia de los datos brutos o estructurados, sin perjuicio de los requisitos en materia de gobernanza de datos establecidos en el presente Reglamento.

(70) A fin de proteger los derechos de terceros frente a la discriminación que podría provocar el sesgo de los sistemas de IA, los proveedores deben —con carácter excepcional, en la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas y tras la aplicación de todas las condiciones aplicables establecidas en el presente Reglamento, además de las condiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680— ser capaces de tratar también categorías especiales de datos personales, como cuestión de interés público esencial en el sentido del artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y del artículo 10, apartado 2, letra g), del Reglamento (UE) 2018/1725.

(71) Para permitir la trazabilidad de los sistemas de IA de alto riesgo, verificar si cumplen los requisitos previstos en el presente Reglamento, así como vigilar su funcionamiento y llevar a cabo la vigilancia poscomercialización, resulta esencial disponer de información comprensible sobre el modo en que se han desarrollado y sobre su funcionamiento durante toda su vida útil. A tal fin, es preciso llevar registros y disponer de documentación técnica que contenga la información necesaria para evaluar si el sistema de IA de que se trate cumple los requisitos pertinentes y facilitar la vigilancia poscomercialización. Dicha información debe incluir las características generales, las capacidades y las limitaciones del sistema y los algoritmos, datos y procesos de entrenamiento, prueba y validación empleados, así como documentación sobre el sistema de gestión de riesgos pertinente, elaborada de manera clara y completa. La documentación técnica debe mantenerse adecuadamente actualizada durante toda la vida útil del sistema de IA. Además, los sistemas de IA de alto riesgo deben permitir técnicamente el registro automático de acontecimientos, mediante archivos de registro, durante toda la vida útil del sistema.

(72) A fin de abordar las preocupaciones relacionadas con la opacidad y complejidad de determinados sistemas de IA y ayudar a los responsables del despliegue a cumplir sus obligaciones en virtud del presente Reglamento, debe exigirse transparencia respecto de los sistemas de IA de alto riesgo antes de

dituzten neurriek, datuak anonimizatzeaz eta zifratzeaz gain, barnean har dezakete, halaber, algoritmoak datuetara eramateko eta AA-sistemak entrenatzeko teknologia erabiltzea, aldean artean datuak transmititzeko beharrik izan gabe eta datu gordinak edo egituratuak kopia beharrik izan gabe, betiere kontuan hartuta datuak gobernatzeari buruz erregelamendu honetan ezarritakoa.

(70) AA-sistemen alborapenak eragin dezakeen diskriminazioaren aurrean hirugarrenen eskubideak babesteko, salbuespen gisa, arrisku handiko AA-sistemei lotutako alborapenak detektatu eta zuzenduko direla bermatzeko behar-beharrezkotzat jotzen bada eta betiere pertsona fisikoen oinarritzko eskubide eta askatasunetarako berme egokiak betez eta erregelamendu honetan ezarritako baldintza aplikagarri guztiak aplikatu ondoren —(EB) 2016/679 Erregelamenduan eta (EB) 2018/1725 Erregelamenduan eta (EB) 2016/680 Zuzentarauan ezarritako baldintzez gain—, hornitzaileek gai izan behar dute datu pertsonalen kategoría bereziak ere interes publikoko funtsezko gai gisa tratatzeko, bat etorrita (EB) 2016/679 Erregelamenduaren 9.2 artikuluko g) letrarekin eta (EB) 2018/1725 Erregelamenduaren 10.2 artikuluko g) letrarekin.

(71) Arrisku handiko AA-sistemen trazabilitatea egin ahal izateko, erregelamendu honetan aurreikusitako betekizunak betetzen dituzten egiaztatzeko eta sistema horien funtzionamendua zaintzeko eta merkaturatu osteko zaintza egiteko, funtsezkoa da informazio ulergarria izatea sistema horiek garatzeko moduari eta haien balio-bizitza osoan izan duten funtzionamenduari buruz. Horretarako, erregistroak eraman eta dokumentazio teknikoak eduki behar da, behar den informazioa jaso dadin horietan, AA-sistemak dagozkion betekizunak betetzen ote dituen ebaluatu eta merkaturatu osteko zaintza egin ahal izateko. Informazio horrek sistemaren ezaugarri orokorrak, gaitasunak eta mugak jaso behar ditu, baita erabilitako algoritmoak, datuak eta entrenamendu-, proba- eta balioztatze-prozesuak ere; orobat, jaso beharrekoa du arriskuak kudeatzeko sistemari buruz dagokion dokumentazioa, modu argi eta osoan landua. Dokumentazio teknikoak behar bezala eguneratuta eduki behar da AA-sistemaren balio-bizitza osoan. Gainera, arrisku handiko AA-sistemek teknikoki aukera eman behar dute gertaerak modu automatikoan erregistratzeko, erregistro-artxiboen bidez, sistemaren balio-bizitza osoan.

(72) AA-sistema jakin batzuen opakutasunak eta konplexutasunak eragiten dituzten kezkei heltzeko eta hedapenaren arduradunei erregelamendu honen arabera dituzten betebeharrak betetzen laguntzeko, garrantasuna eskatu behar da arrisku handiko AA-sistemei dagokienez, sistema horiek merkaturatu jarri edo



su introducción en el mercado o su puesta en servicio. Los sistemas de IA de alto riesgo deben diseñarse de modo que permitan a los responsables del despliegue comprender la manera en que el sistema de IA funciona, evaluar su funcionalidad y comprender sus fortalezas y limitaciones. Los sistemas de IA de alto riesgo deben ir acompañados de la información adecuada en forma de instrucciones de uso. Dicha información debe incluir las características, las capacidades y las limitaciones del funcionamiento del sistema de IA. Estas comprenderían la información sobre las posibles circunstancias conocidas y previsibles relacionadas con el uso del sistema de IA de alto riesgo, incluida la actuación del responsable del despliegue capaz de influir en el comportamiento y el funcionamiento del sistema, en cuyo marco el sistema de IA puede dar lugar a riesgos para la salud, la seguridad y los derechos fundamentales, sobre los cambios que el proveedor haya predeterminado y evaluado para comprobar su conformidad y sobre las medidas pertinentes de supervisión humana, incluidas las medidas para facilitar la interpretación de los resultados de salida del sistema de IA por parte de los responsables del despliegue. La transparencia, incluidas las instrucciones de uso que acompañan a los sistemas de IA, debe ayudar a los responsables del despliegue a utilizar el sistema y tomar decisiones con conocimiento de causa. Los responsables del despliegue deben, entre otras cosas, estar en mejores condiciones para elegir correctamente el sistema que pretenden utilizar a la luz de las obligaciones que les son aplicables, estar informados sobre los usos previstos y excluidos y utilizar el sistema de IA correctamente y según proceda. A fin de mejorar la legibilidad y la accesibilidad de la información incluida en las instrucciones de uso, cuando proceda, deben incluirse ejemplos ilustrativos, por ejemplo sobre las limitaciones y sobre los usos previstos y excluidos del sistema de IA. Los proveedores deben garantizar que toda la documentación, incluidas las instrucciones de uso, contenga información significativa, exhaustiva, accesible y comprensible, que tenga en cuenta las necesidades y los conocimientos previsibles de los responsables del despliegue destinatarios. Las instrucciones de uso deben estar disponibles en una lengua fácilmente comprensible para los responsables del despliegue destinatarios, según lo que decida el Estado miembro de que se trate.

(73) Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que las personas físicas puedan supervisar su funcionamiento, así como asegurarse de que se usan según lo previsto y de que sus repercusiones se abordan a lo largo del ciclo de vida del sistema. A tal fin, el proveedor del sistema debe definir las medidas adecuadas de supervisión humana antes de su introducción en el mercado o puesta en servicio. Cuando proceda, dichas medidas deben garantizar, en concreto, que el sistema esté sujeto a limitaciones operativas incorporadas en el propio

zerbitzuan ipini aurretik. Arrisku handiko AA-sistemak egokiro diseinatu behar dira, hedapenaren arduradunek behar bezala ulertu ahal izan dezaten nola funtzionatzen duen AA-sistemak, zer-nolako funtzionaltasuna duen eta zer indargune eta muga dituen. Arrisku handiko AA-sistemek erabilera-jarraibide egokiak izan behar dituzte beti, behar den informazio guztia emateko, besteak beste AA-sistemaren ezaugarriei, gaitasunei eta funtzionamendu-mugei buruz. Hala, honako alderdi hauen gaineko informazioa jasoko da: batetik, arrisku handiko AA-sistemaren erabilerarekin lotutako inguruabar ezagun eta aurreikusgarriak —hedapenaren arduradunaren jarduketa barne, sistemaren portaeran eta funtzionamenduan eragiteko gai den heinean—, zeinen esparruan AA-sistemak arriskuak eragin baititzake osasunaren, segurtasunaren eta oinarrizko eskubideen eremuetan; bestetik, hornitzaileak adostasuna egiaztatzeko aurrez zehaztu eta ebaluatu dituen aldaketak, eta, azkenik, giza ikuskapenerako neurri egokiak, hedapenaren arduradunek AA-sistemaren irteera-emaitzak interpretatzen laguntzeko neurriak barne. Gardentasunak —barnean direla AA-sistemekin batera doazen erabilera-jarraibideak— sistema erabiltzen eta erabakiak jakinaren gainean hartzen lagundu behar die hedapenaren arduradunei. Hedapenaren arduradunek kokaleku egokian egon behar dute besteak beste, erabili nahi duten sistema behar bezala aukeratzeko aplikatzekoak zaizkien betebeharren arabera; bestalde, aurreikusitako eta baztertutako erabilerei buruzko informazioa izan behar dute, eta AA-sistema behar bezala eta dagokionaren arabera erabili. Erabilera-jarraibideetan jasotako informazioaren irakurgarritasuna eta irisgarritasuna hobetzeko, behar denean, adibide argigarriak txertatu behar dira, AA-sistemaren mugei eta sisteman aurreikusitako eta baztertutako erabilerei buruz, adibidez. Hornitzaileek berariaz bermatu behar dute dokumentazio guztiak —erabilera-jarraibideek barne— informazio adierazgarria, zehatza, irisgarria eta ulergarria duela eta informazio horrek kontuan hartzen dituela hartzaile diren hedapenaren arduradunek seguruenik izango dituzten premiak eta ezagutzak. Erabilera-jarraibideak hedapenaren arduradunek erraz ulertzeko moduko hizkuntza batean egon behar dute, kasuan kasuko estatu kideak erabakitzen duenaren arabera.

(73) Arrisku handiko AA-sistemen diseinuak eta garapenak bide eman behar dute pertsona fisikoek sistemen funtzionamendua ikuskatu ahal izateko eta ziurtatzeko sistemak aurreikusi moduan erabiltzen direla eta haien ondorioak haien bizi-ziklo osoan jorratzen direla. Horretarako, sistemaren hornitzaileak giza ikuskapeneko neurri egokiak zein diren zehaztu behar du, sistema merkatuan jarri edo zerbitzuan ipini aurretik. Behar denean, neurri horiek zehazki bermatu behar dute sistemak muga operatiboak dituela —sisteman bertan txertatuta daudenak eta sistemak desaktibatu ezin



sistema que este no pueda desactivar, que responda al operador humano y que las personas físicas a quienes se haya encomendado la supervisión humana posean las competencias, la formación y la autoridad necesarias para desempeñar esa función. También es esencial, según proceda, garantizar que los sistemas de IA de alto riesgo incluyan mecanismos destinados a orientar e informar a las personas físicas a las que se haya asignado la supervisión humana para que tomen decisiones con conocimiento de causa acerca de si intervenir, cuándo hacerlo y de qué manera, a fin de evitar consecuencias negativas o riesgos, o de detener el sistema si no funciona según lo previsto. Teniendo en cuenta las enormes consecuencias para las personas en caso de una correspondencia incorrecta efectuada por determinados sistemas de identificación biométrica, conviene establecer un requisito de supervisión humana reforzada para dichos sistemas, de modo que el responsable del despliegue no pueda actuar ni tomar ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas la han verificado y confirmado por separado. Dichas personas podrían proceder de una o varias entidades e incluir a la persona que maneja o utiliza el sistema. Este requisito no debe suponer una carga ni retrasos innecesarios y podría bastar con que las verificaciones que las distintas personas efectúen por separado se registren automáticamente en los registros generados por el sistema. Dadas las especificidades de los ámbitos de la garantía del cumplimiento del Derecho, la migración, el control fronterizo y el asilo, ese requisito no debe aplicarse cuando el Derecho nacional o de la Unión considere que su aplicación es desproporcionada.

(74) Los sistemas de IA de alto riesgo deben funcionar de manera uniforme durante todo su ciclo de vida y presentar un nivel adecuado de precisión, solidez y ciberseguridad, a la luz de su finalidad prevista y con arreglo al estado actual de la técnica generalmente reconocido. Se anima a la Comisión y las organizaciones y partes interesadas pertinentes a que tengan debidamente en cuenta la mitigación de los riesgos y las repercusiones negativas del sistema de IA. El nivel previsto de los parámetros de funcionamiento debe declararse en las instrucciones de uso que acompañen a los sistemas de IA. Se insta a los proveedores a que comuniquen dicha información a los responsables del despliegue de manera clara y fácilmente comprensible, sin malentendidos ni afirmaciones engañosas. El Derecho de la Unión en materia de metrología legal, incluidas las Directivas 2014/31/UE (35) y 2014/32/UE (36) del Parlamento Europeo y del Consejo, tiene por objeto garantizar la precisión de las mediciones y contribuir a la transparencia y la equidad de las transacciones comerciales. En ese contexto, en cooperación con las partes interesadas y las organizaciones pertinentes,

dituenak—, sistemak giza operadoreari erantzuten diola eta giza ikuskapena esleitu zaien pertsona fisikoei eginkizun hori betetzeko behar diren konpetentziak, prestakuntza eta aginpidea dituztela. Era berean, funtsezkoa da, behar denean, arrisku handiko AA-sistemek bermatzea mekanismo egokiak barne hartzen dituztela, mekanismo horien bidez orientazioa eta informazioa eman dakien giza ikuskapena esleitu zaien pertsona fisikoei, hartara jakinaren gainean har ditzaten erabakiak: esku hartu edo ez, eta noiz eta nola esku hartu ondorio negatiboak edo arriskuak saihesteko, edo sistema geldiarazi behar ote den aurreikusitakoaren arabera funtzionatzen ez badu. Kontuan hartuta identifikazio biometrikoko sistema jakin batzuek okerreko korrespondentzia eginez gero pertsonentzat zer-nolako ondorio larriak ekar ditzaketen, komeni da sistema horietan giza ikuskapen indartua egiteko betekizuna ezartzea, hedapenaren arduradunarentzat ezinezkoa izan dadin sistemak sortutako identifikazioan oinarrituta jardutea eta erabakirik hartzea; salbu eta gutxienez bi pertsona fisikok, nork bere aldetik, identifikazio hori egiaztatu eta baieztatu badute. Pertsona horiek entitate berekoak izan daitezke edo ez, eta sistema maneiatzen edo erabiltzen duen pertsona ere barne hartu. Betekizun horrek ez du alferreko kargarik edo atzerapenik eragin behar, eta nahikoa izan liteke pertsona horiek nork bere aldetik egiten dituzten egiaztapenak automatikoki erregistratzea sistemak sortutako erregistroetan. Zuzenbidea betearaztearen, migrazioaren, muga-kontrolaren eta asiloaren eremuen berezitasunak kontuan hartuta, betekizun hori ez da aplikatu behar zuzenbide nazionalak edo Batasunekoak neurritz kanpokotzat jotzen badu haren aplikazioa.

(74) Arrisku handiko AA-sistemek modu uniformearen funtzionatu behar dute bizi-ziklo osoan, eta zehaztasun-, sendotasun- eta zibersegurtasun-maila egokia izan, helburu aurrekusiaren arabera eta oro har aitortutako teknikaren unean uneko egoeraren arabera. Bultzatzen da Batzordeari, antolakundeei eta egoki diren alderdi interesdunei, kontuan har dezaten beharrezkoa dela AA-sistemaren arriskuak eta ondorio kaltegarriak leuntzea. AA-sistemen erabilera-jarraibideetan adierazi behar da jardunbide-parametroetarako aurreikusitako maila. Dei egiten da hornitzaileei, informazio hori argi eta modu ulergarriaren jakinaraz diezaieten hedapenaren arduradunei, gaizki-ulerturik eta iruzurrik gerta ez dadin. Batasuneko zuzenbideak metrologiaren arloan emandako arauak —Europako Parlamentuaren eta Kontseiluaren 2014/31/EB (35) eta 2014/32/EB (36) zuzentarauak barne— helburu dute neurketen zehaztasuna bermatzea eta merkataritza-transakzioen garrantasuna eta ekitatea bultzatzea. Hala, egoki diren alderdi interesdun eta antolakundeekin lankidetzan —hor dira, besteak beste, metrologiako eta ebaluazio konparatiboko agintaritzak— Batzordeak bultzada eman behar die, egoki den eran, AA-sistemak neurtzeko



como las autoridades de metrología y de evaluación comparativa, la Comisión debe fomentar, según proceda, el desarrollo de parámetros de referencia y metodologías de medición para los sistemas de IA. Al hacerlo, la Comisión debe tomar nota de los socios internacionales que trabajan en la metrología y los indicadores de medición pertinentes relacionados con la IA y colaborar con ellos.

(75) La solidez técnica es un requisito clave para los sistemas de IA de alto riesgo, que deben ser resilientes en relación con los comportamientos perjudiciales o indeseables por otros motivos que puedan derivarse de limitaciones en los sistemas o del entorno en el que estos funcionan (p. ej., errores, fallos, incoherencias o situaciones inesperadas). Por consiguiente, deben adoptarse medidas técnicas y organizativas para garantizar la solidez de los sistemas de IA de alto riesgo, por ejemplo mediante el diseño y desarrollo de soluciones técnicas adecuadas para prevenir o reducir al mínimo ese comportamiento perjudicial o indeseable. Estas soluciones técnicas pueden incluir, por ejemplo, mecanismos que permitan al sistema interrumpir de forma segura su funcionamiento (planes de prevención contra fallos) en presencia de determinadas anomalías o cuando el funcionamiento tenga lugar fuera de determinados límites predeterminados. El hecho de no adoptar medidas de protección frente a estos riesgos podría tener consecuencias para la seguridad o afectar de manera negativa a los derechos fundamentales, por ejemplo, debido a decisiones equivocadas o resultados de salida erróneos o sesgados generados por el sistema de IA.

(76) La ciberseguridad es fundamental para garantizar que los sistemas de IA resistan a las actuaciones de terceros maliciosos que, aprovechando las vulnerabilidades del sistema, traten de alterar su uso, comportamiento o funcionamiento o de poner en peligro sus propiedades de seguridad. Los ciberataques contra sistemas de IA pueden dirigirse contra activos específicos de la IA, como los conjuntos de datos de entrenamiento (p. ej., envenenamiento de datos) o los modelos entrenados (p. ej., ataques adversarios o inferencia de pertenencia), o aprovechar las vulnerabilidades de los activos digitales del sistema de IA o la infraestructura de TIC subyacente. Por lo tanto, para garantizar un nivel de ciberseguridad adecuado a los riesgos, los proveedores de sistemas de IA de alto riesgo deben adoptar medidas adecuadas, como los controles de seguridad, teniendo también en cuenta, cuando proceda, la infraestructura de TIC subyacente.

(77) Sin perjuicio de los requisitos relacionados con la solidez y la precisión establecidos en el presente Reglamento, los sistemas de IA de alto riesgo que entren en el ámbito de aplicación de un reglamento del Parlamento Europeo y del Consejo relativo a los

erreferentziako parametroei eta metodologiei. Eginkizun horretarako, Batzordeak kontuan hartu behar ditu metrologiaren arloan diharduten nazioarteko bazkideak eta AAri lotutako neurketa-adierazleak, eta haiekin lankidetzan jardun.

(75) Sendotasun teknikoa funtsezko betekizuna da arrisku handiko AA-sistemetarako; izan ere, erresilienteak izan behar dute, sistemetako mugen edo sistemen jardun-inguruneen ondorioz sortutako portaera kaltegarrien edo bestelako nahi gabeko portaeren aurrean (erroreak, hutsegiteak, inkoherentziak edo ustekabeko egoerak eta beste). Ondorioz, neurri teknikoak eta antolakuntzakoak hartu behar dira, arrisku handiko AA-sistemen sendotasuna bermatzeko, adibidez soluzio tekniko egokiak diseinatuta edo garatuta ahal beste prebenitzeko edo murrizteko portaera kaltegarri edo nahi gabeko hori. Soluzio tekniko horien barruan egon daitezke, esaterako, jarduna era seguruan eteteko modua ematen duten mekanismoak (hutsegiteen aurkako prebentzio-planak), abian jar daitezen anomalia jakin batzuk gertatzen direnean edo sistemak aurrez zehaztuta dauden mugetatik kanpo diharduenean. Arrisku horien aurrean babes-neurriak ez hartzeak ondorioak izan ditzake segurtasunean edo kalte egin oinarritzko eskubideei, adibidez AA-sistemak okerreko erabakiak eragin dituelako edo irteera-emitza okerrak edo alboratuak sortu dituelako.

(76) Zibersegurtasuna funtsezkoa da bermatzeko AA-sistemak egokiro aurre egiten diela hirugarren gaiztoen jarduketei, sistemaren ahulguneak aprobetxatuz haren erabilera, portaera edo jardunbidea aldatzen edo segurtasun-propietateak arriskuan jartzen saiatzen badira ere. AA-sistemen kontrako zibererasoak AAren aktibo espezifikoek aurkakoak izan daitezke, hala nola entrenamendu-datuak multzoen aurkakoak (datuak pozoituta, esaterako) edo eredu entrenatuen aurkakoak (aurkarien erasoak edo kidetza-inferentzia, adibidez). Beste aukera bat da AA-sistemaren aktibo digitalen edo azpiko IKT azpiegituraren ahuleziez baliatzea. Hortaz, arriskueta ondo egokitutako zibersegurtasun-maila bermatzeko, arrisku handiko AA-sistemen hornitzaileek neurri aproposak hartu behar dituzte —segurtasun-kontrolak, adibidez— kontuan hartuta, hala badagokio, azpiko IKT azpiegitura.

(77) Elementu digitalak dituzten produktuen zibersegurtasuna bermatzeko betekizun horizontalei buruz Europako Parlamentuak eta Kontseiluak emandako erregelamendu baten aplikazio-eremuan sartzen diren arrisku handiko AA-sistemak,



requisitos horizontales de ciberseguridad para los productos con elementos digitales, de conformidad con dicho reglamento, pueden demostrar el cumplimiento con los requisitos de ciberseguridad del presente Reglamento mediante el cumplimiento de los requisitos esenciales de ciberseguridad establecidos en dicho reglamento. Cuando los sistemas de IA de alto riesgo cumplan los requisitos esenciales de ciberseguridad de un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, debe presumirse que cumplen los requisitos de ciberseguridad del presente Reglamento en la medida en que la satisfacción de esos requisitos se demuestre en la declaración UE de conformidad de emitida con arreglo a dicho reglamento, o partes de esta. A tal fin, la evaluación de los riesgos de ciberseguridad asociados a un producto con elementos digitales clasificado como un sistema de IA de alto riesgo con arreglo al presente Reglamento, realizada en virtud de un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, debe tener en cuenta los riesgos para la ciberresiliencia de un sistema de IA por lo que respecta a los intentos de terceros no autorizados de alterar su uso, comportamiento o funcionamiento, incluidas las vulnerabilidades específicas de la IA, como el envenenamiento de datos o los ataques adversarios, así como, en su caso, los riesgos para los derechos fundamentales, tal como exige el presente Reglamento.

(78) El procedimiento de evaluación de la conformidad establecido en el presente Reglamento debe aplicarse en relación con los requisitos esenciales de ciberseguridad de un producto con elementos digitales regulado por un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y clasificado como sistema de IA de alto riesgo con arreglo al presente Reglamento. Sin embargo, esta norma no debe dar lugar a una reducción del nivel de garantía necesario para los productos críticos con elementos digitales sujetos a un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales. Por consiguiente, no obstante lo dispuesto en esta norma, los sistemas de IA de alto riesgo que entran dentro del ámbito de aplicación del presente Reglamento y que también se consideran productos críticos importantes con elementos digitales en virtud de un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, y a los que se aplica el procedimiento de evaluación de la conformidad fundamentado en un control interno que se establece en

erregelamendu horrekin bat etorrita, hartan ezarritako zibersegurtasuneko funtsezko betekizunak beteta frogatu dezakete erregelamendu honetako zibersegurtasun-betekizunak betetzen dituztela; hargatik eragotzi gabe erregelamendu honetan sendotasunarekin eta zehaztasunarekin lotuta ezarritako betekizunak. Arrisku handiko AA-sistemek Europako Parlamentuaren eta Kontseiluaren erregelamendu bateko zibersegurtasuneko funtsezko betekizunak betetzen dituztenean elementu digitaleko produktuen zibersegurtasuna bermatzeko betekizun horizontalei dagokienez, erregelamendu honetako zibersegurtasuneko betekizunak betetzen dituztela jo behar da, betiere betetze hori erregelamendu haren arabera emandako EB adostasun-adierazpenean eta haren zati batzuetan frogatzen bada. Horretarako, produktu batek erregelamendu honen arabera arrisku handiko AA-sistematzat sailkatutako elementu digitalak dituenean, produktuari lotutako zibersegurtasuneko arriskuak ebaluatzeko orduan bat etorrita elementu digitaleko produktuen zibersegurtasuna bermatzeko betekizun horizontalei buruz Europako Parlamentuak eta Kontseiluak emandako erregelamendu batekin, kontuan hartu beharrekoa da hirugarren ez-baimendu batzuek sistemaren erabilera, portaera edo jardunbidea aldarazteko egiten duten saiakerek zer-nolako arriskua dakarkioten AA-sistema baten zibererresilientziari, kontuan hartuta AA horren kalteberatasun zehatzak, hala nola datuak pozoitzea edo aurkariaren erasoak izatea, bai, halaber, hala behar bada, oinarritzko eskubideetan duen arriskua, erregelamendu honek eskatu bezala.

(78) Erregelamendu honetan ezarritako adostasuna ebaluatzeko prozedura elementu digitaleko produktuen zibersegurtasuna bermatzeko funtsezko betekizunei lotuta aplikatu beharrekoa da, produktu horiek zibersegurtasun-betekizun horizontalei buruz Europako Parlamentuak eta Kontseiluak emandako erregelamendu baten bidez araututa dauden heinean eta honako erregelamendu honen arabera arrisku handiko AA-sistematzat sailkatuta dauden heinean. Arau horrek, alabaina, ez du murriztarazi behar elementu digitaleko produktuen zibersegurtasuna bermatzeko betekizun horizontalei buruz Europako Parlamentuak eta Kontseiluak emandako erregelamendu bati lotutako elementu digitaleko produktu kritikoek eduki beharreko berme-maila. Horrenbestez, arau honetan ezarritakoa gorabehera, erregelamendu honen aplikazio-eremuan sartzen diren arrisku handiko AA-sistemek, elementu digitaleko produktuen zibersegurtasuna bermatzeko betekizun horizontalei buruz Europako Parlamentuak eta Kontseiluak emandako erregelamendu baten arabera elementu digitaleko produktu kritikotzat ere jotzen diren heinean eta adostasuna ebaluatzeko prozedura aplikatzen zaien heinean —erregelamendu honetako eranskin batean ezarritako barne-kontrol batean oinarritutako prozedura berau—, bete beharrekoa dute



un anexo del presente Reglamento, están sujetos a lo dispuesto en un reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales en materia de evaluación de la conformidad por lo que se refiere a los requisitos esenciales de ciberseguridad de dicho reglamento. En tal caso, en relación con todos los demás aspectos que entren en el ámbito de aplicación del presente Reglamento, debe aplicarse lo dispuesto en el anexo VI del presente Reglamento en materia de evaluación de la conformidad fundamentada en un control interno. Habida cuenta de los conocimientos y la experiencia de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en materia de política de ciberseguridad y de las tareas que se le encomiendan en virtud del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo (37), la Comisión debe cooperar con ENISA en las cuestiones relacionadas con la ciberseguridad de los sistemas de IA.

(79) Conviene que una persona física o jurídica concreta, definida como el proveedor, asuma la responsabilidad asociada a la introducción en el mercado o la puesta en servicio de un sistema de IA de alto riesgo, con independencia de si dicha persona física o jurídica es o no quien diseñó o desarrolló el sistema.

(80) Como signatarios de la Convención sobre los Derechos de las Personas con Discapacidad, la Unión y todos los Estados miembros están legalmente obligados a proteger a las personas con discapacidad contra la discriminación y a promover su igualdad, a garantizar que las personas con discapacidad tengan acceso, en igualdad de condiciones con las demás, a las tecnologías y sistemas de la información y las comunicaciones, y a garantizar el respeto a la intimidad de las personas con discapacidad. Habida cuenta de la importancia y el uso crecientes de los sistemas de IA, la aplicación de los principios de diseño universal a todas las nuevas tecnologías y servicios debe garantizar el acceso pleno e igualitario de todas las personas a las que puedan afectar las tecnologías de IA o que puedan utilizar dichas tecnologías, incluidas las personas con discapacidad, de forma que se tenga plenamente en cuenta su dignidad y diversidad inherentes. Por ello es esencial que los proveedores garanticen el pleno cumplimiento de los requisitos de accesibilidad, incluidas la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo (38) y la Directiva (UE) 2019/882. Los proveedores deben garantizar el cumplimiento de estos requisitos desde el diseño. Por consiguiente, las medidas necesarias deben integrarse en la medida de lo posible en el diseño de los sistemas de IA de alto riesgo.

elementu digitaleko produktuetan zibersegurtasuna bermatzeko betekizun horizontalei buruz Europako Parlamentuak eta Kontseiluak emandako erregelamendu batek adostasuna ebaluatzeko arloan xedatutakoa erregelamendu horren funtsezko zibersegurtasun-betekizunei dagokienez. Halakoetan, erregelamendu honen aplikazio-eremuan sartzen diren gainerako alderdietan, erregelamendu honen VI. eranskinean barne-kontrolean oinarritutako adostasunaren ebaluazioaren arloan ezarritakoa da aplikatzekoa. Kontuan hartuta Zibersegurtasunerako Europar Batasuneko Agentziak (ENISA) zibersegurtasun-politikaren arloan dituen ezagutzak eta esperientzia, bai eta Europako Parlamentuaren eta Kontseiluaren (EB) 2019/881 Erregelamenduaren arabera (37) esleitzen zaizkion zereginak ere, Batzordeak ENISArekin lankidetzan aritu behar du AA-sistemen zibersegurtasunarekin lotutako gaitetan.

(79) Komeni da pertsona fisiko edo juridiko jakin batek, hornitzailetzat zehaztutakoa, bere gain hartzea arrisku handiko AA-sistema bat merkatuan jartzeari edo zerbitzuan ipintzeari lotutako erantzukizuna, pertsona fisiko edo juridiko hori sistema diseinatu edo garatu zuen pertsona bera izan zein ez.

(80) Batasuna eta haren estatu kide guztiak, Desgaitasuna duten Pertsonen Eskubideei buruzko Konbentzioa sinatuta dutenez gero, legez behartuta daude desgaitasuna duten pertsonak diskriminazioaren aurka babestera eta haien berdintasuna sustatzera, bai, halaber, bermatzera desgaitasuna duten pertsonen gainerakoen baldintza berberetan dituztela eskuragarri informazioaren eta komunikazioen teknologiak eta sistemak, eta bermatzera, orobat, desgaitasuna duten pertsonen intimitatea errespetatzen dela. Kontuan hartuta AA-sistemak gero eta garrantzi handiagoa hartzen ari direla eta gero eta gehiago erabiltzen direla, diseinu unibertsalaren printzipioak teknologia eta zerbitzu berri guztietan aplikatzeko orduan berariaz bermatu behar da AA-teknologiek ukitu ditzaketen edo teknologia horiek erabil ditzaketen pertsona guztiek — desgaitasuna duten pertsonak barne— sarbide osoa eta berdintasuneko izango dutela, erabat aintzat hartuta pertsona guztiek berezko duten duintasuna eta aniztasuna. Horregatik, funtsezkoa da hornitzaileek bermatzea erabat betetzen direla irisgarritasun-betekizunak, barnean hartuta Europako Parlamentuaren eta Kontseiluaren (EB) 2016/2102 Zuzentaraua (38) eta (EB) 2019/882 Zuzentaraua. Hornitzaileek diseinutik bertatik bermatu behar dute betekizunok betetzen direla. Hala, beharrezkoak diren neurriak ahal bezain beste txertatu behar dira arrisku handiko AA-sistemetan diseinuan.



(81) El proveedor debe instaurar un sistema de gestión de la calidad sólido, velar por que se siga el procedimiento de evaluación de la conformidad necesario, elaborar la documentación pertinente y establecer un sistema de vigilancia poscomercialización sólido. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad con arreglo al Derecho sectorial pertinente de la Unión deben tener la posibilidad de integrar los elementos del sistema de gestión de la calidad establecido en el presente Reglamento en el sistema de gestión de la calidad establecido en dicho Derecho sectorial de la Unión. La complementariedad entre el presente Reglamento y el Derecho sectorial vigente de la Unión también debe tenerse en cuenta en las futuras actividades de normalización o en las orientaciones adoptadas por la Comisión al respecto. Las autoridades públicas que pongan en servicio sistemas de IA de alto riesgo para su propio uso pueden aprobar y aplicar las normas que regulen el sistema de gestión de la calidad en el marco del sistema de gestión de la calidad adoptado a escala nacional o regional, según proceda, teniendo en cuenta las particularidades del sector y las competencias y la organización de la autoridad pública de que se trate.

(82) Para permitir la ejecución del presente Reglamento y ofrecer igualdad de condiciones a los operadores, es importante velar por que una persona establecida en la Unión pueda, en cualquier circunstancia, facilitar a las autoridades toda la información necesaria sobre la conformidad de un sistema de IA, teniendo en cuenta las distintas formas en que se pueden ofrecer productos digitales. Por lo tanto, antes de comercializar sus sistemas de IA en la Unión, los proveedores establecidos fuera de su territorio deben designar, mediante un mandato escrito, a un representante autorizado que se encuentre en la Unión. El representante autorizado desempeña un papel fundamental a la hora de velar por la conformidad de los sistemas de IA de alto riesgo introducidos en el mercado o puestos en servicio en la Unión por esos proveedores no establecidos en la Unión y servir de persona de contacto establecida en la Unión.

(83) Teniendo en cuenta la naturaleza y la complejidad de la cadena de valor de los sistemas de IA y de conformidad con el nuevo marco legislativo, es esencial garantizar la seguridad jurídica y facilitar el cumplimiento del presente Reglamento. Por ello es necesario aclarar la función y las obligaciones específicas de los operadores pertinentes de toda dicha cadena de valor, como los importadores y los distribuidores, que pueden contribuir al desarrollo de sistemas de IA. En determinadas situaciones, esos operadores pueden desempeñar más de una función al mismo tiempo y, por lo tanto, deben cumplir de forma acumulativa todas las obligaciones pertinentes asociadas a dichas funciones.

(81) Hornitzaileak kalitatea kudeatzeko sistema sendo bat ezarri behar du, adostasuna ebaluatzeko dagokion prozedura betetzen dela zaindu, behar den dokumentazioa landu eta merkaturatu osteko zaintza-sistema indartsu bat jarri. Arrisku handiko AA-sistemen hornitzaileak, Batasuneko zuzenbide sektorial zehatz horretarako xedatutako betekizunak bete behar dituzten heinean, aukera izan behar dute erregelamendu honetan kalitatea kudeatzeko ezarritako sistemaren elementuak Batasuneko zuzenbide sektorialean kalitatea kudeatzeko ezarritako sisteman txertatzeko. Erregelamendu honen eta Batasunean indarrean dagoen zuzenbide sektorialaren arteko osagarritasuna ere kontuan hartu behar da etorkizuneko normalizazio-jardueretan edo Batzordeak arlo honetan hartzen dituen orientabideetan. Agintaritza publikoek arrisku handiko AA-sistemak beren barne erabilerarako ipintzen dituztenean zerbitzuan, dena delako estatuan edo erregioan —dagokionaren arabera— kalitatea kudeatzeko ezarritako sistemaren esparruan onartu eta aplikatu ahal izango dituzte kalitatea kudeatzeko sistema erregulatzeko arauak, sektorearen berezitasunak kontuan hartuta eta bat etorrita dena delako agintaritza publikoaren eskumenekin eta antolamenduarekin.

(82) Erregelamendu hau betearazi eta operadore guztiei baldintza berberetan jarduteko modua emateko, garrantzitsua da zaintzea ezen Batasunean kokatutako pertsonak, edozein egoeratan, AA-sistema baten adostasunari buruz behar den informazio guztia eman diezaieketela agintaritzei, produktu digitalak eskaintzeko aukeran dauden askotariko moduak kontuan hartuta. Beraz, Batasunetik kanpo kokatutako hornitzaileek, beren AA-sistemak Batasunean merkaturatu aurretik, Batasunean dagoen ordezkari baimendu bat izendatu behar dute, idatzizko mandatu baten bidez. Ordezkari baimenduak funtsezko eginkizuna betetzen du Batasunetik kanpoko hornitzaileek Batasuneko merkatuan jarritako edo zerbitzuan ipinitako arrisku handiko AA-sistemen adostasuna zaintzeko eta Batasunean harremanetarako pertsona gisa jarduteko.

(83) AA-sistemen balio-katearen izaera eta konplexutasuna kontuan hartuta eta lege-esparru berriarekin bat etorritik, ezinbestekoa da segurtasun juridikoa bermatzea eta erregelamendu hau betetzen laguntzea. Horregatik, beharrezkoa da argitzea zehazki zein eginkizun eta betebeharrak betetzen dituzten balio-kate oso horretan AA-sistemen garapenean esku har dezaketen operadoreek, hala nola inportatzaile eta banatzaileak. Egoera jakin batzuetan, operadore horiek eginkizun bat baino gehiago bete dezakete aldi berean; halakoetan, eginkizun horiei lotuta egoki diren betebeharrak guztiak bete behar dituzte metatuta. Esate baterako,



Por ejemplo, un operador puede actuar como distribuidor e importador al mismo tiempo.

(84) Para garantizar la seguridad jurídica, es necesario aclarar que, en determinadas condiciones específicas, debe considerarse proveedor de un sistema de IA de alto riesgo a cualquier distribuidor, importador, responsable del despliegue u otro tercero que, por tanto, debe asumir todas las obligaciones pertinentes. Este sería el caso si, por ejemplo, esa persona pone su nombre o marca en un sistema de IA de alto riesgo ya introducido en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen otra distribución de las obligaciones. Este también sería el caso si dicha parte modifica sustancialmente un sistema de IA de alto riesgo que ya se haya introducido en el mercado o puesto en servicio de tal manera que el sistema modificado siga siendo un sistema de IA de alto riesgo de conformidad con el presente Reglamento, o si modifica la finalidad prevista de un sistema de IA, como un sistema de IA de uso general, que ya se haya introducido en el mercado o puesto en servicio y que no esté clasificado como sistema de alto riesgo, de tal manera que el sistema modificado pase a ser un sistema de IA de alto riesgo de conformidad con el presente Reglamento. Esas disposiciones deben aplicarse sin perjuicio de las disposiciones más específicas establecidas en determinados actos legislativos de armonización de la Unión basados en el nuevo marco legislativo que se deben aplicar en conjunción con el presente Reglamento. Por ejemplo, el artículo 16, apartado 2, del Reglamento (UE) 2017/745, que establece que determinados cambios no deben considerarse modificaciones de un producto que puedan afectar al cumplimiento de los requisitos aplicables, debe seguir aplicándose a los sistemas de IA de alto riesgo que sean productos sanitarios en el sentido de dicho Reglamento.

(85) Los sistemas de IA de uso general pueden utilizarse como sistemas de IA de alto riesgo por sí solos o ser componentes de sistemas de IA de alto riesgo. Así pues, debido a su particular naturaleza y a fin de garantizar un reparto equitativo de responsabilidades a lo largo de toda la cadena de valor, los proveedores de tales sistemas, con independencia de que estos sistemas puedan ser utilizados como sistemas de IA de alto riesgo por sí solos por otros proveedores o como componentes de sistemas de IA de alto riesgo, y salvo que se disponga otra cosa en el presente Reglamento, deben cooperar estrechamente con los proveedores de los sistemas de IA de alto riesgo correspondientes para que estos puedan cumplir las obligaciones pertinentes en virtud del presente Reglamento, así como con las autoridades competentes establecidas en virtud del presente Reglamento.

operadore batek banatzaile-lanetan eta inportatzaile-lanetan jardun dezake aldi berean.

(84) Segurtasun juridikoa bermatzeko, argitu behar da, ezen, baldintza zehatz jakin batzuetan, edozein banatzaile, inportatzaile hedapenaren arduradun edo bestelako hirugarren bat hartu behar dela arrisku handiko AA-sistema baten hornitzailetzat, eta, beraz, bere gain hartu behar dituela bete beharreko betebeharrak guztiak. Halaxe gertatzen da, adibidez, pertsona horrek bere izena edo marka jartzen dioenean ordurako merkatuan jarrita edo zerbitzuan ipinita dagoen arrisku handiko AA-sistema bati, betebeharren beste banaketa bat ezartzen duten kontratu-akordioak gorabehera. Horixe bera gertatuko da, halaber, alderdi horrek funtsezko aldaketa bat egiten badu jada merkatuan jarrita edo zerbitzuan ipinita dagoen arrisku handiko AA-sistema batean eta aldaketaren ostean ere sistema horrek arrisku handiko AA-sistema izaten jarraitzen badu erregelamendu honen arabera; edo jada merkatuan jarrita edo zerbitzuan ipinita dagoen eta arrisku handiko sistematzat sailkatuta ez dagoen AA-sistema baten helburu aurreikusia aldatzen badu —erabilera orokorreko AA-sistemak ere barne hartuta— eta, aldaketa horren ondorioz, aldatutako sistema arrisku handiko AA-sistema bilakatzen bada erregelamendu honen arabera. Xedapen horiek aplikatzekoak dira hargatik eragotzi gabe erregelamendu honekin bat etorritako aplikatzekoak diren Batasunaren harmonizazioko lege-egintza jakin batzuetan, legeegintza-esparru berrian oinarrituta egonda, ezarritako xedapen zehatzagoak. Adibidez, (EB) 2017/745 Erregelamenduaren 16.2 artikulua —zeinak ezartzen baitu produktu baten aldaketa jakin batzuen kasuan ez dela jo behar aldaketa horiek eragina dutenik aplikatzekoak diren betekizunetan— aplikatzen jarraitu beharrekoa da erregelamendu horren arabera osasun-produktu diren arrisku handiko AA-sistemetan.

(85) Erabilera orokorreko AA-sistemak arrisku handiko AA-sistema modura erabil daitezke modu independentean, edo arrisku handiko AA-sistemen osagai izan. Hala, bada, sistema horien izaera berezia kontuan hartuta eta balio-kate osoan erantzukizunak ekitatez banatuko direla bermatzeko, sistema horien hornitzaileek —beste hornitzaile batzuek sistema horiek arrisku handiko AA-sistema modura erabiltzen dituztenean modu independentean, zein arrisku handiko AA-sistemen osagai modura erabiltzen direnean—, erregelamendu honetan bestelakorik ezartzen ez bada, buruz buru lan egin behar duite arrisku handiko AA-sistemen hornitzaileekin, azken horiek erregelamendu honen arabera bete beharreko betekizunak bete ahal izan ditzaten, eta eskuz esku lan egin beharko dute, halaber, erregelamendu honen arabera eskumenekoak diren agintaritzekin.



(86) Cuando, con arreglo a las condiciones establecidas en el presente Reglamento, el proveedor que introdujo inicialmente el sistema de IA en el mercado o lo puso en servicio ya no deba considerarse el proveedor a los efectos del presente Reglamento, y cuando dicho proveedor no haya excluido expresamente la transformación del sistema de IA en un sistema de IA de alto riesgo, el primer proveedor debe, no obstante, cooperar estrechamente, facilitar la información necesaria y proporcionar el acceso técnico u otra asistencia que quepa esperar razonablemente y que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo.

(87) Además, cuando un sistema de IA de alto riesgo que sea un componente de seguridad de un producto que entre dentro del ámbito de aplicación de un acto legislativo de armonización de la Unión basado en el nuevo marco legislativo no se introduzca en el mercado ni se ponga en servicio de forma independiente del producto, el fabricante del producto, tal como se define en el acto legislativo pertinente, debe cumplir las obligaciones que el presente Reglamento impone al proveedor y, en particular, debe garantizar que el sistema de IA integrado en el producto final cumpla los requisitos del presente Reglamento.

(88) A lo largo de la cadena de valor de la IA, numerosas partes suministran a menudo no solo sistemas, herramientas y servicios de IA, sino también componentes o procesos que el proveedor incorpora al sistema de IA con diversos objetivos, como el entrenamiento de modelos, el reentrenamiento de modelos, la prueba y evaluación de modelos, la integración en el software u otros aspectos del desarrollo de modelos. Dichas partes desempeñan un papel importante en la cadena de valor en relación con el proveedor del sistema de IA de alto riesgo en el que se integran sus sistemas, herramientas, servicios, componentes o procesos de IA, y deben proporcionar a dicho proveedor, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y demás asistencia que sean necesarios habida cuenta del estado actual de la técnica generalmente reconocido, a fin de que el proveedor pueda cumplir íntegramente las obligaciones establecidas en el presente Reglamento, sin comprometer sus propios derechos de propiedad intelectual e industrial o secretos comerciales.

(89) A los terceros que ponen a disposición del público herramientas, servicios, procesos o componentes de IA que no sean modelos de IA de uso general no se les debe imponer la obligación de cumplir los requisitos relativos a las responsabilidades a lo largo de la cadena de valor de la IA, en particular por lo que respecta al proveedor que haya utilizado o integrado dichas

(86) Erregelamendu honetan ezarritako baldintzen arabera hasieran AA-sistema merkatuan jarri edo zerbitzuan ipini zuen hornitzailea jada ez denean hornitzailetzat hartu behar erregelamendu honen ondorioetarako, eta hornitzaile horrek espresuki baztertu ez badu AA-sistema arrisku handiko AA-sistema bihurtzea, lehenengo hornitzaileak, hala ere, lankidetzan estuan jardun behar du, behar den informazioa eman eta sarbide teknikoa edo zentzuz espero izatekoa den bestelako laguntza eman, erregelamendu honetan ezarritako betebeharrak betetzeko beharrezkoa den heinean, bereziki arrisku handiko AA-sistemen adostasunaren ebaluazioa betetze aldera.

(87) Gainera, arrisku handiko AA-sistema bat, legegintza-esparru berrian oinarritutako Batasunaren harmonizazioko lege-egintza baten aplikazio-eremuari dagokion produktu baten segurtasun-osagai dena, ez denean merkatuan jartzen eta zerbitzuan ipintzen produktu horretatik bereiz, produktuaren fabrikatzaileak —dagokion lege-egintzan definitutako moduan— bete beharrekoak izango ditu erregelamendu honetan hornitzaileari ezartzen zaizkion betebeharrak, eta bereziki bermatu beharko du azken produktuan integratutako AA-sistemak erregelamendu honetako betekizunak betetzen dituela.

(88) AAren balio-katean barrena, alderdi ugariak maiz hornitzen dituzte, ez bakarrik AA-sistemak, -tresnak eta -zerbitzuak, bai, halaber, hornitzaileak AA-sisteman hainbat helbururekin txertatzen dituen osagaiak edo prozesuak ere —helburu horien artean direla ereduen entrenamendua, ereduen berentrenamendua, ereduen proba eta ebaluazioa, softwarean integratzeko prozesua edo ereduen garapenaren beste alderdi batzuk—. Alderdi horiek zeregin garrantzitsua betetzen dute balio-katean, beren AA-sistemak, -tresnak, -zerbitzuak, -osagaiak edo -prozesuak barne hartzen dituen arrisku handiko AA-sistemaren hornitzaileari dagokionez, eta hornitzaile horri, idatzizko akordio bidez, beharrezkoak diren informazioa, gaitasunak, sarbide teknikoa eta gainerako laguntza eman behar dizkiote, oro har aintzatetsitako teknikaren unean uneko egoera kontuan hartuta, hartara hornitzaileak erregelamendu honetan ezarritako betebeharrak osorik bete ahal izan ditzan, arriskuan jarri gabe jabetza intelektualaren eta industrialaren eskubideak edo merkataritza-sekretuak.

(89) Erabilera orokorreko AA-ereduak ez diren AA-tresnak, -zerbitzuak, -prozesuak edo -osagaiak herritarren eskura jartzen dituzten hirugarrenei ez zaie inoposatu behar AAren balio-katean barrena erantzukizunei buruzko betekizunak betetzeko betebeharra, bereziki AA-tresna, -zerbitzu, -prozesu edo -osagai horiek erabili edo integratu dituen hornitzaileari



herramientas, servicios, procesos o componentes de IA, cuando el acceso a dichas herramientas, servicios, procesos o componentes de IA esté sujeto a una licencia libre y de código abierto. No obstante, se debe animar a los desarrolladores de herramientas, servicios, procesos o componentes de IA libres y de código abierto que no sean modelos de IA de uso general a que apliquen prácticas de documentación ampliamente adoptadas, como tarjetas de modelo y hojas de datos, como una forma de acelerar el intercambio de información a lo largo de la cadena de valor de la IA, permitiendo la promoción en la Unión de sistemas de IA fiables.

(90) La Comisión podría elaborar y recomendar cláusulas contractuales tipo, de carácter voluntario, entre los proveedores de sistemas de IA de alto riesgo y los terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en los sistemas de IA de alto riesgo, a fin de facilitar la cooperación a lo largo de la cadena de valor. Cuando elabore estas cláusulas contractuales tipo de carácter voluntario, la Comisión también debe tener en cuenta los posibles requisitos contractuales aplicables en determinados sectores o modelos de negocio.

(91) Habida cuenta de las características de los sistemas de IA y de los riesgos que su uso lleva aparejado para la seguridad y los derechos fundamentales, también en lo que respecta a la necesidad de garantizar la correcta vigilancia del funcionamiento de un sistema de IA en un entorno real, conviene establecer las responsabilidades específicas de los responsables del despliegue. En particular, los responsables del despliegue deben adoptar las medidas técnicas y organizativas adecuadas para garantizar que utilizan los sistemas de IA de alto riesgo conforme a las instrucciones de uso. Además, es preciso definir otras obligaciones en relación con la vigilancia del funcionamiento de los sistemas de IA y la conservación de registros, según proceda. Asimismo, los responsables del despliegue deben garantizar que las personas encargadas de poner en práctica las instrucciones de uso y la supervisión humana establecidas en el presente Reglamento tengan las competencias necesarias, en particular un nivel adecuado de alfabetización, formación y autoridad en materia de IA para desempeñar adecuadamente dichas tareas. Dichas obligaciones deben entenderse sin perjuicio de otras obligaciones que tenga el responsable del despliegue en relación con los sistemas de IA de alto riesgo con arreglo al Derecho nacional o de la Unión.

(92) El presente Reglamento se entiende sin perjuicio de la obligación de los empleadores de informar o de informar y consultar a los trabajadores o a sus representantes, en virtud del Derecho o las prácticas

dagokionez, baldin eta AA-tresna, -zerbitzu, -prozesu edo -osagai horietarako sarbidea lizentzia libre eta kode ireki bati lotuta badago. Dena dela erabilera orokorreko AA-eredu ez diren AA libre eta kode irekikoetako tresnak, zerbitzuak, prozesuak edo osagaiak garatzen dituztenei bultzatzea egin behar zaie dokumentazioa zabaltzeko luze-zabal onartutako jardunbideak har ditzaten —hala nola eredu-txartelak edo datu-orriak— AAren balio-katean barrena informazio-trukea bizkortzeko eta, hartara, Batasunean AA-sistema fidagarriak sustatu ahal izateko.

(90) Batzordeak kontratueterako klausula-ereduak presta eta gomenda litzake, borondatezkoak, arrisku handiko AA-sistemen hornitzaileentzat eta arrisku handiko AA-sistemetan erabiltzen edo integratzen diren tresnak, zerbitzuak, osagaiak edo prozesuak hornitzen dituzten hirugarrenentzat, hartara balio-katean barrena lankidetzat errazteko. Kontratueterako borondatezko klausula-eredu horiek egiten dituenean, Batzordeak kontuan hartu behar ditu sektore edo negozio-eredu jakin batzuetan aplikatzekoak izan daitezkeen kontratu-betekizunak.

(91) Kontuan izanda bai AAKo-sistemen ezaugarriak, bai sistema horiek erabiltzeak segurtasunean eta oinarritzko eskubideetan dakartzan arriskuak —barnean hartuta, halaber, ingurune errealean AA-sistema baten funtzionamendua behar bezala zaintzen dela bermatzeko beharra—, komenigarria da hedapenaren arduradunen erantzukizun espezifikoak ezartzea. Zehatzago esateko, hedapenaren arduradunek alderdi teknikoak eta antolakuntzakoak kudeatzeko neurri egokiak hartu behar dituzte, arrisku handiko AA-sistemak erabilera-jarraibideen arabera erabiltzen direla bermatzeko. Horrez gain, beste betebeharrak batzuk ere zehaztu behar dira, AA-sistemen jardunbidea zaintzeko begira eta erregistroak gordetzeko begira, hala behar bada. Era berean, hedapenaren arduradunek bermea eman behar dute erregelamendu honetan ezarritako erabilera-jarraibideak erabiltzeko eta giza ikuskapena egiteko ardura dutenek behar diren konpetentziak izan ditzaten —AAren arloko alfabetatze-, prestakuntza- eta aginpide egokia, zehazki— eginkizun horiek egokiro bete ahal izateko. Betebeharrak horiek ez dituzte eragotziko hedapenaren arduradunak zuzenbide nazionalarekin edota Batasuneko zuzenbidearekin bat etorrita arrisku handiko AA-sistemen arloan dituen bestelako betekizunak.

(92) Erregelamendu honek ez du eragotziko enplegatzaileek langileei edo haien ordezkariak informazioa emateko edo informazioa eman eta kontsulta egiteko duten betebeharra, bat etorrita nazioko



nacionales o de la Unión, incluida la Directiva 2002/14/CE del Parlamento Europeo y del Consejo (39), sobre la decisión de poner en servicio o utilizar sistemas de IA. Se debe velar por que se informe a los trabajadores y a sus representantes sobre el despliegue previsto de sistemas de IA de alto riesgo en el lugar de trabajo incluso aunque no se cumplan las condiciones de las citadas obligaciones de información o de información y consulta previstas en otros instrumentos jurídicos. Además, este derecho de información es accesorio y necesario para el objetivo de protección de los derechos fundamentales que subyace al presente Reglamento. Por consiguiente, debe establecerse en el presente Reglamento un requisito de información a tal efecto, sin que dicho requisito afecte a ningún derecho vigente de los trabajadores.

(93) Aunque los riesgos relacionados con los sistemas de IA pueden derivarse de su diseño, también pueden derivarse riesgos del uso que se hace de ellos. Por ello, los responsables del despliegue de un sistema de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales, como complemento de las obligaciones del proveedor al desarrollar el sistema de IA. Los responsables del despliegue se encuentran en una posición óptima para comprender el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, detectar potenciales riesgos significativos que no se previeron en la fase de desarrollo, al tener un conocimiento más preciso del contexto de uso y de las personas o los colectivos de personas que probablemente se vean afectados, entre los que se incluyen colectivos vulnerables. Los responsables del despliegue de los sistemas de IA de alto riesgo que se enumeran en un anexo del presente Reglamento también desempeñan un papel fundamental a la hora de informar a las personas físicas y, cuando tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, deben, en su caso, informar a las personas físicas de que son objeto de la utilización de un sistema de IA de alto riesgo. Esta información debe incluir la finalidad prevista y el tipo de decisiones que se toman. El responsable del despliegue también debe informar a las personas físicas de su derecho a una explicación con arreglo al presente Reglamento. Por lo que respecta a los sistemas de IA de alto riesgo que se utilizan a efectos de la garantía del cumplimiento del Derecho, esa obligación debe ejecutarse de conformidad con el artículo 13 de la Directiva (UE) 2016/680.

(94) Todo tratamiento de datos biométricos que se produzca en el marco de la utilización de un sistema de IA para la identificación biométrica con fines de garantía del cumplimiento del Derecho debe cumplir lo dispuesto en el artículo 10 de la Directiva (UE) 2016/680, que permite dicho tratamiento solo cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas

edo Batasuneko zuzenbidearekin edo jardunbideekin, barnean dela Europako Parlamentuaren eta Kontseiluaren 2002/14/EE Zuzentaraua (39), AA-sistemak zerbitzuan ipintzeko edo erabiltzeko erabakia dela eta. Berariaz zaindu behar da langileei eta haien ordezkariari informazioa ematen zaiela lantokian arrisku handiko AA-sistemak ezartzea aurreikusten denean; eta, halaxe egin behar da, nahiz eta ez bete beste tresna juridiko batzuetan aurreikusitako informazioa emateko edo informazioa eman eta kontsulta egiteko betebeharren baldintzak. Informazio-eskubide hori, gainera, erregelamendu honen azpian dauden oinarritzko eskubideak babesteko helbururako osagarria eta beharrezkoa da. Horrenbestez, helburu horri begira, beharrezkoa da erregelamendu honetan informazio-betekizun bat ezartzea, betiere langileek indarrean dituzten eskubideei ez eragiteko moduan.

(93) AA-sistemekin lotutako arriskuak haien diseinutik etor daitezkeen arren, sistemen gainean egiten den erabilerak ere arriskuak eragin ditzake. Horregatik, arrisku handiko AA-sistema baten hedapenaren arduradunek funtsezko zeregina betetzen dute oinarritzko eskubideen babesa bermatzeko orduan, hornitzaileak AA-sistema garatzean dituen betebeharren osagarri gisa. Hedapenaren arduradunek kokaleku ezin hobe dute arrisku handiko AA-sistemari emango zaion erabilera zehatza ulertzeko; hala, garapen-fasean aurreikusi ez ziren arrisku potentzial esanguratsuak detekta ditzakete, ezagutza zehatzagoa dutelako erabilera-testuinguruaren gainean eta pertsona edo kolektibo ukiberen gainean (kolektibo kalteberak barne). Erregelamendu honen eranskin batean zerrendatzen diren arrisku handiko AA-sistemen hedapenaren arduradunek ere funtsezko zeregina dute pertsona fisikoei informazioa emateko orduan; hala, bada, pertsona fisikoei lotutako erabakiak hartzen dituztenean edo halako erabakiak hartzen laguntzen dutenean, pertsona fisikoei jakinarazi behar diete arrisku handiko AA-sistema bat erabiltzen ari direla. Informazio horrek helburu aurreikusia eta hartzen diren erabaki motak jaso behar ditu. Hedapenaren arduradunak, halaber, erregelamendu honen arabera azalpen bat jasotzeko eskubidea dutela jakinarazi behar die pertsona fisikoei. Zuzenbidea betearazteko erabiltzen diren arrisku handiko AA-sistemen kasuan, (EB) 2016/680 Zuzentarauaren 13. artikulua araberaz gauzatu behar da betebeharrak.

(94) Zuzenbidea betearazten dela bermatze aldera AA-sistema bat erabiltzen denean identifikazio biometrikoko egiteko, datu biometrikoren tratamendurako ezinbestekoa da (EB) 2016/680 Zuzentarauaren 10. artikuluan xedatutakoa betetzea; bada, artikulua horrek behar-beharrezkoa denean soilik baimentzen du halako tratamendua, interesdunaren eskubide eta askatasunak



para los derechos y libertades del interesado y cuando así lo autorice el Derecho de la Unión o de los Estados miembros. Dicho uso, cuando esté autorizado, también debe respetar los principios establecidos en el artículo 4, apartado 1, de la Directiva (UE) 2016/680, como, entre otros, que el tratamiento sea lícito y leal, la transparencia, la limitación de la finalidad, la exactitud y la limitación del plazo de conservación.

(95) Sin perjuicio del Derecho de la Unión aplicable, en particular el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680, teniendo en cuenta el carácter intrusivo de los sistemas de identificación biométrica remota en diferido, el uso de este tipo de sistemas debe estar sujeto a garantías. Los sistemas de identificación biométrica remota en diferido deben utilizarse siempre de manera proporcionada y legítima, en la medida de lo estrictamente necesario y, por ende, de forma selectiva por lo que respecta a las personas que deben identificarse, la ubicación y el alcance temporal y a partir de un conjunto limitado de datos de grabaciones de vídeo obtenidas legalmente. En cualquier caso, los sistemas de identificación biométrica remota en diferido no deben utilizarse en el marco de la garantía del cumplimiento del Derecho de tal forma que se produzca una vigilancia indiscriminada. Las condiciones para la identificación biométrica remota en diferido en ningún caso deben servir para eludir las condiciones de la prohibición y las estrictas excepciones aplicables a la identificación biométrica remota en tiempo real.

(96) A fin de garantizar eficazmente la protección de los derechos fundamentales, los responsables del despliegue de sistemas de IA de alto riesgo que sean organismos de Derecho público, o las entidades privadas que presten servicios públicos y los responsables del despliegue de determinados sistemas de IA de alto riesgo enumerados en un anexo del presente Reglamento, como las entidades bancarias o de seguros, deben llevar a cabo una evaluación de impacto relativa a los derechos fundamentales antes de su puesta en funcionamiento. Algunos servicios importantes para las personas que son de carácter público también pueden ser prestados por entidades privadas. Las entidades privadas que prestan estos servicios públicos se vinculan a funciones de interés público, por ejemplo, en el ámbito de la educación, la asistencia sanitaria, los servicios sociales, la vivienda y la administración de justicia. El objetivo de la evaluación de impacto relativa a los derechos fundamentales es que el responsable del despliegue determine los riesgos específicos para los derechos de las personas o colectivos de personas que probablemente se vean afectados y defina las medidas que deben adoptarse en caso de que se materialicen dichos riesgos. La evaluación de impacto debe llevarse a cabo antes del despliegue del sistema de IA de alto riesgo y debe actualizarse cuando el responsable del despliegue considere que alguno de los factores pertinentes ha

egokiro babestuta eta betiere Batasuneko edo estatu kideetako zuzenbideak hala baimentzen duenean. Erabilera horrek, baimenduta dagoenean, (EB) 2016/680 Zuzentarauaren 4.1 artikuluan ezarritako printzipioak ere errespetatu behar ditu: besteak beste, tratamendua zilegia eta leiala izatea, gardentasunez jokatzeta, xedea zedarritzeta, zehaztasuna izatea eta gordetzeko epea mugatzeta.

(95) Batasuneko zuzenbide aplikagarria alde batera utzi gabe —bereziki (EB) 2016/679 Erregelamendua eta (EB) 2016/680 Zuzentaraua—, kontuan hartuta gerora egiten den urruneko identifikazio biometrikoko sistemen izaera intrusiboa, halako sistemak erabiltzeko, berme batzuk eduki behar dira ezinbestean. Gerora egiten den urruneko identifikazio biometrikoko sistemak neurritz eta modu legítimoan erabili behar dira beti, behar-beharrezkoa denean baino ez eta, beraz, zorrotz mugatuta identifikatu behar diren pertsonak, kokapena eta denbora-tartea, eta, betiere, legez lortutako bideo-grabazioetako datu multzo mugatu bat abiaburu hartuta. Bestalde, gerora egiten den urruneko identifikazio biometrikoko sistemak ez dira zuzenbidea betearazteko testuinguruan erabili behar, baldin eta erabilera horrek bereizkuntzarik gabeko zaintza eskatzen badu. Gerora egiten den urruneko identifikazio biometrikorako baldintzek ez dute inolaz ere bide eman behar itzuri egiteko denbora errealean egiten den urruneko identifikazio biometrikorako debeku-baldintzei eta salbuespen zorrotzei.

(96) Oinarritzko eskubideak eraginkortasunez babesteko, arrisku handiko AA-sistemen hedapenaren arduradunek —zuzenbide publikoko organismoak direla, zerbitzu publikoak eskaintzen dituzten entitate pribatuak direla edo erregelamendu honen eranskin batean zerrendatutako arrisku handiko AA-sistema jakin batzuen hedapenaren arduradunak direla, hala nola banku- edo aseguru-entitateak—, sistemak oinarritzko eskubideetan dakarren inpaktuari buruzko ebaluazioa egin behar dute, abian jarri aurretik. Gerta liteke pertsonentzako garrantzitsuak diren izaera publikoko zerbitzu batzuk entitate pribatuek ematea. Zerbitzu publiko horiek ematen dituzten entitate pribatuak interes publikoko arlo hauetakoak izaten dira besteak beste: hezkuntza, osasun-laguntza, gizarte-zerbitzuak, etxebizitza eta justizia-administrazioa. Oinarritzko eskubideen gaineko inpaktuaren ebaluazioaren helburua da hedapenaren arduradunak zehaztea zer arrisku espezifiko dakartzkien sistemak pertsona edo kolektibo ukiberen eskubideei, eta zehaztea zer neurri hartu behar diren arrisku horiek gauzatzen badira. Arrisku handiko AA-sistema hedatu aurretik egin behar da inpaktuaren ebaluazioa, eta eguneratu egin behar da, hedapenaren arduradunak iritiz gero faktore esanguratsuren bat aldatu dela. Inpaktuaren ebaluazioak zehaztu behar du hedapenaren arduradunak zein prozesutan erabiliko duen arrisku handiko AA-sistema, helburu aurreikusiarekin bat etorritz, eta sistema zer denbora-



cambiado. La evaluación de impacto debe determinar los procesos pertinentes del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista y debe incluir una descripción del plazo de tiempo y la frecuencia en que se pretende utilizar el sistema, así como de las categorías concretas de personas físicas y de colectivos de personas que probablemente se vean afectados por el uso del sistema de IA de alto riesgo en ese contexto de uso específico. La evaluación también debe determinar los riesgos de perjuicio específicos que probablemente afecten a los derechos fundamentales de dichas personas o colectivos. Al llevar a cabo esta evaluación, el responsable del despliegue debe tener en cuenta la información pertinente para una evaluación adecuada del impacto, lo que incluye, por ejemplo, la información facilitada por el proveedor del sistema de IA de alto riesgo en las instrucciones de uso. A la luz de los riesgos detectados, los responsables del despliegue deben determinar las medidas que han de adoptarse en caso de que se materialicen dichos riesgos, entre las que se incluyen, por ejemplo, sistemas de gobernanza para ese contexto de uso específico, como los mecanismos de supervisión humana con arreglo a las instrucciones de uso, los procedimientos de tramitación de reclamaciones y de recurso, ya que podrían ser fundamentales para mitigar los riesgos para los derechos fundamentales en casos de uso concretos. Tras llevar a cabo dicha evaluación de impacto, el responsable del despliegue debe notificarlo a la autoridad de vigilancia del mercado pertinente. Cuando proceda, para recopilar la información pertinente necesaria para llevar a cabo la evaluación de impacto, los responsables del despliegue de un sistema de IA de alto riesgo, en particular cuando el sistema de IA se utilice en el sector público, pueden contar con la participación de las partes interesadas pertinentes, como, por ejemplo, los representantes de colectivos de personas que probablemente se vean afectados por el sistema de IA, expertos independientes u organizaciones de la sociedad civil, en la realización de dichas evaluaciones de impacto y en el diseño de las medidas que deben adoptarse en caso de materialización de los riesgos. La Oficina Europea de Inteligencia Artificial (en lo sucesivo, «Oficina de IA») debe elaborar un modelo de cuestionario con el fin de facilitar el cumplimiento y reducir la carga administrativa para los responsables del despliegue.

(97) El concepto de modelos de IA de uso general debe definirse claramente y diferenciarse del concepto de sistemas de IA con el fin de garantizar la seguridad jurídica. La definición debe basarse en las características funcionales esenciales de un modelo de IA de uso general, en particular la generalidad y la capacidad de realizar de manera competente una amplia variedad de tareas diferenciadas. Estos modelos suelen entrenarse usando grandes volúmenes de datos y a través de diversos

epetan eta zer maiztasunez erabili nahi den deskribatu behar du, bai eta erabilera-testuinguru espezifiko horretan arrisku handiko AA-sistema erabiltzeak pertsona fisikoen eta kolektibo ukiberen zer kategoriari eragingo dien zehazki. Ebaluazioak berariaz jaso behar ditu, halaber, pertsona edo kolektibo horien oinarritzko eskubideei eragiteko probabilitate handia duten kalte-arriskuak. Ebaluazio hori egitean, hedapenaren arduradunak kontuan izan behar du inpaktuari buruzko ebaluazio egokia egiteko zer informazio den egokia: besteak beste, arrisku handiko AA-sistemaren hornitzaileak erabilera-jarraibideetan emandako informazioa. Hedapenaren arduradunek, hautemandako arriskuei so, zehaztu behar dute zer neurri hartu behar diren arriskuak gauzatuz gero; hor dira, besteak beste, erabilera-testuinguru zehatz horretarako gobernantza-sistemak, hala nola erabilera-jarraibideen araberrako giza ikuskapeneko mekanismoak eta erreklamazioak eta errekurtsioak izapidetzeko prozedurak, funtsezkoak izan baitaitezke erabilera zehatzetako oinarritzko eskubideetarako arriskuak arintzeko. Inpaktuaren ebaluazio hori egin ostean, hedapenaren arduradunak merkatua zaintzeko dagokion agintaritzari jakinarazi behar dio. Hala dagokionean, inpaktuaren ebaluazioa egiteko beharrezkoa den informazioa biltzeko, bereziki AA-sistema sektore publikoan erabiltzeko denean, arrisku handiko AA-sistemaren hedapenaren arduradunekin batera, egoki diren alderdi interesdunek ere parte har dezakete —horien artean dira, besteak beste, AA-sistemaren eraginpeko pertsona-kolektibo ukiberen ordezkariak, aditu independenteak eta gizarte zibileko antolakundeak— inpaktuaren ebaluazio horiek egiten eta arriskuak gauzatuz gero hartu behar diren neurriak diseinatzen laguntzeko. Adimen Artifizialaren Europako Bulegoak (aurrerantzean, «AA-bulegoa») galdetegi-eredu bat landu behar du, errazago bete ahal izan dadin eta hedapenaren arduradunek administrazio-karga txikiagoa izan dezaten.

(97) Erabilera orokorreko AA-ereduen kontzeptua argi eta garbi zehaztu behar da eta AA-sistemen kontzeptutik bereizi, hartara segurtasun juridikoa bermatzeko. Definizioak erabilera orokorreko AA-eredu baten funtsezko ezaugarri funtzionalak hartu behar ditu oinarri: zehazki, zeregin desberdin ugari modu gaituan egiteko orokortasuna eta gaitasuna. Eredu horiek datu-bolumen handiak erabiliz entrenatzen dira, askotariko metodoak baliatuta, hala nola ikaskuntza autoikuskatua, ikuskatu



métodos, como el aprendizaje autosupervisado, no supervisado o por refuerzo. Los modelos de IA de uso general pueden introducirse en el mercado de diversas maneras, por ejemplo, a través de bibliotecas, interfaces de programación de aplicaciones (API), como descarga directa o como copia física. Estos modelos pueden modificarse o perfeccionarse y transformarse en nuevos modelos. Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen por sí mismos sistemas de IA. Los modelos de IA requieren que se les añadan otros componentes, como, por ejemplo, una interfaz de usuario, para convertirse en sistemas de IA. Los modelos de IA suelen estar integrados en los sistemas de IA y formar parte de dichos sistemas. El presente Reglamento establece normas específicas para los modelos de IA de uso general y para los modelos de IA de uso general que entrañan riesgos sistémicos, que deben aplicarse también cuando estos modelos estén integrados en un sistema de IA o formen parte de un sistema de IA. Debe entenderse que las obligaciones de los proveedores de modelos de IA de uso general deben aplicarse una vez que los modelos de IA de uso general se introduzcan en el mercado. Cuando el proveedor de un modelo de IA de uso general integre un modelo propio en un sistema de IA propio que se comercialice o ponga en servicio, se debe considerar que dicho modelo se ha introducido en el mercado y, por tanto, se deben seguir aplicando las obligaciones establecidas en el presente Reglamento en relación con los modelos, además de las establecidas en relación con los sistemas de IA. En cualquier caso, las obligaciones establecidas en relación con los modelos no deben aplicarse cuando un modelo propio se utilice en procesos puramente internos que no sean esenciales para suministrar un producto o un servicio a un tercero y los derechos de las personas físicas no se vean afectados. Teniendo en cuenta su potencial para causar efectos negativos importantes, los modelos de IA de uso general con riesgo sistémico deben estar siempre sujetos a las obligaciones pertinentes establecidas en el presente Reglamento. La definición no debe incluir los modelos de IA utilizados antes de su introducción en el mercado únicamente para actividades de investigación, desarrollo y creación de prototipos. Lo anterior se entiende sin perjuicio de la obligación de cumplir lo dispuesto en el presente Reglamento cuando, tras haber realizado dichas actividades, el modelo se introduzca en el mercado.

(98) Aunque la generalidad de un modelo también podría determinarse, entre otras cosas, mediante una serie de parámetros, debe considerarse que los modelos que tengan al menos mil millones de parámetros y se hayan entrenado con un gran volumen de datos utilizando la autosupervisión a escala presentan un grado significativo de generalidad y realizan de manera competente una amplia variedad de tareas diferenciadas.

(99) Los grandes modelos de IA generativa son un ejemplo típico de un modelo de IA de uso general, ya que permiten la generación flexible de contenidos, por

gabee eta errefortzu bidezkoa. Erabilera orokorreko AA-ereduak hainbat modutan jar daitezke merkatuan, hala nola liburutegien bidez, aplikazio-programaren interfazeen bidez (API), zuzeneko deskarga gisa zein kopia fisiko gisa. Eredu horiek aldatu edo hobetu egin daitezke, eta eredu berri bihurtu. AA-ereduak AA-sistemen funtsezko osagaiak diren arren, ez dute beren kabuz AA-sistema bat osatzen. AA-ereduei beste osagai batzuk gehitu behar zaizkie —hala nola erabiltzaile-interfaze bat— AA-sistema bihurtzeko. AA-ereduak AA-sistemetan txertatuta egoten dira eta sistema horien parte izaten dira. Erregelamendu honek arau zehatzak ezartzen ditu erabilera orokorreko AA-ereduetarako eta arrisku sistemikoak dakartzaten erabilera orokorreko AA-ereduetarako (ereduak AA-sistema batean txertatuta daudenean edo AA-sistema baten parte direnean ere aplikatzekoak dira arau horiek). Erabilera orokorreko AA-ereduen hornitzaileen betebeharrak erabilera orokorreko AA-ereduak merkatuan jarritakoan aplikatu behar dira. Erabilera orokorreko AA-eredu baten hornitzaileak eredu propio bat txertatzen duenean merkaturatutako edo zerbitzuan ipinitako AA-sistema propio batean, kontuan hartu behar da eredu hori merkatuan jarri dela eta, beraz, AA-sistemetakoko ezarritako betebeharrak betetzeaz gain, beharrezkoa dela erregelamendu honetan ereduetakoko ezarritako betebeharrak aplikatzen jarraitzea. Aitzitik, ereduetakoko ezarritako betebeharrak ez dira aplikatu behar eredu propio bat bete-beteko barne-prozesuetan erabiltzen denean, betiere prozesu horiek ez badira funtsezkoak hirugarren bati produktu edo zerbitzu bat emateko eta pertsona fisikoen eskubideak ukitzen ez badituzte. Arrisku sistemikoa dakarten erabilera orokorreko AA-ereduek, ondorio kaltegarri garrantzitsuak eragiteko nolako ahalmena duten kontuan hartuta, erregelamendu honetan ezarritako betebeharrak bete behar dituzte beti. Definizioak ez ditu barne hartu behar merkatuan jarri aurretik ikerketarako, garapenerako eta prototipoak sortzeko jardueretarako soilik erabiltzen diren AA-ereduak; nolanahi ere, horrek ez du eragotziko erregelamendu honetan xedatutakoa bete behar izatea jarduera horiek egin ondoren eredu merkatuan jartzen denean.

(98) Eredu baten orokortasuna, besteak beste, zenbait parametroren bidez ere zehaztu badaiteke ere, kontuan hartu behar da ezen gutxienez mila milioi parametro dituzten eta eskalako autoikuskapena erabiliz datu-bolumen handiarekin entrenatu diren ereduak orokortasun-maila nabarmena dutela eta modu gaituan egiten dituztela zeregin berezitu ugari.

(99) AA-eredu sortzaile handiak erabilera orokorreko AA-ereduen adibide tipikoa dira; izan ere, edukiak malgutasunez sortzeko aukera ematen dute, adibidez,



ejemplo, en formato de texto, audio, imágenes o vídeo, que pueden adaptarse fácilmente a una amplia gama de tareas diferenciadas.

(100) Cuando un modelo de IA de uso general esté integrado en un sistema de IA o forme parte de él, este sistema debe considerarse un sistema de IA de uso general cuando, debido a esta integración, el sistema tenga la capacidad de servir a diversos fines. Un sistema de IA de uso general puede utilizarse directamente e integrarse en otros sistemas de IA.

(101) Los proveedores de modelos de IA de uso general tienen una función y una responsabilidad particulares a lo largo de la cadena de valor de la IA, ya que los modelos que suministran pueden constituir la base de diversos sistemas de etapas posteriores, que a menudo son suministrados por proveedores posteriores que necesitan entender bien los modelos y sus capacidades, tanto para permitir la integración de dichos modelos en sus productos como para cumplir sus obligaciones en virtud del presente Reglamento o de otros reglamentos. Por consiguiente, deben establecerse medidas de transparencia proporcionadas, lo que incluye elaborar documentación y mantenerla actualizada y facilitar información sobre el modelo de IA de uso general para su uso por parte de los proveedores posteriores. El proveedor del modelo de IA de uso general debe elaborar y mantener actualizada la documentación técnica con el fin de ponerla a disposición, previa solicitud, de la Oficina de IA y de las autoridades nacionales competentes. Los elementos mínimos que debe contener dicha documentación deben establecerse en anexos específicos del presente Reglamento. La Comisión debe estar facultada para modificar dichos anexos mediante actos delegados en función de los avances tecnológicos.

(102) El software y los datos, incluidos los modelos, divulgados con arreglo a una licencia libre y de código abierto que permita compartirlos abiertamente y que los usuarios puedan acceder a ellos, o a versiones modificadas de dicho software y dichos datos, o utilizarlos, modificarlos y redistribuirlos libremente, pueden contribuir a la investigación y la innovación en el mercado y pueden ofrecer importantes oportunidades de crecimiento para la economía de la Unión. Debe considerarse que los modelos de IA de uso general divulgados con arreglo a una licencia libre y de código abierto garantizan altos niveles de transparencia y apertura si sus parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se ponen a disposición del público. La licencia debe considerarse libre y de código abierto cuando permita a los usuarios ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software y los datos, incluidos los modelos a condición de que se cite al proveedor original del

testu-, audio-, irudi- edo bideo-formatuan, eta eduki horiek erraz egokitu daitezke ataza bereizi askotara.

(100) Erabilera orokorreko AA-eredu bat AA-sistema batean integratuta dagoenean edo haren parte denean, sistema hori erabilera orokorreko AA-sistematzat hartu behar da integrazio horren ondorioz sistemak gaitasuna duenean zenbait helburutarako balio izateko. Erabilera orokorreko AA-sistema bat zuzenean erabil daiteke, edo beste AA-sistema batzuetan integratuta.

(101) Erabilera orokorreko AA-ereduen hornitzaileek eginkizun eta erantzukizun zehatzak dituzte AAren balio-katean barrena; izan ere, hornitzen dituzten ereduak oinarritzat erabil daitezke ondorengo etapetan sistemak eratzeko, eta sistema horiek, askotan, ondorengo hornitzaileek hornitzen dituzte, eta hornitzaile horiek egokiro ulertu behar dituzte ereduak eta haien gaitasunak, hala eredu horiek beren produktuetan integratu ahal izateko, nola erregelamendu honen edo beste erregelamendu batzuen arabera dituzten betebeharrak bete ahal izateko. Horrenbestez, gardentasun-neurri proportzionatuak ezarri behar dira, barruan direla dokumentazioa eratzea eta eguneratuta izatea eta erabilera orokorreko AA-ereduaren gaineko informazioa ematea, ondorengo hornitzaileek erabili ahal izateko. Erabilera orokorreko AA-ereduaren hornitzaileak dokumentazio teknikoak eratu eta eguneratuta mantendu behar du, AA-bulegoaren eta agintaritzaren nazional eskudunen eskura jartzeko, haiek aurrez hala eskatuta. Erregelamendu honen eranskin espezifikotik ezarri behar da zein diren dokumentazio horrek gutxienez eduki beharreko elementuak. Batzordeak ahalmena izan behar du eranskin horiek egintza eskuordetuen bidez aldatzeko, aurrerapen teknologikoei erantzuteko.

(102) Softwarea eta datuak —ereduak barne— lizentzia libre eta kode irekiarekin jendarteratzen direnean eta, beraz, aukera ematen dutenean askatasunez partekatzeko eta erabiltzaileek haietara edo haien bertsio moldatuetara sarbidea izateko eta askatasunez erabili, moldatu eta birbanatzeko, lagungarriak izan daitezke ikerketaren eta merkatutako berrikuntzaren arloetarako, eta hazkuntza-aukera bikaina eskain dezakete Batasunaren ekonomiarako. Lizentzia librez eta kode irekiarekin jendarteratutako erabilera orokorreko AA-ereduek gardentasun- eta irekitasun-maila handiak bermatzen dituzte, baldin eta herritarren eskura jartzen badira haien parametroak —pisuak, ereduaren arkitekturari buruzko informazioa eta ereduaren erabilari buruzko informazioa barne—. Lizentzia libretzat eta kode irekikotzat jotzen da, baldin eta aukera ematen badie erabiltzaileei softwarea eta datuak egikaritzeko, kopiatzeko, banatzeko, aztertzeko, aldatzeko eta hobetzeko —ereduak ere bai, ereduaren jatorriko hornitzailea nor den aipatuz gero—, betiere



modelo, si se respetan unas condiciones de distribución idénticas o comparables.

(103) Los componentes de IA libres y de código abierto comprenden el software y los datos, incluidos los modelos y los modelos de IA de uso general, las herramientas, los servicios y los procesos de un sistema de IA. Los componentes de IA libres y de código abierto pueden suministrarse a través de diferentes canales, lo que incluye la posibilidad de desarrollarlos en repositorios abiertos. A los efectos del presente Reglamento, los componentes de IA que se suministren a cambio de una contraprestación o que se monetizen de cualquier otro modo, como, por ejemplo, mediante la prestación de apoyo técnico u otros servicios en relación con el componente de IA, ya sea a través de una plataforma de software o por otros medios, o mediante el uso de datos personales con fines que no se refieran exclusivamente a la mejora de la seguridad, la compatibilidad o la interoperabilidad del software, salvo si se trata de operaciones entre microempresas, no deben poder acogerse a las excepciones previstas para los componentes de IA libres y de código abierto. La disponibilidad de un componente de IA a través de repositorios abiertos no debe constituir, de por sí, una monetización.

(104) Los proveedores de modelos de IA de uso general divulgados con arreglo a una licencia libre y de código abierto cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se ponen a disposición del público deben estar sujetos a excepciones por lo que respecta a los requisitos de transparencia que se imponen a los modelos de IA de uso general, a menos que pueda considerarse que presentan un riesgo sistémico, en cuyo caso la circunstancia de que el modelo sea transparente y vaya acompañado de una licencia de código abierto no debe considerarse una razón suficiente para que quede exento del cumplimiento de las obligaciones establecidas en el presente Reglamento. En cualquier caso, dado que la divulgación de modelos de IA de uso general con arreglo a una licencia libre y de código abierto no necesariamente revela información sustancial sobre el conjunto de datos utilizado para entrenar el modelo o realizar ajustes en relación con este ni sobre la manera en que se garantizó el cumplimiento del Derecho en materia de derechos de autor, la excepción prevista para los modelos de IA de uso general en relación con el cumplimiento de los requisitos de transparencia no debe eximir de la obligación de presentar un resumen del contenido utilizado para el entrenamiento del modelo ni de la obligación de adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor, en particular para identificar y respetar la reserva de derechos prevista en el artículo 4, apartado 3, de la

bermatuta banaketa-baldintzak lehengo berdina edo haien parekoak izango direla.

(103) AA-osagai libre eta kode irekikoak softwareaz eta datuez osatuta daude, barnean direla AA-sistemen ereduak eta erabilera orokorreko AA-ereduak, tresnak, zerbitzuak eta prozesuak. AA-osagai libre eta kode irekikoak kanal batetik baino gehiagotik hornitu daitezke, eta, hala, osagai horiek gordailu irekietan garatzeko aukera ere badago. Erregelamendu honen ondorioetarako, AA-osagaiak kontraprestazio baten truke hornitzen direnean edo beste edozein modutan monetizatzen direnean —hala nola AA-osagaiei lotutako laguntza tekniko edo beste zerbitzu batzuk emanez—, dela software-plataforma baten edo beste bitarteko batzuen bidez, dela datu pertsonalak softwarearen segurtasuna, bateragarritasuna edo elkarreragingarritasuna hobetzeaz bestelako helburu batzuetarako ere erabiliz, ezin izango dira bildu AA-osagai libre eta kode irekikoetarako aurreikusitako salbuespenetara, non eta ez diren mikroenpresen arteko eragiketak. AA-osagai bat gordailu irekien bidez eskura jartzeak ez du, berez, monetizaziorik ekarri behar.

(104) Lizentzia libre eta kode irekiko batekin jendarteratutako erabilera orokorreko AA-ereduen hornitzaileei, haien parametroak (hala nola pisuak, ereduaren arkitekturari buruzko informazioa eta ereduaren erabilerari buruzko informazioa) herritarren eskura jartzen diren heinean, salbuespenak jarri behar zaizkie erabilera orokorreko AA-ereduei ezartzen zaizkien gardentasun-betekizunetan. Alabaina, ez zaie salbuespenik aplikatuko arrisku sistemikoa dakartela jotzen bada; izan ere, kasu horretan, eredia gardena izatea eta kode irekiko lizentzia bat izatea ez da arrazoi nahikotzat hartu behar erregelamendu honetan ezarritako betebeharrak betetzetik salbuetsita geratzeko. Zernahi gisaz, erabilera orokorreko AA-ereduak lizentzia libre eta kode ireki baten arabera jendarteratzeak ez duenez nahitaez funtsezko informaziorik ematen eredia entrenatzeko edo harekin lotutako doikuntzak egiteko erabilitako datu multzoari buruz, ez eta egile-eskubideen arloko zuzenbidea bete dela bermatzeko erabilitako moduari buruz ere, gardentasun-betekizunak betetzeari dagokionez erabilera orokorreko AA-ereduetarako aurreikusitako salbuespenak ez du salbuetsi behar eredia entrenatzeko erabilitako edukiaren laburpen bat aurkezteko betebeharretik, ez eta egile-eskubideen arloan Batasuneko zuzenbidea betetzeko gidalerroak hartzeko betebeharretik ere, bereziki Europako Parlamentuaren eta Kontseiluaren (EB) 2019/790 Zuzentarauaren 4.3 artikuluan (40) aurreikusitako eskubide-erreserba identifikatzeko eta errespetatzeko.



Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo (40).

(105) Los modelos de IA de uso general, en particular los grandes modelos de IA generativos, capaces de generar texto, imágenes y otros contenidos, presentan unas oportunidades de innovación únicas, pero también representan un desafío para los artistas, autores y demás creadores y para la manera en que se crea, distribuye, utiliza y consume su contenido creativo. El desarrollo y el entrenamiento de estos modelos requiere acceder a grandes cantidades de texto, imágenes, vídeos y otros datos. Las técnicas de prospección de textos y datos pueden utilizarse ampliamente en este contexto para la recuperación y el análisis de tales contenidos, que pueden estar protegidos por derechos de autor y derechos afines. Todo uso de contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos de que se trate, salvo que se apliquen las excepciones y limitaciones pertinentes en materia de derechos de autor. La Directiva (UE) 2019/790 introdujo excepciones y limitaciones que permiten reproducciones y extracciones de obras y otras prestaciones con fines de prospección de textos y datos en determinadas circunstancias. Con arreglo a estas normas, los titulares de derechos pueden optar por reservarse sus derechos en relación con sus obras u otras prestaciones para evitar la prospección de textos y datos, salvo que su finalidad sea la investigación científica. Cuando el titular del derecho se haya reservado de manera adecuada el derecho de exclusión, los proveedores de modelos de IA de uso general deben obtener su autorización para llevar a cabo una prospección de textos y datos con dichas obras.

(106) Los proveedores que introduzcan modelos de IA de uso general en el mercado de la Unión deben garantizar el cumplimiento de las obligaciones pertinentes establecidas en el presente Reglamento. A tal fin, los proveedores de modelos de IA de uso general deben adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para detectar y cumplir la reserva de derechos expresada por los titulares de derechos con arreglo al artículo 4, apartado 3, de la Directiva (UE) 2019/790. Todo proveedor que introduzca un modelo de IA de uso general en el mercado de la Unión debe cumplir esta obligación, independientemente de la jurisdicción en la que tengan lugar los actos pertinentes en materia de derechos de autor que sustentan el entrenamiento de dichos modelos de IA de uso general. Esta medida es necesaria para garantizar unas condiciones de competencia equitativas entre los proveedores de modelos de IA de uso general que impidan que un proveedor obtenga una ventaja competitiva en el mercado de la Unión aplicando normas en materia de

(105) Erabilera orokorreko AA-ereduek, bereziki AA-eredu sortzaile handiek, testuak, irudiak eta bestelako edukiak sortzeko gai diren heinean, berrikuntzarako aukera paregabeak dituzte, baina, aldi berean, erronka egiten diete artistei, autoreei eta beste sortzaile guztiei, baita haien sorkuntzak eratzeko, zabaltzeko, erabiltzeko eta kontsumitzeko moduei ere. Eredu horiek garatzeko eta entrenatzeko, material asko eta asko behar da: testuak, irudiak, bideoak eta bestelako datuak. Testuak eta datuak aztertzeko teknikak luze-zabal erabil daitezke testuinguru honetan eduki horiek berreskuratzeko eta aztertzeko; eduki horiek, baina, babestuta egon daitezke egile-eskubideen bidez edo antzeko beste eskubide batzuen bidez. Egile-eskubideen bidez babestutako edukiak erabiltzeko, eskubide horien titularraren baimena behar da nahitaez, salbu eta egile-eskubideen arloko salbuespenak eta mugak aplikatzekoak badira. (EB) 2019/790 Zuzentarauak salbuespenak eta mugak ezarri zituen obrak erreproduzitu edo erauzi ahal izateko eta beste prestazio batzuetarako, egoera jakinetan testuen eta datuen prospekzioa egite aldera. Arau horiekin bat etorrita, eskubideen titularrek aukera dute obren edo bestelako prestazioen gainean dituzten eskubideak gordetzeko, testuen eta datuen prospekziarik egin ez dadin, salbu eta helburua ikerketa zientifikoa bada. Eskubidearen titularrak egokiro gorde badu eskusio-eskubidea, erabilera orokorreko AA-ereduen hornitzaileek haren baimena lortu beharko dute haren obretako testuen eta datuen prospekzioa egiteko.

(106) Batasuneko merkatuan erabilera orokorreko AA-ereduak jartzen dituzten hornitzaileek berariaz bermatu behar dute erregelamendu honetan ezarritako betebeharrak betetzen direla. Horretarako, erabilera orokorreko AA-ereduen hornitzaileek egoki diren gidalerroak onartu behar dituzte, egile-eskubideen eta antzeko eskubideen arloan Batasuneko zuzenbidea betetzeko, bereziki eskubideen titularrek adierazitako eskubide-erreserba detektatzeko eta betetzeko bat etorrita (EB) 2019/790 Zuzentarauaren 4.3 artikuluaekin. Batasuneko merkatuan erabilera orokorreko AA-eredu bat jartzen duten hornitzaile guztiek bete behar dute betebeharrak hori, edozein jurisdikziotan gertatzen direla ere erabilera orokorreko AA-eredu horien entrenamenduaren oinarri diren egile-eskubideen arloko egintzak. Neurri hori beharrezkoa da erabilera orokorreko AA-ereduen hornitzaileen artean lehia-baldintza ekitatiboak bermatzeko, baldintza horien bidez saihestu ahal izateko hornitzaile batek lehia-abantailak izatea egile-eskubideen arloan Batasunean



derechos de autor menos estrictas que las establecidas en la Unión.

(107) Con el fin de aumentar la transparencia en relación con los datos utilizados en el entrenamiento previo y el entrenamiento de los modelos de IA de uso general, incluidos los textos y los datos protegidos por el Derecho en materia de derechos de autor, procede que los proveedores de dichos modelos elaboren y pongan a disposición del público un resumen suficientemente detallado de los contenidos utilizados para el entrenamiento del modelo de IA de uso general. Este resumen debe tener debidamente en cuenta la necesidad de proteger los secretos comerciales y la información empresarial confidencial y, al mismo tiempo, debe ser exhaustivo en general en su alcance en vez de técnicamente detallado, a fin de facilitar que las partes con intereses legítimos, incluidos los titulares de derechos de autor, ejerzan y hagan cumplir sus derechos en virtud del Derecho de la Unión, por ejemplo, enumerando los principales conjuntos o recopilaciones de datos que hayan servido para entrenar al modelo, como los grandes archivos de datos o bases de datos privados o públicos, y proporcionando una explicación descriptiva sobre otras fuentes de datos utilizadas. Conviene que la Oficina de IA proporcione un modelo para el resumen, que debe ser sencillo y eficaz y permitir que el proveedor proporcione el resumen requerido en forma descriptiva.

(108) Por lo que se refiere a las obligaciones impuestas a los proveedores de modelos de IA de uso general de adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y de poner a disposición del público un resumen de los contenidos utilizados para el entrenamiento, la Oficina de IA debe supervisar si el proveedor ha cumplido dichas obligaciones sin verificar ni proceder a una evaluación obra por obra de los datos de entrenamiento en cuanto al respeto de los derechos de autor. El presente Reglamento no afecta al cumplimiento de las normas en materia de derechos de autor previstas en el Derecho de la Unión.

(109) El cumplimiento de las obligaciones aplicables a los proveedores de modelos de IA de uso general debe ser proporcionado y adecuado al tipo de proveedor de modelos. Debe eximirse de la obligación de cumplimiento a las personas que desarrollan o utilizan modelos con fines no profesionales o de investigación científica. No obstante, debe animarse a estas personas a cumplir voluntariamente estos requisitos. Sin perjuicio del Derecho de la Unión en materia de derechos de autor, el cumplimiento de esas obligaciones debe tener debidamente en cuenta el tamaño del proveedor y permitir formas simplificadas de cumplimiento para las pymes, incluidas las empresas emergentes, que no deben suponer un coste excesivo ni desincentivar el uso

bezain zorrotzak ez diren arauak aplikatzen dituelako Batasuneko merkatuan.

(107) Erabilera orokorreko AA-ereduen aurre-entrenamenduan eta entrenamenduan erabilitako datuen gaineko gardentasuna areagotzeko — zuzenbideak egile-eskubideen arloan babestutako testuak eta datuak barne—, egokia da eredu horien hornitzaileek behar bezain laburpen zehatza egitea erabilera orokorreko AA-eredua entrenatzeko erabilitako edukien gainean, eta herritarren eskura jartzea laburpen hori. Laburpen horrek zorrotz hartu behar du kontuan merkataritza-sekretuak eta enpresa-informazio konfidentziala babesteko beharra, eta, aldi berean, sakona izan behar du irismenari begira, teknikoki hain xehatua izan beharrean, hartara interes legítimoak dituzten alderdiek, egile-eskubideen titularrak barne, beren eskubideak Batasuneko zuzenbidearen arabera egikaritu eta betearazi ahal izan ditzaten; horretarako, adibidez, ereduaren entrenatzeko balio izan duten datuen multzo edo bilduma nagusiak zerrendatuko dira —hala nola datu-fitxategi handiak edo datu-base pribatu edo publikoak—, eta erabilitako beste datu-iturri batzuei buruzko azalpen deskribatzailea emango da. Komeni da, batetik, AA-bulegoak laburpenerako eredu bat eratzea —eredu erraz eta eraginkor bat— eta, bestetik, hornitzaileak laburpena modu deskribatzailean ematea.

(108) Bai egile-eskubideen arloan Batasuneko zuzenbidea betetzeko gidalerroak onartzeko erabilera orokorreko AA-ereduen hornitzaileei ezarritako betebeharrari dagokienez, bai, halaber, entrenamendurako erabilitako edukien laburpena herritarren eskura jartzeko betebeharrari dagokionez, AA-bulegoaren ardura da ikuskatzea ea hornitzaileak betebeharrari bete dituen entrenamendu-datuak obra obra egiaztatu gabe eta ebaluatu gabe egile-eskubideak errespetatzeari dagokionez. Erregelamendu honek ez dio eragiten Batasuneko zuzenbidean egile-eskubideen arloan aurreikusitako arauak betetzeko beharrari.

(109) Erabilera orokorreko AA-ereduen hornitzailea zer motakoa den, haren neurrikoak eta hari egokituak izan behar dute hari dagozkion betebeharrak. Salbuespen modura, ereduak helburu ez-profesionalekin edo ikerketa zientifikorako garatzen edo erabiltzen dituzten pertsonak ez dituzte betekizun horiek bete beharko. Bultzatzen da behar bezala, nolabait ere, betekizunak beren borondatez bete ditzaten. Batasuneko zuzenbideak egile-eskubideen arloan xedatutakoa alde batera utzi gabe, betebeharrari bete behar duen prozedura, behar bezala hartu behar da kontuan hornitzailearen tamaina, eta betetze modu sinplifikatuak onartu ETEentzat —enpresa emergenteak ere barne—, ez dezaten gehiegizko kosturik eragin, ezta



de dichos modelos. En caso de que se modifique o ajuste un modelo, las obligaciones de los proveedores de modelos de IA de uso general deben limitarse a esa modificación o esos ajustes, por ejemplo, complementando la documentación técnica ya existente con información sobre las modificaciones, incluidas las nuevas fuentes de datos de entrenamiento, para cumplir las obligaciones relacionadas con la cadena de valor establecidas en el presente Reglamento.

(110) Los modelos de IA de uso general pueden plantear riesgos sistémicos, por ejemplo, cualquier efecto negativo real o razonablemente previsible en relación con accidentes graves, perturbaciones de sectores críticos y consecuencias graves para la salud y la seguridad públicas, cualquier efecto negativo real o razonablemente previsible sobre los procesos democráticos y la seguridad pública y económica o la difusión de contenidos ilícitos, falsos o discriminatorios. Debe entenderse que los riesgos sistémicos aumentan con las capacidades y el alcance de los modelos, pueden surgir durante todo el ciclo de vida del modelo y se ven influidos por las condiciones de uso indebido, la fiabilidad del modelo, la equidad y la seguridad del modelo, el nivel de autonomía del modelo, su acceso a herramientas, modalidades novedosas o combinadas, las estrategias de divulgación y distribución, la posibilidad de eliminar las salvaguardias y otros factores. En particular, los enfoques internacionales han establecido hasta la fecha la necesidad de prestar atención a los riesgos derivados de posibles usos indebidos intencionados o de problemas en materia de control relacionados con la armonización con la intención humana no deseados, a los riesgos químicos, biológicos, radiológicos y nucleares, como las maneras en que las barreras a la entrada pueden reducirse, también para el desarrollo, el diseño, la adquisición o el uso de armas, a las cibercapacidades ofensivas, como las maneras en que pueden propiciarse el descubrimiento, la explotación o el uso operativo de vulnerabilidades, a los efectos de la interacción y el uso de herramientas, incluida, por ejemplo, la capacidad de controlar sistemas físicos e interferir en el funcionamiento de infraestructuras críticas, a los riesgos derivados del hecho que los modelos hagan copias de sí mismos o se «autorrepliquen» o entrenen a otros modelos, a las maneras en que los modelos pueden dar lugar a sesgos dañinos y discriminación que entrañan riesgos para las personas, las comunidades o las sociedades, a la facilitación de la desinformación o el menoscabo de la intimidad, que suponen una amenaza para los valores democráticos y los derechos humanos, al riesgo de que un acontecimiento concreto dé lugar a una reacción en cadena con efectos negativos considerables que podrían afectar incluso a una ciudad entera, un ámbito de actividad entero o una comunidad entera.

eredu horiek erabiltzeko adoregabatu. Ereduek aldatuz edo doitu gero, aldaketa edo doikuntza horretara mugatu behar dira erabilera orokorreko AA-ereduen hornitzaileen betebeharrak: esaterako, ordura arte aldaketen gainean jasotako dokumentazio tekniko osatuko da, entrenamendu-datuak iturri berriak ere jasota, erregelamendu honetan balio-katearekin lotutako betebeharrak betetzeko.

(110) Erabilera orokorreko AA-ereduek arrisku sistemikoak eragin ditzakete. Hor dira, besteak beste, benetakoak edo arrazoiz aurreikusgarriak diren ondorio kaltegarriak, askotariko arrazoiei lotuta, hala nola istripu larriak, sektore kritikoen nahasmenduak eta osasun eta segurtasun publikorako ondorio larriak; baita benetakoak edo arrazoiz aurreikusgarriak diren ondorio kaltegarriak —prozesu demokratikoen eta segurtasun publiko eta ekonomikoren gainekoak— eta eduki ez-zilegi, faltsu edo diskriminatzaileen zabalkundea ere. Arrisku sistemikoak areagotu egiten dira ereduen gaitasunak eta irismena areagotu ahala. Arriskuak ereduen bizi-ziklo osoan sor daitezke, eta hainbat faktoreren mende daude: behar ez bezalako erabilerak, ereduen fidagarritasuna, ereduen ekitatea eta segurtasuna, ereduen autonomia-maila, tresnetarako irisgarritasuna, modalitate berritzaileak edo konbinatuak, dibulgazio- eta banaketa-estrategiak, babesak ezabatzeko aukerak eta beste faktore batzuk. Hauek dira, zehazki, nazioarteko ikuspegiak orain arte nabarmendu dituzten arretaguneak: nahita egindako erabilera bidegabeak dakartzaten arriskuak edo giza asmoekiko harmonizazioarekin lotuta nahi gabe sortutako kontrol-arazoak dakartzaten arriskuak; arrisku kimiko, biologiko, erradiologiko eta nuklearrak, hala nola sarbide-oztopoak murrizteko moduak, baita armak garatzeko, diseinatzeko, eskuratzeko edo erabiltzeko arloan ere; erasorako zibergaitasunak, hala nola kalteberatasunak aurkitzeko, ustiatzeko edo baliatzeko bideak sustatzeko moduak; interakzioaren eta tresnen erabileraren eraginak, barruan dela, esaterako, sistema fisikoak kontrolatzeko gaitasuna eta azpiegitura kritikoen funtzionamenduan esku hartzeko gaitasuna; ereduek beren buruen kopiak edo «autorreplikak» egiteak edo ereduek beste eredu batzuk entrenatzeak dakartzan arriskuak; ereduek alborapen kaltegarriak eta diskriminazioa sor ditzaketen moduak, arriskutsuak izan daitezkeen heinean pertsonentzat, komunitateentzat edo gizarteentzat; desinformazioaren zabalkundea edo intimitatearen urraketa, mehatxu diren heinean balio demokratikoetarako eta giza eskubideetarako; gertaera jakin batek kate-erreakzio bat eragiteko arriskua, erreakzio horrek ondorio kaltegarri nabarmenak sor ditzakeenean eta hiri oso batean edo jarduera-arlo oso batean edo komunitate oso batean ere eragin.



(111) Conviene establecer una metodología para la clasificación de los modelos de IA de uso general como modelos de IA de uso general con riesgos sistémicos. Dado que los riesgos sistémicos se derivan de capacidades especialmente elevadas, debe considerarse que un modelo de IA de uso general presenta riesgos sistémicos si tiene capacidades de gran impacto —evaluadas mediante herramientas y metodologías técnicas adecuadas— o unas repercusiones considerables en el mercado interior debido a su alcance. Las capacidades de gran impacto en modelos de IA de uso general son capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados. La introducción en el mercado de un modelo o las interacciones de los responsables del despliegue con él permiten comprender mejor el conjunto de sus capacidades. Según el estado de la técnica en el momento de la entrada en vigor del presente Reglamento, la cantidad acumulada de cálculo utilizado para el entrenamiento del modelo de IA de uso general, medida en operaciones de coma flotante, es una de las aproximaciones pertinentes para las capacidades del modelo. La cantidad acumulada de cálculo utilizado para el entrenamiento incluye los cálculos utilizados en las distintas actividades y métodos destinados a mejorar las capacidades del modelo antes del despliegue, como el entrenamiento previo, la generación de datos sintéticos y la realización de ajustes. Por lo tanto, debe establecerse un umbral inicial de operaciones de coma flotante que, de ser alcanzado por un modelo de IA de uso general, dé lugar a la presunción de que el modelo es un modelo de IA de uso general con riesgos sistémicos. Este umbral deberá irse ajustando para reflejar los cambios tecnológicos e industriales, como las mejoras algorítmicas o el aumento de la eficiencia del hardware, y debe complementarse con parámetros de referencia e indicadores de la capacidad de los modelos. Para fundamentar esto, la Oficina de IA debe colaborar con la comunidad científica, la industria, la sociedad civil y otros expertos. Los umbrales, así como las herramientas y los parámetros de referencia para la evaluación de las capacidades de gran impacto, deben servir para predecir con fiabilidad la generalidad, las capacidades y el riesgo sistémico asociado de los modelos de IA de uso general, y podrían tener en cuenta la manera en que el modelo se introducirá en el mercado o el número de usuarios a los que podría afectar. Para complementar este sistema, la Comisión debe poder adoptar decisiones individuales por las que se designe un modelo de IA de uso general como modelo de IA de uso general con riesgo sistémico si se determina que dicho modelo tiene capacidades o repercusiones equivalentes a las reflejadas por el umbral establecido. Dicha decisión debe adoptarse atendiendo a una evaluación global de los criterios para la designación de modelos de IA de uso general con riesgo sistémico establecidos en un anexo del presente Reglamento, como la calidad o el tamaño del conjunto

(111) Komenigarria da metodologia bat ezartzea erabilera orokorreko AA-ereduak arrisku sistemikoak dakartzaten erabilera orokorreko AA-eredu gisa sailkatzeko. Arrisku sistemikoak sistemek gaitasun bereziki handiak dituztenean sortzen direnez, erabilera orokorreko AA-eredu batek arrisku sistemikoak dakartzala joko da inpaktu handiko gaitasunak dituztenean —tresna edo metodologia tekniko egokien bidez ebaluatuta— edo, irismen handia izanik, ondorio nabarmenak dituztenean barne-merkatuan. Erabilera orokorreko AA-eredu aurreratuenek erakutsitako gaitasunen pareko gaitasunak edo hortik gorakoak dira inpaktu handiko gaitasunak erabilera orokorreko AA-ereduetan. Eredu bat merkatuan jartzen denean edo hedapenaren arduradunek ereduarekin interakzioak sortzen dituztenean, hobeto ulertzen dira ereduaren gaitasunak. Kontuan hartuta zer egoeratan den teknika erregelamendu hau indarrean sartzen denean, erabilera orokorreko AA-eredua entrenatzeko erabilitako kalkulu-kopuru metatua —koma mugikorrek eragiketetan neurtua— erabil daiteke ereduaren gaitasunen gaineko hurbilketa bat egiteko. Entrenamendurako erabilitako kalkulu-kopuru metatuaren barruan sartzen dira ereduak hedatu aurretik haren gaitasunak hobetzeko egindako jardueretan eta metodoetan erabilitako kalkuluak —jarduera eta metodo horien artean dira, besteak beste, aurre-entrenamendua, datu sintetikoaren sorkuntza edo doikuntza—. Hortaz, koma mugikorrek eragiketen hasierako atalase bat ezarri behar da; hala, erabilera orokorreko AA-eredu bat atalase horretara iritsiz gero, horrek aditzera emango du eredu hori arrisku sistemikoa dakarren erabilera orokorreko AA-eredua izan daitekeela. Atalase hori doitzen joango da, gertatzen diren aldaketa teknologikoekin eta industrialekin bat etortzeko, adibidez algoritmoak hobetzen direnean edo hardwarearen efizientzia handitzen denean, eta ereduaren gaitasunaren adierazleekin eta erreferentziako parametroekin osatu behar da. Hori guztia hezurramitzeko, AA-bulegoak lankidetzan aritu behar du komunitate zientifikoarekin, industriarekin, gizarte zibilarekin eta beste aditu batzuekin. Bai atalaseek, bai inpaktu handiko gaitasunak ebaluatzeko erreferentzia-parametroek eta tresnek baliagarriak izan behar dute fidagarritasunez aurreikusteko erabilera orokorreko AA-ereduen orokortasuna, gaitasunak eta arrisku sistemikoa; horrez gain, kontuan har lezake nola jarriko den eredu merkatuan edo zenbat erabiltzailerik eragin liezaiekeen. Sistema hau osatzeko, Batzordeak aukera izan behar du erabaki individualak hartzeko, haien bidez erabilera orokorreko AA-eredu bat arrisku sistemikoa dakarren erabilera orokorreko AA-eredu izendatzeko, baldin eta ondorioztatzen bada finkatutako atalasean zehaztutako gaitasunen edo ondorioen baliokideak direla eredu horren gaitasunak edo ondorioak. Erabaki hori hartzeko, ebaluazio global bat egin behar da arrisku sistemikoak dakartzaten erabilera orokorreko AA-ereduak —erregelamendu honen eranskin batean zehaztutakoak— izendatzeko irizpideen gainean, hala nola entrenamendu-datuaren multzoaren



de datos de entrenamiento, el número de usuarios profesionales y finales, sus modalidades de entrada y de salida, su nivel de autonomía y escalabilidad o las herramientas a las que tiene acceso. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de uso general con riesgo sistémico, la Comisión debe tener en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de uso general presenta riesgos sistémicos.

(112) También es necesario aclarar un procedimiento para la clasificación de un modelo de IA de uso general con riesgos sistémicos. Debe presumirse que un modelo de IA de uso general que alcanza el umbral aplicable para las capacidades de gran impacto es un modelo de IA de uso general con riesgo sistémico. El proveedor debe enviar una notificación a la Oficina de IA a más tardar dos semanas después de que se cumplan los requisitos o de que se sepa que un modelo de IA de uso general cumplirá los requisitos que conducen a la presunción. Esto es especialmente pertinente en relación con el umbral de operaciones de coma flotante, ya que el entrenamiento de los modelos de IA de uso general requiere una planificación considerable que incluye la asignación previa de recursos computacionales y, por tanto, los proveedores de modelos de IA de uso general pueden saber si su modelo alcanzará el umbral antes del fin del entrenamiento. En el contexto de dicha notificación, el proveedor debe poder demostrar que, debido a sus características específicas, un modelo de IA de uso general no presenta excepcionalmente riesgos sistémicos y que, por tanto, no debe clasificarse como modelo de IA de uso general con riesgos sistémicos. Esa información es valiosa para que la Oficina de IA anticipe la introducción en el mercado de modelos de IA de uso general con riesgos sistémicos y para que los proveedores pueden empezar a colaborar con la Oficina de IA en una fase temprana. Dicha información es especialmente importante cuando esté previsto divulgar un modelo de IA de uso general como modelo de código abierto, dado que, tras la divulgación de modelos de código abierto, puede resultar más difícil aplicar las medidas necesarias para garantizar el cumplimiento de las obligaciones establecidas en el presente Reglamento.

(113) Si la Comisión descubre que un modelo de IA de uso general del que no tenía conocimiento o que el proveedor pertinente no le había notificado cumple los requisitos para ser clasificado como modelo de IA de uso general con riesgo sistémico, la Comisión debe estar facultada para designarlo. Además de las actividades de supervisión de la Oficina de IA, un sistema de alertas cualificadas debe garantizar que la Oficina de IA sea informada por el grupo de expertos científicos de la existencia de modelos de IA de uso

kalitatea edo tamaina, erabiltzaile profesionalen eta azken erabiltzaileen kopurua, sarrera- eta irteera-modalitateak, autonomia-maila eta eskalagarritasuna edo eskura dituen tresnak. Arrisku sistemikoa dakarren erabilera orokorreko AA-eredu gisa sailkatutako ereduaren hornitzaile batek eskaera arrazoitua egin ondoren, Batzordeak kontuan hartu behar du eskaera, eta berriz ebaluatu ahal izango du ea erabilera orokorreko AA-ereduak arrisku sistemikoak dakartzan oraindik.

(112) Beharrezkoa da, halaber, arrisku sistemikoak dakartzan erabilera orokorreko AA-ereduak sailkatzeko prozedura zehaztea. Inpaktu handiko gaitasunei dagokien atalaseira iristen den erabilera orokorreko AA-eredu bat uste izatekoa da arrisku sistemikoa dakarren erabilera orokorreko AA-eredu bat dela. Hornitzaileak jakinarazpen bat bidali behar dio AA-bulegoari, beranduenez ere bi astera betekizunak betetzen direnetik edo erabilera orokorreko AA-eredu batek uste hori eragiten duten betekizunak beteko dituela jakiten denetik. Jardunbide hori bereziki egokia da koma mugikorrek eragiketen atalaseari dagokionez; izan ere, erabilera orokorreko AA-ereduen entrenamenduak plangintza handia eskatzen du, baliabide konputazionalen alde aurreko esleipena barne, eta, beraz, erabilera orokorreko AA-ereduen hornitzaileek beren ereduaren entrenamendua amaitu baino lehen atalaseira iritsiko den jakin dezakete. Jakinarazpen horren testuinguruan, hornitzaileak modua izan behar du egiaztatzeko ezen, erabilera orokorreko AA-eredua batek, haren ezaugarri espezifikoak direla-eta, ez dakarrela aparteko arrisku sistemikorik eta, beraz, ez dela sailkatu behar arrisku sistemikoak dakartzan erabilera orokorreko AA-eredu gisa. Informazio hori oso erabilgarria da AA-bulegoak arrisku sistemikoak dakartzaten erabilera orokorreko AA-ereduak merkatuan jartzeko prozesua aurreratu ahal izateko eta hornitzaileak fase goiztiar batean hasi ahal izateko AA-bulegoarekin lankidetzan. Informazio horrek garrantzi berezia hartzen du erabilera orokorreko AA-eredu bat kode irekiko eredu gisa jendarteratzea aurreikusten denean; izan ere, kode irekiko ereduak jendartera zabaltu ostean, zailagoa gerta daiteke erregelamendu honetan ezarritako betebeharrak betetzen direla bermatzeko beharrezkoak diren neurriak aplikatzea.

(113) Batzordeak jakiten badu erabilera orokorreko AA-eredu batek arrisku sistemikoa dakarren erabilera orokorreko AA-eredutzat sailkatzeko betekizunak betetzen dituela, eta alde aurretik horren berri izan ez bazuen edo hornitzaileak horren berri eman ez bazion, Batzordeak ahalmena izan behar du eredu hori arrisku sistemikoa dakarren erabilera orokorreko AA-eredutzat sailkatzeko. Alerta kualifikatuen sistema bat ezarri behar da; AA-bulegoaren ikuskatze-jarduerak egiteaz gain, bermatu behar du aditu zientifikoek taldeak AA-



general que podrían ser clasificados como modelos de IA de uso general con riesgos sistémico.

(114) Los proveedores de modelos de IA de uso general que presenten riesgos sistémicos deben estar sujetos, además de a las obligaciones impuestas a los proveedores de modelos de IA de uso general, a obligaciones encaminadas a detectar y atenuar dichos riesgos y a garantizar un nivel adecuado de protección en materia de ciberseguridad, independientemente de si dichos modelos se ofrecen como modelos independientes o están integrados en sistemas de IA o en productos. Para alcanzar esos objetivos, el presente Reglamento debe exigir a los proveedores que lleven a cabo las evaluaciones de los modelos necesarias, en particular antes de la primera introducción en el mercado, y que, por ejemplo, lleven a cabo y documenten pruebas de simulación de adversarios, también, según proceda, mediante pruebas externas independientes o pruebas internas. Además, los proveedores de modelos de IA de uso general con riesgos sistémicos deben evaluar y mitigar continuamente los riesgos sistémicos, por ejemplo, mediante el establecimiento de políticas de gestión de riesgos, como procesos de rendición de cuentas y gobernanza, la puesta en práctica de la vigilancia poscomercialización, la adopción de medidas adecuadas durante todo el ciclo de vida del modelo y la cooperación con los agentes pertinentes a lo largo de la cadena de valor de la IA.

(115) Los proveedores de modelos de IA de uso general con riesgos sistémicos deben evaluar y mitigar los posibles riesgos sistémicos. Si, a pesar de los esfuerzos por detectar y prevenir los riesgos relacionados con un modelo de IA de uso general que pueda presentar riesgos sistémicos, el desarrollo o el uso del modelo provoca un incidente grave, el proveedor del modelo de IA de uso general debe, sin demora indebida, hacer un seguimiento del incidente y comunicar toda la información pertinente y las posibles medidas correctoras a la Comisión y a las autoridades nacionales competentes. Además, los proveedores deben garantizar que el modelo y su infraestructura física, si procede, tengan un nivel adecuado de protección en materia de ciberseguridad durante todo el ciclo de vida del modelo. La protección en materia de ciberseguridad relacionada con los riesgos sistémicos asociados al uso malintencionado o a los ataques debe tener debidamente en cuenta las fugas accidentales de modelos, las divulgaciones no autorizadas, la elusión de las medidas de seguridad y la defensa contra los ciberataques, el acceso no autorizado o el robo de modelos. Esa protección podría facilitarse asegurando los pesos, los algoritmos, los servidores y los conjuntos de datos del modelo, por ejemplo, mediante medidas de seguridad operativa para la seguridad de la información, medidas específicas en materia de ciberseguridad, soluciones técnicas adecuadas y establecidas y

bulegoari jakinaraziko diola badirela erabilera orokorreko AA-eredu batzuk arrisku sistemikoa dakarten erabilera orokorreko AA-eredutzat sailkatu litezkeenak.

(114) Arrisku sistemikoak dakartzaten erabilera orokorreko AA-ereduen hornitzaileek, erabilera orokorreko AA-ereduen hornitzaileei ezarritako betekizunez gain, bestelako betekizun batzuk ere bete behar dituzte, arrisku horiek hautemateko eta leuntzeko eta zibersegurtasunaren arloan babes-maila egokia bermatzeko, eredu horiek eredu independente modura eskaini zein AA-sistemetan edo -produktuetan txertatuta egon. Helburu horiek lortzeko, erregelamendu honek hertsiki eskatu behar die hornitzaileei beharrezko ebaluazioak egin ditzaten ereduetan, batez ere merkatuan lehenengoz jarri aurretik, eta, esaterako, ereduaren aurkaritza-probak egin eta dokumentatu ditzaten, egoki denean kanpoko proba independenteak edo barruko probak ere eginda. Gainera, erabilera orokorreko AA-ereduen hornitzaileek etengabe ebaluatu eta leundu behar dituzte arrisku sistemikoak, eta, horretarako, adibidez, arriskuak kudeatzeko politikak ezarri behar dituzte, hala nola kontu-emate eta gobernanzako politikak, eta merkaturatu osteko zaintza egin, ereduaren bizi-ziklo osorako neurri egokiak hartu eta egoki diren eragileekin lankidetzan aritu AAren balio-kate osoan barrena.

(115) Arrisku sistemikoak dakartzaten erabilera orokorreko AA-ereduen hornitzaileek sor daitezkeen arrisku sistemikoak ebaluatu eta leundu behar dituzte. Arrisku sistemikoak ekar ditzakeen erabilera orokorreko AA-ereduekin lotutako arriskuak hautemateko eta saihesteko ahaleginak ahalegin, ereduak, garatzen edo erabiltzen ari den bitartean, gorabehera larriren bat eragiten badu, erabilera orokorreko AA-ereduaren hornitzaileak gertaeraren segimendua egin beharko du bidegabeko atzerapenik gabe, eta Batzordeari zein agintaritza nazional eskudunei beharrezko informazio guztia jakinarazi, baita har daitezkeen neurri zuzentzaileen berri eman ere. Hornitzaileek, gainera, bermatu behar dute ereduak eta haren azpiegitura fisikoak, hala badagokio, zibersegurtasuneko babes-maila egokia dutela ereduaren bizi-ziklo osoan. Asmo txarreko erabilerak edo erasoak izateko arrisku sistemikoei aurre egiteko zibersegurtasun-babesak zorrotz hartu behar ditu kontuan honelako egoerak: ereduak istripuz ihes egitea, ereduak baimenik gabe zabaltzea, segurtasun-neurriak eta zibererasoen aurkako babesa ez betetzea, eredura baimenik gabe sartzea edo ereduak lapurtzea. Ereduaren pisuak, algoritmoak, zerbitzariak eta datu multzoak segurtatzea izan daiteke babes hori lortzeko modu bat: adibidez, informazioa segurtatzeko segurtasun-neurri operatiboak hartuz, zibersegurtasun-arloko neurriak zehaztuz, aurrez ezarritako soluzio tekniko egokiak emanez eta sarbide



controles de acceso cibernéticos y físicos, en función de las circunstancias pertinentes y los riesgos existentes.

(116) La Oficina de IA debe fomentar y facilitar la elaboración, revisión y adaptación de códigos de buenas prácticas, teniendo en cuenta los enfoques internacionales. Podría invitarse a participar a todos los proveedores de modelos de IA de uso general. Para garantizar que los códigos de buenas prácticas reflejen el estado actual de la técnica y tengan debidamente en cuenta perspectivas distintas, la Oficina de IA debe colaborar con las autoridades nacionales competentes pertinentes y, cuando proceda, podrá consultar a organizaciones de la sociedad civil y a otras partes interesadas y expertos pertinentes, incluido el Grupo de Expertos Científicos, por lo que respecta a la elaboración de dichos códigos. Los códigos de buenas prácticas deben comprender las obligaciones de los proveedores de modelos de IA de uso general y de modelos de IA de uso general que presenten riesgos sistémicos. Además, en lo que respecta a los riesgos sistémicos, los códigos de buenas prácticas deben ayudar a establecer una taxonomía de riesgos en la que figuren el tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluidas sus fuentes. Asimismo, los códigos de buenas prácticas deben centrarse en medidas específicas de evaluación y reducción de riesgos.

(117) Los códigos de buenas prácticas deben constituir una herramienta fundamental para el cumplimiento adecuado de las obligaciones previstas en el presente Reglamento para los proveedores de modelos de IA de uso general. Los proveedores deben poder basarse en códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones. Mediante actos de ejecución, la Comisión podrá decidir aprobar un código de buenas prácticas y conferirle una validez general dentro de la Unión o, alternatively, establecer normas comunes para la puesta en práctica de las obligaciones pertinentes si, para el momento en que el presente Reglamento sea aplicable, no ha podido finalizarse un código de buenas prácticas o la Oficina de IA no lo considera adecuado. Una vez que se haya publicado una norma armonizada y que la Oficina de IA la considere adecuada para cubrir las obligaciones pertinentes, el cumplimiento de una norma armonizada europea debe dar a los proveedores la presunción de conformidad. Además, los proveedores de modelos de IA de uso general deben poder demostrar el cumplimiento utilizando medios alternativos adecuados si no se dispone de códigos de buenas prácticas o de normas armonizadas, o si deciden no basarse en ellos.

(118) El presente Reglamento regula los sistemas de IA y modelos de IA imponiendo determinados requisitos y obligaciones a los agentes pertinentes del mercado que los introduzcan en el mercado, los pongan en servicio o

zibernetikoak eta fisikoak kontrolatuz, unean uneko egoeraren eta arriskuen arabera.

(116) AA-bulegoak jardunbide egokien kodeak berrikusi eta egokitzea sustatu eta erraztu behar du, nazioarteko ikuspuntuak kontuan hartuta. Erabilera orokorreko AA-ereduen hornitzaile guztiei dei egin ahal izango zaie parte har dezaten. Jardunbide egokien kodeek teknikaren unean uneko egoera islatu dezaten eta egokiro barne har ditzaten askotariko ikuspegiak, AA-bulegoak lankidetzan aritu behar du agintaritza nazional eskudunekin, eta, egoki denean, gizarte zibileko antolakundeei ere galde egin ahal izango die, baita beste alderdi interesdun eta aditu batzuei ere, Aditu Zientifikoen Taldea ere barne, kode horiek eratze aldera. Erabilera orokorreko AA-ereduen zein arrisku sistemikoak dakartzaten erabilera orokorreko AA-ereduen hornitzaileen betebeharrak ere jaso behar dituzte jardunbide egokien kodeek. Arrisku sistemikoei begira, jardunbide egokien kodeek arriskuen taxonomia bat ezartzen lagundu behar dute, hartan jasotzeko Batasunaren eremuan dauden arrisku sistemikoen motak eta izaera, baita iturriak ere. Horrez gain, jardunbide egokien kodeek arriskuak ebaluatzeko eta murrizteko neurri zehatzak hartu behar dituzte.

(117) Jardunbide egokien kodeek funtsezko tresna izan behar dute erabilera orokorreko AA-ereduen hornitzaileei erregelamendu honetan aurreikusitako betebeharrak egokiro betetzen laguntzeko. Hala, jardunbide egokien kodeek modua eman behar diete hornitzaileei betebeharrak betetzen dituztela erakusteko. Betearazpen-egintzen bidez, Batzordeak jardunbide egokien kode bat onartzeko erabakia hartu ahal izango du, eta baliozkotasun orokorra eman Batasunaren barruan, edo arau komunak ezarri zenbait betebeharrak abian jartzeko, erregelamendu hau aplikagarri jartzen den unerako oraindik jardunbide egokien kode bat gauzatu ez balitz ere edo AA-bulegoak egokitzen joko ez balu ere. Behin arau harmonizatua argitaratutakoan eta AA-bulegoak arau hori egoki diren betebeharrak betetzeko aipostatzat jotakoan, Europako arau harmonizatua betetzeak adostasun-presuntzioa eman behar die hornitzaileei. Erabilera orokorreko AA-ereduen hornitzaileek bitarteko alternatibo egokiak eduki behar dituzte betebeharrak betetzen dituztela frogatu ahal izateko, ez badago jardunbide egokien koderik edo arau harmonizaturik, edo bitarteko horiek ez erabiltzea erabakitzen bada.

(118) Erregelamendu honek AA-sistemak eta AA-ereduak arautzen ditu, eta betekizun eta betebeharrak jakin batzuk ezartzen dizkie ereduok Batasunean merkatuan jartzen, zerbitzuan ipintzen edo erabiltzen dituzten



los utilicen en la Unión, complementando así las obligaciones de los prestadores de servicios intermediarios que integren dichos sistemas o modelos en sus servicios, regulados por el Reglamento (UE) 2022/2065. En la medida en que dichos sistemas o modelos estén integrados en plataformas en línea de muy gran tamaño o en motores de búsqueda en línea de muy gran tamaño que hayan sido designados, están sujetos al marco de gestión de riesgos establecido en el Reglamento (UE) 2022/2065. Por consiguiente, debe presumirse que se han cumplido las obligaciones correspondientes del presente Reglamento a menos que surjan riesgos sistémicos significativos no cubiertos por el Reglamento (UE) 2022/2065 y se detecten en dichos modelos. En este marco, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño están obligados a evaluar los posibles riesgos sistémicos derivados del diseño, el funcionamiento y el uso de sus servicios, incluido el modo en que el diseño de los sistemas algorítmicos utilizados en el servicio puede contribuir a dichos riesgos, así como los riesgos sistémicos derivados de posibles usos indebidos. Dichos prestadores también están obligados a adoptar las medidas de reducción de riesgos adecuadas respetando los derechos fundamentales.

(119) Tomando en consideración el rápido ritmo de innovación y la evolución tecnológica de los servicios digitales incluidos en el ámbito de aplicación de diferentes instrumentos del Derecho de la Unión, en particular teniendo en cuenta el uso y la percepción de sus destinatarios, los sistemas de IA sujetos al presente Reglamento pueden prestarse como servicios intermediarios, o partes de estos, en el sentido del Reglamento (UE) 2022/2065, que debe interpretarse de manera tecnológicamente neutra. Por ejemplo, los sistemas de IA pueden utilizarse para ofrecer motores de búsqueda en línea, en particular en la medida en que un sistema de IA, como un chatbot en línea, efectúe búsquedas, en principio, en todos los sitios web, incorpore a continuación los resultados a sus conocimientos existentes y utilice los conocimientos actualizados para generar una única información de salida que combine diferentes fuentes de información.

(120) Además, las obligaciones impuestas a los proveedores y a los responsables del despliegue de determinados sistemas de IA en el presente Reglamento destinadas a permitir que se detecte y divulgue que los resultados de salida de dichos sistemas han sido generados o manipulados de manera artificial resultan especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular a las obligaciones de los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda en línea de muy gran tamaño de detectar y mitigar los riesgos sistémicos que pueden surgir de la divulgación de contenidos que hayan sido generados o

merkatuko eragileei. Horrela, sistema edo eredu horiek beren zerbitzuetan integratuko dituzten bitarteko zerbitzuen emaileen betebeharrak osatzen dituzte [zerbitzuok (EB) 2022/2065 Erregelamenduan daude araututa]. Sistema edo eredu horiek aurrez izendatu diren lineako plataforma oso handietan edo lineako bilaketa-motor oso handietan txertatuta dauden heinean, (EB) 2022/2065 Erregelamenduan ezarritako arriskuak kudeatzeko esparruari lotuta daude. Ondorioz, pentsatzekoa da, halaber, erregelamendu honetatik dagozkion betebeharrak bete direla, salbu eta (EB) 2022/2065 Erregelamenduak barne hartu gabeko arrisku sistemiko nabarmenak sortu eta eredu horietan hautematen badira. Testuinguru horretan, lineako plataforma eta lineako bilaketa-motor oso handi horien emaileek beren zerbitzuen diseinutik, funtzionamendutik eta erabileratik erator daitezkeen arrisku sistemikoak ebaluatzeko betebeharra dute, eta, betebeharrak horren barruan, berariaz neurtu behar dute zerbitzuan erabiltzen diren sistema algoritmikoen diseinuak zer ekarpen egin dezakeen arrisku horietan, eta zer arrisku sistemiko sor daitezkeen bidegabeko erabileren ondorioz. Zerbitzu-emaile horiek, orobat, arriskuak murrizteko neurri egokiak hartzeko betebeharra dute, oinarritzko eskubideak errespetatuta beti.

(119) Aintzakotzat izanda Batasuneko zuzenbidearen hainbat tresnaren aplikazio-eremuan sartutako zerbitzu digitalek zer berrikuntza-erritmo bizia duten eta nolako bilakaera teknologikoa dakarten, bereziki kontuan hartuta hartzaileen erabilera eta pertzepzioa, erregelamendu honi lotutako AA-sistemak bitarteko zerbitzu gisa edo horien zati gisa eman daitezke, (EB) 2022/2065 Erregelamenduari zentzuan, zeina modu teknologikoki neutroan interpretatu behar baita. Adibidez, lineako bilaketa-motorrak eskaintzeko erabil daitezke AA-sistemak; izan ere, AA-sistema batek—esaterako, lineako txatbotak—, bilaketak egin ditzake, hasteko webgune guztietan, eta lehendik zituen ezagutzetan gehitu bilaketaren emaitzak; hala, ezagutza eguneratuak erabiliko ditu irteera-informazio bakarra sortzeko informazio-iturri desberdinak konbinatuta.

(120) Gainera, AA-sistema jakin batzuen irteera-emaitzak modu artifizialean sortu edo manipulatu direla detektatu eta jendarteratu ahal izateko erregelamendu honetan sistema horien hornitzaileei eta hedapenaren arduradunei ezarritako betebeharrak egoki-egokiak dira (EB) 2022/2065 Erregelamendua eraginkortasunez aplikatu ahal izateko. Bereziki aplikatzen da alderdi hori lineako plataforma oso handien edo lineako bilaketa-motor oso handien emaileen kasuan, modu artifizialean sortu edo manipulatu diren edukiak jendartean zabaltzeak sor ditzakeen arrisku sistemikoak hautemateko eta arintzeko betebeharra duten heinean, batez ere prozesu demokratikoetan, diskurtso zibikoan



manipulados de manera artificial, en particular el riesgo de los efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, también a través de la desinformación.

(121) La normalización debe desempeñar un papel fundamental para proporcionar soluciones técnicas a los proveedores para garantizar el cumplimiento del presente Reglamento, en consonancia con el estado actual de la técnica, para promover la innovación, así como la competitividad y el crecimiento en el mercado único. El cumplimiento de las normas armonizadas definidas en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo (41), que generalmente se espera que reflejen el estado actual de la técnica, debe ser un medio para que los proveedores demuestren la conformidad con los requisitos previstos en el presente Reglamento. Por consiguiente, debe fomentarse una representación equilibrada de los intereses de todas las partes interesadas pertinentes —en particular las pymes, las organizaciones de consumidores y las partes interesadas de los ámbitos social y medioambiental— en la elaboración de normas, de conformidad con los artículos 5 y 6 del Reglamento (UE) n.º 1025/2012. A fin de facilitar el cumplimiento, la Comisión debe emitir las peticiones de normalización sin demora indebida. Al preparar la petición de normalización, la Comisión debe consultar al foro consultivo y al Consejo de IA para recabar los conocimientos especializados pertinentes. No obstante, a falta de referencias pertinentes a las normas armonizadas, la Comisión debe poder establecer, mediante actos de ejecución y previa consulta al foro consultivo, especificaciones comunes para determinados requisitos previstos en el presente Reglamento. Las especificaciones comunes deben ser una solución alternativa excepcional para facilitar la obligación del proveedor de cumplir los requisitos del presente Reglamento cuando ninguna de las organizaciones europeas de normalización haya aceptado la petición de normalización, cuando las normas armonizadas pertinentes respondan de forma insuficiente a las preocupaciones en materia de derechos fundamentales, cuando las normas armonizadas no cumplan la petición o cuando se produzcan retrasos en la adopción de una norma armonizada adecuada. Cuando dichos retrasos en la adopción de una norma armonizada se deban a la complejidad técnica de dicha norma, la Comisión debe tenerlo en cuenta antes de considerar la posibilidad de establecer especificaciones comunes. Se anima a la Comisión a que, a la hora de elaborar especificaciones comunes, coopere con los socios internacionales y los organismos internacionales de normalización.

(122) Conviene que, sin perjuicio del uso de normas armonizadas y especificaciones comunes, se presuma que los proveedores de un sistema de IA de alto riesgo que haya sido entrenado y probado con datos que

eta hauteskunde-prozesuetan, baita desinformazioaren bidez ere, ondorio negatiboak —benetakoak edo aurreikusgarriak— eragiteko arriskuari begira.

(121) Normalizazioak funtsezko eginkizuna bete behar du hornitzaileei soluzio teknikoak emateko, erregelamendu hau betetzen dela bermatze aldera, teknikaren unean uneko egoerarekin bat etorrita, modu horretara berrikuntza, lehiakortasuna eta hazkundera sustatzeko merkatu bakarrean. Europako Parlamentuaren eta Kontseiluaren (EB) 1025/2012 Erregelamenduaren 2.1 artikuluko c) letran (41) definitutako arau bateratuak betetzeak —oro har espero izanda teknikaren unean uneko egoera islatzea— bitarteko izan behar du hornitzaileek erregelamendu honetan aurreikusitako betekizunekin bat egiten dutela frogatzeko. Horrenbestez, arauak egiteko orduan egoki diren alderdi interesdun guztien interesak modu orekatuan ordezkatuta egotea sustatu behar da —bereziki ETEak, kontsumitzaileen antolakundeak eta gizarte- eta ingurumen-eremuetako alderdi interesdunak—, bat etorrita hartara (EB) 1025/2012 Erregelamenduaren 5. eta 6. artikuluekin. Horretarako, Batzordeak bidegabeko atzerapenik gabe bideratu behar ditu normalizazio-eskaerak. Normalizazio-eskaera prestatzean, Batzordeak kontsulta-foroari eta AA-kontseiluari galdetu behar die, behar diren ezagutza espezializatuak biltzeko. Arau harmonizatuen gaineko erreferentzia egokirik ez badago, Batzordeak aukera izan behar du, betearazpen-egintzen bidez eta kontsulta-foroari galdetu ostean, erregelamendu honetan aurreikusitako betekizun jakin batzuetarako zehaztaperen komunak ezartzeko. Nolanahi ere, zehaztaperen komun horiek salbuespeneko soluzio alternatiboa izan behar dute, hornitzaileari erregelamendu honetako betekizunak betetzeko beharrean laguntzeko, egoera jakin batzuetan: Europako normalizazio-antolakundeetako inork onartu ez duenean normalizazio-eskaera; arau harmonizatuek ez dutenean eman erantzun nahikorik oinarritzko eskubideen arloan sortutako kezkei; arau harmonizatuek ez dutenean eskaera betetzen, edo atzerapenak gertatzen direnean arau harmonizatu egokia eratzeko orduan. Arauaren konplexutasuna dela-eta atzeratzen ari bada arau harmonizatua eratzeko prozesua, Batzordeak kontuan hartu behar du egoera hori, zehaztaperen komunak ezartzeko aukera aintzat hartu aurretik. Bestalde, bultza egiten zaio Batzordeari lankidetzan jardun dezan nazioarteko bazkideekin eta normalizazioko nazioarteko organismoekin, zehaztaperen komunak elkarrekin lantzeko.

(122) Arau harmonizatuak eta zehaztaperen komunak erabiltzea eragotzi gabe, arrisku handiko AA-sistemen kasuan —AA-sistema horiek zer ingurunetan erabiltzea aurreikusten den, ingurune geografiko, konduktual,



reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto que se utilice el sistema de IA cumplen la medida pertinente prevista en el requisito en materia de gobernanza de datos establecido en el presente Reglamento. Sin perjuicio de los requisitos relacionados con la solidez y la precisión establecidos en el presente Reglamento, de conformidad con el artículo 54, apartado 3, del Reglamento (UE) 2019/881, debe presumirse que los sistemas de IA de alto riesgo que cuenten con una certificación o una declaración de conformidad en virtud de un esquema de certificación de la ciberseguridad con arreglo a dicho Reglamento y cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea cumplen el requisito de ciberseguridad del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad, o partes de estos, contemplen dicho requisito. Esto se entiende sin perjuicio del carácter voluntario de dicho esquema de ciberseguridad.

(123) A fin de garantizar que los sistemas de IA de alto riesgo sean altamente fiables, debe someterse a dichos sistemas a una evaluación de la conformidad antes de su introducción en el mercado o puesta en servicio.

(124) Para reducir al mínimo la carga que deben soportar los operadores y evitar posibles duplicidades, conviene, en el caso de los sistemas de IA de alto riesgo asociados a productos regulados por la legislación de armonización de la Unión vigente basada en el nuevo marco legislativo, que la conformidad de dichos sistemas de IA con los requisitos establecidos en el presente Reglamento se evalúe en el marco de la evaluación de la conformidad ya prevista en dicha legislación. Por lo tanto, la aplicabilidad de los requisitos del presente Reglamento no debe afectar a la lógica, la metodología o la estructura general específicas de la evaluación de la conformidad prevista en los actos legislativos de armonización pertinentes de la Unión.

(125) Dada la complejidad de los sistemas de IA de alto riesgo y los riesgos asociados a ellos, es importante desarrollar un procedimiento adecuado de evaluación de la conformidad de los sistemas de IA de alto riesgo en el que participen organismos notificados, denominado «evaluación de la conformidad de terceros». No obstante, habida cuenta de la experiencia actual de los profesionales que realizan la certificación previa a la comercialización en el campo de la seguridad de los productos y de la distinta naturaleza de los riesgos implicados, procede limitar, al menos en la fase inicial de aplicación del presente Reglamento, el alcance de las evaluaciones externas de la conformidad a los sistemas de IA de alto riesgo que no están asociados a productos. En consecuencia, el proveedor es quien, por norma general, debe llevar a cabo la evaluación de la conformidad de dichos sistemas bajo su propia

kontestual edo funtzional horixe islatzeko datuekin entrenatuta eta probatuta dauden heinean— komeni da suposatzea sistema horien hornitzaileek betetzen dutela datuen gobernantzaren arloan erregelamendu honetan ezarritako betekizunean aurreikusitako neurria. Erregelamendu honetan sendotasunarekin eta zehaztasunarekin lotuta ezarritako betekizunak bazter utzi gabe, (EB) 2019/881 Erregelamenduaren 54.3 artikulua arabera, baldin eta arrisku handiko AA-sistemek erregelamendu horri jarraikiz zibersegurtasunaren ziurtapen-eskema baten arabera ziurtapen edo adostasun-adierazpen bat badute eta haien erreferentziak Europar Batasunaren Aldizkari Ofizialean argitaratu badira, suposatu behar da erregelamendu honen zibersegurtasun-betekizuna betetzen dutela, zibersegurtasun-ziurtagiriak edo adostasun-adierazpenak, edo haien zati batzuek, baldintza hori jasotzen duten heinean. Nolanahi ere, zibersegurtasun-eskema hori borondatezkoa da.

(123) Arrisku handiko AA-sistemek fidagarritasun altua dutela bermatzeko, beharrezkoa da sistema horien adostasuna ebaluatzea sistemak merkaturan jarri edo zerbitzuan ipini aurretik.

(124) Operadoreek jasan beharreko karga ahalik eta gehien murrizteko eta bikoiztasunak saihesteko, legegintza-esparru berrian oinarrituta indarrean dagoen Batasunaren harmonizazioko legeriak araututako produktuei lotutako arrisku handiko AA-sistemen kasuan, komenigarria da legerian jada aurreikutsita dagoen adostasunaren ebaluazioaren testuinguruan ebaluatzea AA-sistema horiek erregelamendu honetan ezarritako betekizunekin duten adostasuna. Hortaz, erregelamendu honetako betekizunen aplikagarritasunak ez die eragin behar Batasunaren harmonizazioko lege-egintzetan aurreikusitako adostasuna ebaluatzeko logika, metodologia edo egitura orokor zehatzei.

(125) Arrisku handiko AA-sistemen konplexutasuna eta horiei lotutako arriskuak kontuan hartuta, garrantzitsua da arrisku handiko AA-sistemen adostasuna ebaluatzeko prozedura egoki bat garatzea, «hirugarrenen adostasunaren ebaluazioa» izeneko, organismo jakinaraziek hartan parte har dezaten. Dena dela, kontuan hartuta produktuen segurtasunaren arloan merkaturatu aurreko ziurtagiria egiten duten profesionalen egungo esperientzia eta inplikaturako arriskuen izaera askotarikoa, bidezkoa da muga jartzea produktuekin loturarik ez duten arrisku handiko AA-sistemen adostasunaren kanpoko ebaluazioen irismenari, erregelamendu honen aplikazioaren hasierako fasean behintzat. Ondorioz, oro har, hornitzaileak ebaluatu behar du sistema horien adostasuna, bere erantzukizunpean. Biometriarako



responsabilidad, con la única excepción de los sistemas de IA que están destinados a utilizarse para la biometría.

(126) Para poder realizar las evaluaciones de la conformidad de terceros cuando así se les exija, las autoridades nacionales competentes deben notificar, en virtud del presente Reglamento, a los organismos notificados, siempre que cumplan una serie de requisitos, en particular en lo que respecta a su independencia, sus competencias y la ausencia de conflictos de intereses, así como requisitos adecuados de ciberseguridad. Las autoridades nacionales competentes deben enviar la notificación de dichos organismos a la Comisión y a los demás Estados miembros a través del sistema de notificación electrónica desarrollado y gestionado por la Comisión con arreglo a lo dispuesto en el artículo R23 del anexo I de la Decisión n.º 768/2008/CE.

(127) En consonancia con los compromisos contraídos por la Unión en virtud del Acuerdo sobre Obstáculos Técnicos al Comercio, de la Organización Mundial del Comercio, es adecuado facilitar el reconocimiento mutuo de los resultados de las evaluaciones de la conformidad realizadas por organismos de evaluación de la conformidad competentes, con independencia del territorio en el que estén establecidos, siempre que dichos organismos de evaluación de la conformidad establecidos con arreglo al Derecho de un tercer país cumplan los requisitos aplicables del presente Reglamento y la Unión haya celebrado un acuerdo en ese sentido. En este contexto, la Comisión debe estudiar activamente posibles instrumentos internacionales a tal efecto y, en particular, procurar celebrar acuerdos de reconocimiento mutuo con terceros países.

(128) En consonancia con el concepto comúnmente establecido de «modificación sustancial» de los productos regulados por los actos legislativos de armonización de la Unión, conviene que, cada vez que se produzca un cambio que pueda afectar al cumplimiento del presente Reglamento por parte de un sistema de IA de alto riesgo (por ejemplo, un cambio de sistema operativo o de arquitectura de software) o cuando cambie la finalidad prevista del sistema, dicho sistema de IA se considere un sistema de IA nuevo que debe someterse a una nueva evaluación de la conformidad. Sin embargo, los cambios que se produzcan en el algoritmo y en el funcionamiento de los sistemas de IA que sigan «aprendiendo» después de su introducción en el mercado o su puesta en servicio, a saber, adaptando automáticamente el modo en que desempeñan sus funciones, no deben constituir una modificación sustancial, siempre que dichos cambios hayan sido predeterminados por el proveedor y se

erabilitzekoak diren AA-sistemak dira salbuespen bakarrak.

(126) Hirugarrenen adostasunaren ebaluazioak egin ahal izateko, erregelamendu honen arabera, agintaritza nazional eskudunek, hala eskatzen zaienean, organismo jakinaraziei eman behar diete jakitera, betiere egokiro betetzen badituzte zenbait betekizun —bereziki haien independentziari, eskumenei eta interes-gatazkarik ezari dagokienez— baita behar diren zibersegurtasun-betekizunak ere. Agintaritza nazional eskudunek organismo horien jakinarazpena bidali behar diete bai Batzordeari, bai gainerako estatu kideei, 768/2008/EE Erabakiaren I. eranskineko R23 artikuluan xedatutakoaren arabera Batzordeak garatu eta kudeatutako jakinarazpen elektronikoko sistemaren bidez.

(127) Bat etorrita Munduko Merkataritza Antolakundeak hitzartutako Merkataritzarako Oztopo Teknikoei buruzko Akordioaren arabera Batasunak hartutako konpromisoekin, egokia da adostasuna ebaluatzeneko organismo eskudunek elkarri aitortzea egindako adostasun-ebaluazioen emaitzak, organismo horiek edozein lurraldetan ezarrita daudela ere, baldin eta hirugarren herrialde bateko zuzenbidearen arabera ezarritako adostasuna ebaluatzeneko organismo horiek erregelamendu honetatik aplikatzekoak zaizkien betekizunak betetzen badituzte eta Batasunak akordio bat egin badu gai horretarako. Horiek horrela, Batzordeak zoli aztertu behar ditu nazioartean eremu hori jorratzeko egon daitezkeen tresnak, eta, bereziki, hirugarren herrialde batzuekin elkar aitortzeko akordioak egiten saiatu.

(128) Batasunaren harmonizazioko lege-egintzek araututako produktuen «funtsezko aldaketaren» kontzeptu orokorrarekin bat etorritik, aldaketa bat gertatzen den bakoitzean, aldaketa horrek kolokan jar badezake arrisku handiko AA-sistema batek erregelamendu hau bete ahal izatea (adibidez, sistema eragilea edo software-arkitektura aldatzen denean), edo sistemaren helburu aurreikusia aldatzen denean, komeni da AA-sistema hori AA-sistema berritatzat hartzea eta, beraz, haren adostasuna berriro ebaluatzea. Nolanahi ere, merkatuan jarri edo zerbitzuan ipini ostean «ikasten» jarraitzen duten AA-sistemen algoritmoan eta funtzionamenduan aldaketak gertatzen badira eta beren eginkizunak betetzeko modua automatikoki egokitzen badute, hori ez da funtsezko aldaketatzat jo behar, baldin eta hornitzaileak aurrez zehaztuta baditu aldaketa horiek eta adostasuna ebaluatzeneko unean jada ebaluatu badira.



hayan evaluado en el momento de la evaluación de la conformidad.

(129) Los sistemas de IA de alto riesgo deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interior. En el caso de los sistemas de IA de alto riesgo integrados en un producto, se debe colocar un marcado CE físico, que puede complementarse con un marcado CE digital. En el caso de los sistemas de IA de alto riesgo que solo se proporcionen digitalmente, debe utilizarse un marcado CE digital. Los Estados miembros no deben crear obstáculos injustificados a la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE.

(130) En determinadas condiciones, la rápida disponibilidad de tecnologías innovadoras puede ser crucial para la salud y la seguridad de las personas, la protección del medio ambiente y la mitigación del cambio climático, y para la sociedad en su conjunto. Por consiguiente, resulta oportuno que las autoridades de vigilancia del mercado puedan autorizar, por motivos excepcionales de seguridad pública o con vistas a proteger la vida y la salud de personas físicas, el medio ambiente y activos fundamentales de la industria y de las infraestructuras, la introducción en el mercado o la puesta en servicio de sistemas de IA que no hayan sido sometidos a una evaluación de la conformidad. En situaciones debidamente justificadas previstas en el presente Reglamento, las autoridades garantes del cumplimiento del Derecho o las autoridades de protección civil podrán poner en servicio un sistema de IA de alto riesgo específico sin la autorización de la autoridad de vigilancia del mercado, siempre que se solicite la autorización durante el uso o después de este sin demora indebida.

(131) Con el objetivo de facilitar la labor de la Comisión y de los Estados miembros en el ámbito de la IA, así como de incrementar la transparencia de cara al público, debe exigirse a los proveedores de sistemas de IA de alto riesgo que no estén asociados a productos que entren dentro del ámbito de aplicación de los actos legislativos de armonización de la Unión que sean pertinentes y estén en vigor, y a los proveedores que consideren que alguno de los sistemas de IA enumerados en los casos de uso de alto riesgo en un anexo del presente Reglamento no es de alto riesgo sobre la base de una excepción que se registren y que registren información sobre sus sistemas de IA en una base de datos de la UE, de cuya creación y gestión se encargará la Comisión. Antes de utilizar tal sistema de IA enumerado en los casos de uso de alto riesgo en un anexo del presente Reglamento, los responsables del despliegue de sistemas de IA de alto riesgo que sean

(129) Arrisku handiko AA-sistemek CE marka eduki behar dute egiaztatzeko ados datozela erregelamenduarekin, hartara askatasunez zirkulatu ahal izateko barne-merkatuan. Produktu batean txertatutako arrisku handiko AA-sistemen kasuan, CE marka fisiko bat jarri behar da, eta CE marka digital batekin ere osa daiteke. Digitalki soilik eskaintzen diren arrisku handiko AA-sistemen kasuan, CE marka digitala erabili behar da. Estatu kideek ez dute justifikatu gabeko trabarik jarri behar arrisku handiko AA-sistemak merkatuan jartzeko edo zerbitzuan ipintzeko, sistema horiek erregelamendu honetan ezarritako betekizunak betetzen dituzten heinean eta CE marka duten heinean.

(130) Teknologia berritzaileak hain arin ari dira garatzen, egoera jakin batzuetan funtsezkoak izan baitaitezke pertsonen osasuna eta segurtasuna zaintzeko, ingurumena babestu eta klima-aldaketa leuntzeko eta gizarteri oro har onura ekartzeko. Horrenbestez, egokia da merkaturak zaintzeko agintaritzek modua izatea adostasunaren ebaluazioa izan ez duten AA-sistemak merkatuan jartzeko eta zerbitzuan ipintzeko, betiere segurtasun publikoko salbuespeneko egoeretan edo helburua denean babesa ematea pertsona fisikoen biziari eta osasunari, ingurumenari eta industriaren eta azpiegituren funtsezko aktiboei. Erregelamendu honetan aurreikusitako eta behar bezala justifikatutako egoeretan, zuzenbidea betearazteko agintaritzek edo babes zibileko agintaritzek eskumena izango dute arrisku handiko AA-sistema jakin bat zerbitzuan ipintzeko merkaturak zaintzeko agintaritzaren baimenik gabe. Horretarako, bidegabeko atzerapenik gabe eskatu beharko dute baimena, sistema jardunean dela edo jardun ostean.

(131) Batzordeak eta estatu kideek AAren arloan egiten duten lana bultzatzeko eta herritarrei begira gardentasuna areagotzeko, arrisku handiko AA-sistemak ez daudenean lotuta egoki diren eta indarrean diren Batasunaren harmonizazioko lege-egintzen aplikazio-eremuan sartutako produktuekin, edo AA-sistemen hornitzaileek uste dutenean erregelamendu honetako eranskin batean zerrendatutako arrisku handiko erabileretan jasotako AA-sistema bat ez dela arrisku handikoa salbuespen batean oinarrituta, halako egoeretan hornitzaile horiei eskatu behar zaie erregistra daitezela eta erregistra dezatela beren AA-sistemen gaineke informazioa EBren datu-base batean (Batzordea arduratuko da datu-base hori sortzeaz eta kudeatzeaz). Erregelamendu honetako eranskin batean zehaztutako zerrendan arrisku handikotzat jasotako AA-sistema bat erabili aurretik, arrisku handiko AA-sistemaren hedapenaren arduradunak agintaritza,



autoridades, órganos u organismos públicos deben registrarse en dicha base de datos y seleccionar el sistema que tengan previsto utilizar. Los demás responsables del despliegue deben poder efectuar dicho registro con carácter voluntario. Esta sección de la base de datos de la UE debe ser de acceso público y gratuito, debe ser fácil navegar por la información, y esta ha de ser comprensible y legible por máquina. La base de datos de la UE también debe ser fácil de utilizar, por ejemplo, proporcionando funcionalidades de búsqueda, también a través de palabras clave, que permitan al público en general encontrar la información que debe presentarse para el registro de los sistemas de IA de alto riesgo y relativa a los casos de uso de sistemas de IA de alto riesgo contemplados en un anexo del presente Reglamento, a la que corresponden los sistemas de IA de alto riesgo. También debe registrarse en la base de datos de la UE toda modificación sustancial de sistemas de IA de alto riesgo. En el caso de los sistemas de IA de alto riesgo en el ámbito de la garantía del cumplimiento del Derecho y de la gestión de la migración, el asilo y el control fronterizo, las obligaciones de registro deben cumplirse en una sección segura no pública de la base de datos de la UE. El acceso a esa sección debe limitarse estrictamente a la Comisión y a las autoridades de vigilancia del mercado en lo que respecta a su sección nacional de dicha base de datos. Los sistemas de IA de alto riesgo en el ámbito de las infraestructuras críticas solo deben registrarse a nivel nacional. La Comisión debe ser la responsable del tratamiento de la base de datos de la UE, de conformidad con el Reglamento (UE) 2018/1725. Con vistas a garantizar la funcionalidad plena de la base de datos de la UE una vez que esté en funcionamiento, el procedimiento para su creación debe comprender el desarrollo de especificaciones funcionales por parte de la Comisión y la redacción de un informe de auditoría independiente. Al ejercer sus funciones como responsable del tratamiento de la base de datos de la UE, la Comisión debe tener en cuenta los riesgos de ciberseguridad. Con el fin de maximizar la disponibilidad y el uso de la base de datos de la UE por parte del público, la base de datos de la UE y la información facilitada a través de ella deben cumplir los requisitos establecidos en la Directiva (UE) 2019/882.

(132) Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden plantear riesgos específicos de suplantación o engaño, con independencia de si cumplen las condiciones para ser considerados como de alto riesgo o no. Por consiguiente, el uso de estos sistemas debe estar sujeto, en determinadas circunstancias, a obligaciones de transparencia específicas, sin perjuicio de los requisitos y las obligaciones aplicables a los sistemas de IA de alto riesgo y a excepciones específicas a fin de tener en cuenta las necesidades especiales de la garantía del cumplimiento del Derecho.

organo edo organismo publikoak direnean, datu-base horretan erregistratu behar dira, eta erabiltzea aurreikusten duten sistema hautatu. Hedapenaren gainerako arduradunek ere erregistro hori egiteko aukera izan behar dute, hala nahi izanez gero. EBren datu-basearen atal horrek sarbide publikokoa eta doakoa izan behar du; informazioan erraz nabigatzeko modua eman behar du, eta makinak erraz ulertzeko eta irakurtzeko modukoa izan. Era berean, EBren datu-base horrek erraz erabiltzeko modukoa izan behar du; esaterako, bilaketak egiteko funtzionalitateak eman behar ditu, baita gako-hitzak erabiliz ere, herritarrek erraz topa dezaten, adibidez, zer informazio aurkeztu behar den arrisku handiko AA-sistemak erregistratzeko, edo zer egin behar den arrisku handiko AA-sistemak zerrendatzen dituen erregelamendu honetako eranskin batean jasota dauden arrisku handiko AA-sistemen erabilera-kasuetan. Arrisku handiko AA-sistemetan egindako funtsezko aldaketa guztiak ere erregistratu beharko dira EBren datu-basean. Zuzenbidea betearazteko eta migrazioa, asiloa eta muga-kontrola kudeatzeko arrisku handiko AA-sistemen kasuan, erregistro-betekizunak EBren datu-basearen atal seguru eta ez-publiko batean bete behar dira. Atal horretarako sarbidea honako hauek izango dute bakar-bakarrik: Batzordeak eta merkatua zaintzeko agintaritzek —datu-basetik dagokien atal nazionalen—. Azpiegitura kritikoen arloko arrisku handiko AA-sistemak, berriz, nazio-mailan bakarrik erregistratu behar dira. Batzordeak izan behar du EBren datu-basearen tratamenduaren arduraduna, (EB) 2018/1725 Erregelamenduarekin bat etorrita. EBren datu-baseak abian jarritakoan erabateko funtzionaltasuna duela bermatzeko, datu-basea sortzeko prozesuan, Batzordearen zehaztapen funtzionalak garatu behar dira eta auditoretza independente batek txostena idatzi behar du. Batzordeak, EBren datu-basearen tratamenduaren arduraduna den aldetik, bere eginkizunak betetzen dituenean, kontuan izan behar ditu zibersegurtasuneko arriskuak. Herritarrek EBren datu-basea ahalik eta eskuren izan eta ahalik eta gehien erabil dezaten, datu-baseak berak eta haren bitartez ematen den informazioak (EB) 2019/882 Zuzentarauan ezarrita dauden betekizunak bete behar dituzte.

(132) Pertsona fisikoekin elkarreraginean izatea edo edukiak sortzea helburu duten AA-sistema batzuek ordezen- edo engainu-arrisku zehatz batzuk ekar ditzakete, arrisku handikotzat jotzeko baldintzak bete zein ez. Horregatik, bada, sistema horiek erabiltzeko orduan, egoera jakin batzuetan, gardentasun-betebehar zehatz batzuk bete behar dira, hartatik eragotzi gabe arrisku handiko AA-sistemei aplikatzekoak zaizkien betekizunak eta betebeharrak, eta salbuespen zehatzei lotuta zuzenbidea betearazteko beharrian bereziak kontuan hartze aldera. AA-sistema batekin elkarreraginean diren pertsona fisikoei berariaz



En particular, es preciso comunicar a las personas físicas que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física normalmente informada y razonablemente atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Al aplicar dicha obligación, deben tenerse en cuenta las características de las personas físicas pertenecientes a colectivos vulnerables debido a su edad o discapacidad en la medida en que el sistema de IA esté destinado a interactuar también con dichos colectivos. Además, es preciso notificar a las personas físicas cuando estén expuestas a sistemas de IA que, mediante el tratamiento de sus datos biométricos, puedan determinar o inferir sus emociones o intenciones o incluirlas en categorías específicas. Estas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de ojos, los tatuajes, los rasgos personales, el origen étnico o las preferencias e intereses personales. Esta información y estas notificaciones deben facilitarse en formatos accesibles a las personas con discapacidad.

(133) Una diversidad de sistemas de IA puede generar grandes cantidades de contenidos sintéticos que para las personas cada vez es más difícil distinguir del contenido auténtico generado por seres humanos. La amplia disponibilidad y las crecientes capacidades de dichos sistemas tienen importantes repercusiones en la integridad del ecosistema de la información y en la confianza en este, haciendo surgir nuevos riesgos de desinformación y manipulación a escala, fraude, suplantación de identidad y engaño a los consumidores. En vista de estos efectos, el rápido desarrollo tecnológico y la necesidad de nuevos métodos y técnicas para asegurar la trazabilidad del origen de la información, procede exigir a los proveedores de tales sistemas que integren soluciones técnicas que permitan marcar, en un formato legible por máquina, y detectar que el resultado de salida ha sido generado o manipulado por un sistema de IA y no por un ser humano. Dichas técnicas y métodos deben ser lo suficientemente fiables, interoperables, eficaces y sólidos, en la medida en que sea técnicamente viable, teniendo en cuenta las técnicas disponibles o una combinación de dichas técnicas, como marcas de agua, identificación de metadatos, métodos criptográficos para demostrar la procedencia y la autenticidad del contenido, métodos de registro, impresiones dactilares u otras técnicas, según proceda. A la hora de aplicar esta obligación, los proveedores también deben tener en cuenta las especificidades y las limitaciones de los diferentes tipos de contenidos y los avances tecnológicos y del mercado pertinentes en ese ámbito, tal como se refleja en el estado de la técnica generalmente reconocido. Dichas técnicas y métodos pueden implantarse a nivel de sistema de IA o a nivel de modelo de IA, incluidos modelos de IA de uso general que generan contenidos, facilitando así el cumplimiento

jakinarazi behar zaie hala ari direla, salbu eta agerikoa denean, pertsona fisiko aski informatu, erne eta zoli baten ikuspegitik, erabilera-testuingurua eta inguruabarrak kontuan hartuta. Betebehar hori aplikatzean, bereziki hartu behar dira kontuan adinagatik edo desgaitasunagatik kolektibo kalteberetakoak diren pertsonen ezaugarriak, AA-sistema kolektibo horiekin elkarreraginean egotera bideratuta dagoen heinean. Gainera, pertsona fisikoak beren datu biometrikoak tratatzen dituen AA-sistema batekiko esposiziopean daudenean eta sistema horrek pertsonen emozioak edo asmoak zehaztu edo ondorioztatu eta kategoria jakinetan sailkatu ditzakeenean, beharrezkoa da egoera horren berri ematea pertsona horiei. Kategoría espezifiko horiek askotariko alderdietan oinarritu daitezke: sexua, adina, ile-kolorea, begi-kolorea, tatuajeak, bereizgarri pertsonalak, jatorri etnikoa edota lehenetasun eta interes pertsonalak. Informazio eta jakinarazpen horiek desgaitasuna duten pertsonentzako moduko formatu irisgarrian eman behar dira.

(133) AA-sistemen dibertsitateak eduki sintetikoen kantitate handiak sor ditzake, eta gero eta zailagoa gerta dakieke pertsonen eduki hori gizakiek sortutako benetako edukitik bereiztea. Sistema horiek hain eskuragarri egoteak eta halako ahalmena izateak ondorio garrantzitsuak ditu informazioaren ekosistemaren integritatean eta harekiko konfiantzan; izan ere, arrisku berriak sortzen ditu hainbat mailatan: eskalako desinformazioa eta manipulazioa, iruzurra, identitatearen ordezpina eta kontsumitzaileenganako engainua. Kontuan hartuta nolako eraginak dituen AAk, nolako abiadan ari den garatzen teknologia eta zer premia dagoen metodo eta teknika berriak sortzeko haien bidez informazioaren jatorriaren trazabilitatea ziurtatzeko, hornitzaileei eskatzekoa da sistema horiek soluzio teknikoak izan ditzatela markatu ahal izateko —makina batek irakurtzeko moduko formatuan— eta hauteman ahal izateko dena delako iteera-emaiza AA-sistema batek —eta ez gizaki batek— sortua edo manipulatu dela. Teknika eta metodo horiek teknikoki ahal den bezain fidagarriak, elkarreragingarriak, efikazak eta sendoak izan behar dute, kontuan hartuta erabilgarri dauden teknikak edo teknika horien konbinazioa, hau da: ur-markak, metadatuen identifikazioa, edukiaren jatorria eta benetakotasuna egiaztatzeko metodo kriptografikoak, erregistro-metodoak, hatz-markak eta bestelako teknikak, egoki den moduan. Betebehar hori aplikatzeko orduan, hornitzaileek eduki moten berezitasunak eta mugak ere hartu behar dituzte kontuan, baita esparru horretan teknologian eta merkatuan egiten diren aurrerapenak ere, oro har aintzatetsitako teknikaren egoeran islatzen den bezala. Teknika eta metodo horiek AA-sisteman ezar daitezke edo AA-ereduan, barruan direla edukiak sortzen dituzten erabilera orokorreko AA-ereduak; horrela, AA-sistemaren ondorengo hornitzaileak errazago bete ahal



de esta obligación por parte del proveedor posterior del sistema de IA. Para garantizar la proporcionalidad, conviene prever que esta obligación de marcado no se aplique a los sistemas de IA que desempeñen una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica.

(134) Además de las soluciones técnicas utilizadas por los proveedores del sistema de IA, los responsables del despliegue que utilicen un sistema de IA para generar o manipular un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeje notablemente a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos (ultrasuplantaciones) deben también hacer público, de manera clara y distinguible, que este contenido ha sido creado o manipulado de manera artificial etiquetando los resultados de salida generados por la IA en consecuencia e indicando su origen artificial. El cumplimiento de esta obligación de transparencia no debe interpretarse como un indicador de que la utilización del sistema de IA o de sus resultados de salida obstaculiza el derecho a la libertad de expresión y el derecho a la libertad de las artes y de las ciencias, garantizados por la Carta, en particular cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, con sujeción a unas garantías adecuadas para los derechos y libertades de terceros. En tales casos, la obligación de transparencia en relación con las ultrasuplantaciones establecida en el presente Reglamento se limita a revelar la existencia de tales contenidos generados o manipulados de una manera adecuada que no obstaculice la presentación y el disfrute de la obra, también su explotación y uso normales, al tiempo que se conservan la utilidad y la calidad de la obra. Además, también conviene prever una obligación de divulgación similar en relación con el texto generado o manipulado por una IA en la medida en que se publique con el fin de informar al público sobre asuntos de interés público, a menos que el contenido generado por la IA haya sido sometido a un proceso de revisión humana o de control editorial y que una persona física o jurídica ejerza la responsabilidad editorial de la publicación del contenido.

(135) Sin perjuicio del carácter obligatorio y de la plena aplicabilidad de las obligaciones de transparencia, la Comisión podrá también fomentar y facilitar la elaboración de códigos de buenas prácticas a escala de la Unión, a fin de facilitar la aplicación eficaz de las obligaciones en materia de detección y etiquetado de contenidos generados o manipulados de manera artificial, también para apoyar disposiciones prácticas para que, según proceda, los mecanismos de detección sean accesibles y facilitar la cooperación con otros

izango du betebeharrak. Proporzionaltasuna bermatzeko, komeni da aurreikustea markatze-betebeharrak ez dela aplikatzekoa edizio estandarren lagungarritzat diharduten AA-sistemetan edo hedapenaren arduradunek emandako sarrera-datuak edo haien semantika funtsetik aldatzen ez dituzten AA-sistemetan.

(134) AA-sistemaren hornitzaileek erabilitako soluzio teknikoek gain, hedapenaren arduradunek, baldin eta AA-sistema bat erabiltzen badute irudi, audio edo bideo baten edukia sortzeko edo manipulatzeko eta irudi, audio edo bideo horrek antz nabarmena badu benetako pertsona, objektu, leku, entitate edo gertaerekin eta, ondorioz, pentsatzera eraman badezake, okerki, eduki hori benetakoa edo egiazkoa dela (faltsutze sakona), halako egoeretan argi eta garbi aditzera eman behar dute eduki hori modu artifizialean sortu edo manipulatu dela, eta, horretarako, etiketatu egin behar ditu AAK sortutako irteera-emaitzak, eta haien jatorria artifiziala dela adierazi. Gardentasun-betebeharrak hori betetzeak ez du adierazten AA-sistema edo haren irteera-emaitzak erabiltzea oztopo denik adierazpen-askatasunaren eskubiderako edo arteen eta zientzien askatasunaren eskubiderako —bi-biak Gutunean bermatuak—, bereziki eduki hori obra edo programa nabarmenki sortzaile, satiriko, artistiko, fikziozko edo antzeko baten parte denean, hirugarren batzuen eskubide eta askatasunerako berme egokiei lotuta. Halakoetan, faltsutze sakonei aurre egiteko erregelamendu honetan ezarritako gardentasun-betebeharra zera eskatzera mugatzen da: sortutako edo manipulatutako eduki horien berri ematera, halako moduan non eta ez zaion trabarik egiten obraren aurkezpenari eta hartaz gozatzeko aukerari, ezta obraren ustiapen eta erabilera normalari ere, aldi berean obraren erabilera eta kalitatea mantenduta. Gainera, AA batek sortutako edo manipulatutako testuaren kasuan, komeni da jendartearen horren berri emateko antzeko betebeharrak bat aurreikustea, testu horren helburua herritarrei interes publikoko gaien berri ematea den heinean. Salbuetsita egongo da, baldin eta AAK sortutako edukia gizakiak berrikusi badu edo edizio-kontrola igaro badu eta pertsona fisiko edo juridiko batek eduki horren argitalpen-erantzukizuna badu.

(135) Bazter utzi gabe gardentasun-betebeharrak nahitaezkoak direla eta erabateko aplikagarritasuna dutela, Batasunaren esparruan jardunbide egokien kodeak egin daitezten sustatu eta bideratu ahal izango du Batzordeak, modu eraginkorrean aplikatu daitezten artifizialki sortutako edo manipulatutako edukiak detektatzeko eta etiketatzeko arloan ezarritako betebeharrak; horren barruan, akordio praktikoa ere sustatuko dira, hala badagokio, detekzio-mekanismoak irisgarriak izan daitezten eta balio-kateko beste eragile



agentes de la cadena de valor, difundiendo los contenidos o comprobando su autenticidad y procedencia, a fin de que el público pueda distinguir efectivamente los contenidos generados por IA.

(136) Las obligaciones impuestas a los proveedores y a los responsables del despliegue de determinados sistemas de IA en el presente Reglamento destinadas a permitir que se detecte y divulgue que los resultados de salida de dichos sistemas han sido generados o manipulados de manera artificial resultan especialmente pertinentes para facilitar la aplicación efectiva del Reglamento (UE) 2022/2065. Esto se aplica en particular en lo referente a las obligaciones de los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda en línea de muy gran tamaño para detectar y mitigar los riesgos sistémicos que pueden surgir de la divulgación de contenidos que hayan sido generados o manipulados de manera artificial, en particular el riesgo de los efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, como a través de la desinformación. La exigencia de etiquetar los contenidos generados por sistemas de IA con arreglo al presente Reglamento se entiende sin perjuicio de la obligación prevista en el artículo 16, apartado 6, del Reglamento (UE) 2022/2065 para los prestadores de servicios de alojamiento de datos de tratar las notificaciones que reciban sobre contenidos ilícitos en virtud del artículo 16, apartado 1, de dicho Reglamento, y no debe influir en la evaluación y la decisión sobre el carácter ilícito del contenido de que se trate. Dicha evaluación debe realizarse únicamente con referencia a las normas que rigen la legalidad del contenido.

(137) El cumplimiento de las obligaciones de transparencia aplicables a los sistemas de IA que entran en el ámbito de aplicación del presente Reglamento no debe interpretarse como un indicador de que la utilización del sistema de IA o de sus resultados de salida es lícito en virtud del presente Reglamento o de otras disposiciones del Derecho de la Unión y de los Estados miembros, y debe entenderse sin perjuicio de otras obligaciones de transparencia aplicables a los responsables del despliegue de sistemas de IA establecidas en el Derecho de la Unión o nacional.

(138) La IA es una familia de tecnologías de rápida evolución que requiere vigilancia regulatoria y un espacio seguro y controlado para la experimentación, así como que se garantice la innovación responsable y la integración de salvaguardias éticas y medidas de reducción de riesgos adecuadas. Para conseguir un marco jurídico que promueva la innovación, resista el paso del tiempo y sea resiliente a las perturbaciones, los Estados miembros deben velar por que sus autoridades nacionales competentes establezcan al menos un

batzuekiko lankidetza bultza dadin, edukiak hedatzeko edo haien benetakotasuna eta jatorria egiaztatzeko, AAK sortutako edukiak benetan bereizi ahal izan ditzaten erabiltzaileek.

(136) AA-sistema jakin batzuen irteera-emaizak modu artifizialean sortu edo manipulatu direla hauteman eta jendartean horren berri eman ahal izateko erregelamendu honetan sistema horien hornitzaileei eta hedapenaren arduradunei ezarritako betebeharrak oso egokiak dira (EB) 2022/2065 Erregelamendua eraginkortasunez aplikatu ahal izateko. Bereziki aplikatzen da hori lineako plataforma oso handien edo lineako bilaketa-motor oso handien emailen kasuan, modu artifizialean sortu edo manipulatu diren edukiak jendartean zabaltzeak sor ditzakeen arrisku sistemikoak hautemateko eta arintzeko betebeharra duten heinean, batez ere prozesu demokratikoetan, diskurtso zibikoan eta hauteskunde-prozesuetan, baita desinformazioaren bidez ere, ondorio negatiboak —benetakoak edo aurreikusgarriak— eragiteko arriskuari begira. Erregelamendu honen arabera AA-sistemek sortutako edukiak etiketatzeak betebeharrak ez du ezertan eragozten (EB) 2022/2065 Erregelamenduaren 16.6 artikuluan aurreikusitako betebeharra, hots, datuak ostatzeko zerbitzuaren emailak eduki ez-zilegien gainean jasotzen dituzten jakinarazpenak tratatzeko duten betebeharra, erregelamendu horren 16.1 artikuluan arabera; betebeharrak horrek, era berean, ez du eraginik izan behar dena delako edukiaren ez-zilegitasuna aztertzeko eta horren gaineko erabakia hartzeko orduan. Ebaluazio hori egiteko, edukien legezkotasuna ezartzen duten arauak jarraituko zaie bakar-bakarrik.

(137) Erregelamendu honen aplikazio-eremuan sartzen diren AA-sistemei aplikatu beharreko gardentasun-betebeharrak betetzeak ez du adierazten AA-sistemaren edo haren irteera-emaizten erabilera zilegia denik erregelamendu honen edo Batasuneko eta estatu kideetako zuzenbideko beste xedapen batzuen arabera; betebeharrak horrek, bestalde, ez ditu ezertan eragozten Batasuneko zuzenbidean edo zuzenbide nazionalan ezarritako AA-sistemen hedapenaren arduradunei aplikatu beharreko bestelako gardentasun-betebeharrak batzuk.

(138) AA bilakaera azkarreko teknologien familia da, eta arauzko zaintza eta esperimentaziorako espazio seguru eta kontrolatua behar ditu; beharrezkoa du, halaber, bermatzea berrikuntza arduratsua egiten dela eta egokiro txertatzen direla behar diren babes etikoak eta arriskuak murrizteko neurriak. Esparru juridiko proposatutako bat lortzeko —berrikuntza sustatzen duena, denboraren joana ondo kudeatzen duena eta gorabeheren aurrean erresilientea dena—, estatu kideek bereziki zaindu behar dute beren agintaritzak nazional eskudunek



espacio controlado de pruebas para la IA a escala nacional que facilite el desarrollo y la prueba de sistemas de IA innovadores bajo una estricta vigilancia regulatoria antes de su introducción en el mercado o puesta en servicio. Los Estados miembros también podrían cumplir esta obligación participando en los espacios controlados de pruebas ya existentes o estableciendo un espacio de pruebas conjuntamente con las autoridades competentes de uno o varios Estados miembros, en la medida en que dicha participación proporcione un nivel de cobertura nacional equivalente para los Estados miembros participantes. Los espacios controlados de pruebas para la IA podrían establecerse de forma física, digital o híbrida y podrán albergar productos tanto físicos como digitales. Las autoridades que los creen deben también garantizar que los espacios controlados de pruebas para la IA dispongan de recursos adecuados para su funcionamiento, incluidos recursos financieros y humanos.

(139) Los espacios controlados de pruebas para la IA deben tener los objetivos de impulsar la innovación en el ámbito de la IA estableciendo un entorno de experimentación y prueba controlado en la fase de desarrollo y previa a la comercialización, con vistas a garantizar que los sistemas de IA innovadores cumplan lo dispuesto en el presente Reglamento y en otras disposiciones pertinentes del Derecho de la Unión y nacional. Además, los espacios controlados de pruebas para la IA deben tener por objeto mejorar la seguridad jurídica de que gozan los innovadores y favorecer la vigilancia de las autoridades competentes y su entendimiento de las oportunidades, los riesgos emergentes y las consecuencias del uso de la IA, de facilitar el aprendizaje normativo de las autoridades y empresas, también con vistas a futuras adaptaciones del marco jurídico, de apoyar la cooperación y el intercambio de mejores prácticas con las autoridades que intervienen en el espacio controlado de pruebas y de acelerar el acceso a los mercados, también eliminando los obstáculos para las pequeñas y medianas empresas, incluidas las empresas emergentes. Los espacios controlados de pruebas para la IA deben estar ampliamente disponibles en toda la Unión y debe prestarse especial atención a que sean accesibles para las pymes, incluidas las empresas emergentes. La participación en el espacio controlado de pruebas para la IA debe centrarse en cuestiones que generen inseguridad jurídica y que, por lo tanto, dificulten que los proveedores y los proveedores potenciales innoven y experimenten con la IA en la Unión y contribuir a un aprendizaje normativo basado en datos contrastados. Por consiguiente, la supervisión de los sistemas de IA en el espacio controlado de pruebas para la IA debe comprender su desarrollo, entrenamiento, prueba y validación antes de su introducción en el mercado o puesta en servicio, así

AArako proba-ingurune arautu bat ezartzen dutela, gutxienez, nazio-mailan AA-sistema berritzaileak garatzeko eta probatzeko, arau zorrotzen pean, sistema merkatuan jarri edo zerbitzuan ipini aurretik. Estatu kideek ere betebeharrak hori bete ahal izango lukete, dagoeneko abian diren proba-ingurune arautuetan parte hartuz edo estatu kide bateko edo gehiagoko agintaritzak eskudunekin bat eginda elkarrekin proba-ingurune bat ezarriz; parte-hartze horrek, betiere, pareko estaldura-maila eman beharko du parte hartzen duten estatu kide guztietan. AArako proba-ingurune arautuak modu fisiko, digital zein hibridoan ezar daitezke, eta produktu fisikoak nahiz digitalak barne har ditzakete. AArako proba-ingurune arautu horiek sortzen dituzten agintaritzek bermatu beharra dute, orobat, ingurune horiek jardunerako baliabide egokiak dituztela, baliabide finantzarioak eta giza baliabideak barne.

(139) AArako proba-ingurune arautuek helburutzat hartu behar dute berrikuntza sustatzea AAren eremuan, esperimentazio- eta proba-ingurune arautu bat ezarrita sistemaren garapen fasean, merkaturatu aurretik, hartara bermatu ahal izango baita AA-sistema berritzaileak betetzen dutela erregelamendu honetan ezarritakoa eta Batasuneko zuzenbidean zein zuzenbide nazionalako beste xedapen batzuetan ezarritakoa. AArako proba-ingurune arautuen helburu izan behar du, orobat, hobetzea eraberritzaileek duten segurtasun juridikoa eta bidea ematea agintaritzak eskudunek zaintza egokia egiteko eta ulertzeko AAren erabilerak nolako aukerak, arrisku emergenteak eta ondorioak ekartzen dituen; horrekin batera, lagungarriak izan behar dute, berebat, agintariek eta enpresek errazago ikas ditzaten arauak —baita etorkizunean esparru juridikoa egokitu behar bada ere—, eta proba-ingurune arautuan esku hartzen duten agintaritzekiko lankidetzak eta jardunbide egokiak trukea babestu behar dute, bai, halaber, merkatuetarako sarbidea bizkortu ere, besteak beste oztupoak ezabatuz enpresa txiki eta ertainei begira —enpresa emergenteak ere barne—. AArako proba-ingurune arautuek luze-zabal egon behar dute eskuragarri Batasun osoan, eta bereziki irisgarri izan behar dute ETEentzat —enpresa emergenteak ere barne—. AArako proba-ingurune arautuko parte-hartzaileak segurtasun juridiko eza eragiten duten alderdiak hartu behar ditu oinarritzat, alderdi horiek oztopagarri izaten baitira hornitzaileentzat eta hornitzaile potentzialentzat Batasunaren barruan AArekin berrikuntzan jarduteko eta esperimentatzeko, eta lagungarria izan behar du datu egiaztatuetan funtsatutako arau-ikaskuntza garatzeko. Horrenbestez, AA-sistemak AArako proba-ingurune arautuan berrikusten direnean, alderdi hauek hartu behar dira aintzat: sistemak merkatuan jarri edo zerbitzuan ipini aurretik izan duen garapena, entrenamendua, proba eta



como el concepto de «modificación sustancial» y su materialización, que puede hacer necesario un nuevo procedimiento de evaluación de la conformidad. Cualquier riesgo significativo detectado durante el proceso de desarrollo y prueba de estos sistemas de IA debe dar lugar a la adopción de medidas de reducción adecuadas y, en su defecto, a la suspensión del proceso de desarrollo y prueba. Cuando proceda, las autoridades nacionales competentes que establezcan espacios controlados de pruebas para la IA deben cooperar con otras autoridades pertinentes, incluidas las que supervisan la protección de los derechos fundamentales, y pueden dar cabida a otros agentes del ecosistema de la IA, como organizaciones de normalización nacionales o europeas, organismos notificados, instalaciones de ensayo y experimentación, laboratorios de investigación y experimentación, centros europeos de innovación digital y organizaciones de partes interesadas y de la sociedad civil pertinentes. Para garantizar una aplicación uniforme en toda la Unión y conseguir economías de escala, resulta oportuno establecer normas comunes para la creación de espacios controlados de pruebas para la IA, así como un marco para la cooperación entre las autoridades pertinentes implicadas en la supervisión de dichos espacios. Los espacios controlados de pruebas para la IA establecidos en virtud del presente Reglamento deben entenderse sin perjuicio de otros actos legislativos que permitan el establecimiento de otros espacios controlados de pruebas encaminados a garantizar el cumplimiento de actos legislativos distintos del presente Reglamento. Cuando proceda, las autoridades competentes pertinentes encargadas de esos otros espacios controlados de pruebas deben ponderar las ventajas de utilizarlos también con el fin de garantizar el cumplimiento del presente Reglamento por parte de los sistemas de IA. Previo acuerdo entre las autoridades nacionales competentes y los participantes en el espacio controlado de pruebas para la IA, las pruebas en condiciones reales también podrán gestionarse y supervisarse en el marco del espacio controlado de pruebas para la IA.

(140) El presente Reglamento debe proporcionar la base jurídica para que los proveedores y los proveedores potenciales en el espacio controlado de pruebas para la IA utilicen datos personales recabados para otros fines para desarrollar determinados sistemas de IA en favor del interés público en el espacio controlado de pruebas para la IA, únicamente en determinadas condiciones, de conformidad con el artículo 6, apartado 4, y el artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y los artículos 5, 6 y 10 del Reglamento (UE) 2018/1725, y sin perjuicio de lo dispuesto en el artículo 4, apartado 2, y el artículo 10 de la Directiva (UE) 2016/680. Siguen siendo aplicables las demás obligaciones de los responsables del tratamiento y los derechos de los interesados en virtud del Reglamento (UE) 2016/679, el Reglamento (UE)

balioztatzea, bai, halaber, «funtsezko aldaketaren» kontzeptua eta kontzeptu hori hezurmamitzeko modua, adostasuna ebaluatzeko beste prozedura bat behar izatea eragin baitezake. AA-sistema horiek garatzeko eta probatzeko prozesuan arrisku adierazgarriren bat hautemanez gero, arriskua murrizteko neurriak hartu behar dira, edo, bestela, garapen- eta proba-prozesua eten. Behar denean, AArako proba-ingurune arautuak ezartzen dituzten agintaritza nazional eskudunek lankidetzan jardun behar dute egoki diren beste agintaritza batzuekin —barnean direla oinarritzko eskubideen babesa ikuskatzen dihardutenak—, eta AAren ekosistemako beste eragile batzuk ere onartu ahal izango dituzte, hala nola normalizazio-antolakunde nazionalak edo europarrak, organismo jakinaraziak, saiakuntza- eta esperimentazio-instalazioak, ikerketa- eta esperimentazio-laborategiak, berrikuntza digitaleko Europako guneak eta alderdi interesdunen eta gizarte zibilaren antolakundeak. Batasun osoan berdin aplikatzen dela bermatzeko eta eskala-ekonomiak lortzeko, bidezkoa da arau komunak ezartzea AArako proba-ingurune arautuak sortzeko, bai eta lankidetzarako esparru bat ere gune horiek ikuskatzeko prozesuan partaide diren agintaritzek elkarrekin jarduteko. Erregelamendu honen arabera ezarritako AArako proba-ingurune arautuek ez dituzte eragotziko beste lege-egintza batzuk, bide ematen dutenak erregelamendu honetaz bestelako lege-egintzak betetzen direla bermatzen duten beste proba-ingurune arautu batzuk ezartzeko. Egoki denean, beste proba-ingurune arautu horien ardura duten agintaritza eskudunen egitekoa izango da neurtzea ea proba-ingurune horien erabilerak zer-nolako abantailak dakartzan erregelamendu hau betetzen dela bermatzeko. Agintaritza nazional eskudunen eta AArako proba-ingurune arautuko parte-hartzaileen artean aurrez hala adostuta, baldintza errealeko probak AArako proba-ingurune arautuan ere kudeatu eta ikuskatu ahal izango dira.

(140) Erregelamendu honek oinarri juridikoa eman behar du AArako proba-ingurune arautuan diharduten hornitzaileek eta hornitzaile potentzialek modua izan dezaten beste helburu batzuetarako bildutako datu pertsonalak AArako proba-ingurune arautuan interes publikoaren aldeko AA-sistema jakin batzuk garatzeko erabili ahal izateko, egoera zehatz batzuetan bakar-bakarrak, bat etorrita (EB) 2016/679 Erregelamenduaren 6.4 artikuluekin eta 9.2 artikuluko g) letrarekin eta (EB) 2018/1725 Erregelamenduaren 5., 6. eta 10. artikuluekin, eta kalterik egin gabe (EB) 2016/680 Zuzentarauaren 4.2 artikuluan eta 10. artikuluan xedatutakoari. Tratamenduaren arduradunen gainerako betebeharrak eta interesdunen eskubideak aplikagarriak izaten jarraitzen dute (EB) 2016/679 Erregelamenduaren, (EB) 2018/1725



2018/1725 y la Directiva (UE) 2016/680. En particular, el presente Reglamento no debe ofrecer una base jurídica en el sentido del artículo 22, apartado 2, letra b), del Reglamento (UE) 2016/679 y del artículo 24, apartado 2, letra b), del Reglamento (UE) 2018/1725. Los proveedores y los proveedores potenciales en el espacio controlado de pruebas para la IA deben proporcionar las garantías adecuadas y cooperar con las autoridades competentes, también siguiendo sus indicaciones y actuando con rapidez y de buena fe para mitigar adecuadamente cualquier riesgo considerable para la seguridad, la salud y los derechos fundamentales que se detecte y pueda surgir durante el desarrollo, las pruebas y la experimentación en dicho espacio.

(141) A fin de acelerar el proceso de desarrollo e introducción en el mercado de los sistemas de IA de alto riesgo enumerados en un anexo del presente Reglamento, es importante que los proveedores o proveedores potenciales de dichos sistemas también puedan beneficiarse de un régimen específico para probar dichos sistemas en condiciones reales, sin participar en un espacio controlado de pruebas para la IA. No obstante, en tales casos, teniendo en cuenta las posibles consecuencias de dichas pruebas para las personas físicas, debe garantizarse que el Reglamento establezca garantías y condiciones adecuadas y suficientes para los proveedores o proveedores potenciales. Estas garantías deben incluir, entre otras cosas, la solicitud del consentimiento informado de las personas físicas para participar en pruebas en condiciones reales, salvo en lo que respecta a la garantía del cumplimiento del Derecho cuando intentar obtener el consentimiento informado impediría que se probara el sistema de IA. El consentimiento de los sujetos para participar en tales pruebas en virtud del presente Reglamento es distinto del consentimiento de los interesados para el tratamiento de sus datos personales con arreglo al Derecho pertinente en materia de protección de datos y se entiende sin perjuicio de este. También es importante reducir al mínimo los riesgos y permitir la supervisión por parte de las autoridades competentes y, por tanto, exigir a los proveedores potenciales que presenten a la autoridad de vigilancia del mercado competente un plan de la prueba en condiciones reales, registren la prueba en las secciones específicas de la base de datos de la UE, sin perjuicio de algunas excepciones limitadas, establezcan limitaciones sobre el período durante el que puede llevarse a cabo la prueba y exijan garantías adicionales para las personas pertenecientes a determinados colectivos vulnerables, así como un acuerdo por escrito que defina las funciones y responsabilidades de los proveedores potenciales y de los responsables del despliegue y una supervisión eficaz por parte de personal competente que intervenga en la prueba en condiciones reales. Además, conviene prever garantías

Erregelamenduaren eta (EB) 2016/680 Zuzentarauaren arabera. Zehazki, erregelamendu honek ez du oinarri juridikorik eman behar (EB) 2016/679 Erregelamenduaren 22.2 artikulua b) letraren eta 2018/1725 (EB) Erregelamenduaren 24.2 artikulua b) letraren zentzuan. AArako proba-ingurune arautuko hornitzaileek eta hornitzaile potentzialak berme egokiak eman behar dituzte, eta agintaritza eskudunekin lankidetzan aritu behar dute, haien jarraibideen arabera eta azkar eta fede onez jardunda, egokiro leuntzeko ingurune horretan AA garatzen, probatzen eta esperimentatzen den bitartean segurtasunaren, osasunaren eta oinarrizko eskubideen esparruan hautematen diren eta sor daitezkeen arrisku nabarmen guztiak.

(141) Erregelamendu honen eranskin batean zerrendatutako arrisku handiko AA-sistemak garatzeko eta merkatuan jartzeko prozesua bizkortzeko, garrantzitsua da sistema horien hornitzaileek edo hornitzaile potentzialak ere araubide berezi bat izatea sistema horiek egoera errealetan probatu ahal izateko, AArako proba-ingurune arautu batean parte hartu gabe. Dena dela, halakoetan, proba horiek pertsona fisikoei ekar diezazkieketen ondorioak kontuan hartuta, berariaz bermatu behar da erregelamenduak berme eta baldintza egokiak eta nahikoak ezarriko dituela hornitzaileentzat eta hornitzaile potentzialentzat. Berme horien barruan jaso behar da, besteak beste, pertsona fisikoei baldintza errealeko probetan parte hartzeko egin beharreko adostasun informatuaren eskaera, salbu eta zuzenbidea betearazteari dagokionez baldin eta adostasun informatua lortzen saiatzeak AA-sistema probatzea oztopatuko balu. Erregelamendu honen arabera parte-hartzaileek proba horietan parte hartzeko baimena ez dator bat interesdunek beren datu pertsonalak datuen babesaren arloko zuzenbide egokiaren arabera tratatzeko emandako adostasunarekin, hargatik erregelamendu hau eragotzi gabe. Garrantzitsua da, halaber, arriskuak ahal beste murriztea eta agintaritza eskudunei ikuskapena egiteko bide ematea; hortaz, garrantzitsua da hornitzaile potentzialei betebeharrak batzuk exijitzea, hots: baldintza errealeko probaren plan bat aurkeztea merkatua zaintzeko agintaritzari; EBren datu-basetik dagokien atalean erregistratzea proba hori, zenbait salbuespen mugatu gorabehera; proba egiteko aldia mugatzea, eta berme gehiago eskatzea kolektibo kaltebera jakin batzuetako pertsonen begira, bai, orobat, idatzizko akordio bat egitea hornitzaile potentzialen eta hedapenaren arduradunen eginkizunak eta erantzukizunak zehazteko eta baldintza errealeko proban parte hartzen duten langile eskudunen ikuskapen eraginkorra gauzatzea. Horrez gain, komeni da berme osagarri batzuk ere aurreikustea, ziurtatzeko AA-sistemaren iragarpenak, gomendioak eta erabakiak eraginkortasunez leheneratu daitezkeela eta datu pertsonalak egokiro babesten direla, baita ezabatu ere,



adicionales para asegurarse de que sea posible revertir efectivamente y descartar las predicciones, recomendaciones o decisiones del sistema de IA y de que los datos personales se protejan y se supriman cuando los sujetos retiren su consentimiento a participar en la prueba, sin perjuicio de sus derechos como interesados en virtud del Derecho de la Unión en materia de protección de datos. Por lo que respecta a la transferencia de datos, conviene también prever que los datos recopilados y tratados a efectos de las pruebas en condiciones reales solo deben transferirse a terceros países cuando existan garantías adecuadas y aplicables con arreglo al Derecho de la Unión, en particular, de conformidad con las bases para la transferencia de datos personales previstas en el Derecho de la Unión en materia de protección de datos y, en lo referente a los datos no personales, existan garantías adecuadas con arreglo al Derecho de la Unión, como los Reglamentos (UE) 2022/868 (42) y (UE) 2023/2854 (43) del Parlamento Europeo y del Consejo.

(142) A fin de garantizar que la IA conduzca a resultados positivos desde el punto de vista social y medioambiental, se anima a los Estados miembros a que respalden y promuevan la investigación y el desarrollo de soluciones de IA en apoyo a tales resultados, como soluciones basadas en la IA para aumentar la accesibilidad para las personas con discapacidad, atajar desigualdades socioeconómicas o cumplir los objetivos en materia de medio ambiente, asignando recursos suficientes, incluidos fondos públicos y de la Unión, y, cuando proceda y siempre que se cumplan los criterios de admisibilidad y selección, teniendo en consideración especialmente proyectos que persigan tales objetivos. Dichos proyectos deben basarse en el principio de cooperación interdisciplinaria entre desarrolladores de IA, expertos en desigualdad y no discriminación, en accesibilidad y en derechos del consumidor, medioambientales y digitales, así como representantes del mundo académico.

(143) Para promover y proteger la innovación, es importante tener en particular consideración los intereses de las pymes, incluidas las empresas emergentes, que sean proveedores o responsables del despliegue de sistemas de IA. A tal fin, los Estados miembros deben desarrollar iniciativas en materia de concienciación y comunicación de información, entre otros aspectos, dirigidas a dichos operadores. Los Estados miembros deben proporcionar a las pymes, incluidas las empresas emergentes, que tengan un domicilio social o una sucursal en la Unión, un acceso prioritario a los espacios controlados de pruebas para la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección y sin impedir que otros proveedores y proveedores potenciales accedan a los espacios controlados de pruebas, siempre que se cumplan las mismas condiciones y

parte-hartzaileek proban parte hartzeko onespenez kenduz gero; hori guztia betiere kalterik egin gabe datuen babesaren arloan Batasuneko zuzenbideak xedatutakoaren arabera parte-hartzaileek interesdun modura dituzten eskubideei. Datuen transferentziaren arloan, komenigarria da aurreikustea ezen, baldintza errealeko probarako bildutako eta tratatutako datuak hirugarren herrialdeetara transferitu ahal izateko, ezinbestekoa dela, batetik, Batasuneko zuzenbidearen araberako bermeak egotea —benetako berme aplikagarriak—, bereziki bat etorrita Batasuneko zuzenbideak datuen babesaren arloan xedatutakoaren arabera datu pertsonalen transferentziarako aurreikusitako oinarriekin, eta, bestetik, datu ez-pertsonalen arloan, berme egokiak egotea, bat etorrita Batasuneko zuzenbidearekin —hor dira Europako Parlamentuaren eta Kontseiluaren (EB) 2022/868 Erregelamendua (42) eta (EB) 2023/2854 Erregelamendua(43)—.

(142) AAk emaitza onak eman ditzan gizartearen eta ingurumenaren ikuspegitik, bultza egiten zaie estatu kideei AA-soluzioak ikertzeko eta garatzeko ekimenak babestu eta sustatu ditzaten halako emaitzak lortze aldera: adibidez, desgaitasuna duten pertsonen irisgarritasuna hobetzeko soluzioak, desberdinkeria sozioekonomikoak eragoztekoak edota ingurumenaren arloko helburuak betetzekoak. Eta dei egiten zaie horretarako nahikoa baliabide ezar ditzaten —funts publikoak eta Batasuneko funtsak barne— eta, egoki denean eta onargarritasun- eta hautespen-irizpideak betetzen direnean, bereziki kontuan har ditzaten helburu horiek dituzten proiektuak. Proiektu horiek diziplinarteko kooperazioaren printzipioa hartu behar dute ardatz, elkarrekin lankidetzan aritu daitezen AA-garatzailleak, hainbat arlotako adituak —hala nola, desberdinkeria eta diskriminazio-ezaren arlokoak eta kontsumitzailearen eskubideen, ingurumen-eskubideen eta eskubide digitalen arloetakoak— eta mundu akademikoaren ordezkariak.

(143) Berrikuntza sustatzeko eta babesteko, garrantzitsua da oso kontuan hartzea AA-sistemen hornitzaile edo hedapenaren arduradun diren ETEen interesak —enpresa emergenteak ere barnean direla—. Horretarako, estatu kideek kontzientziazioa eta informazioaren komunikazioa sustatzeko ekimenak garatu behar dituzte, operadore horiei zuzenduta, besteak beste. Estatu kideek AArako proba-ingurune arautuetara sartzeko lehentasunezko sarbidea emango diete egoitza sozial bat edo sukurtsal bat Batasunean duten ETEei —enpresa emergenteak barne—, betiere onargarritasun-baldintzak eta hautaketa-irizpideak betetzen badituzte eta eragotzi gabe beste hornitzaile edo hornitzaile potentzial batzuek proba-ingurune arautuetara sartu ahal izatea, baldintza eta irizpide berberak betez gero. Estatu kideek abian dauden kanalak erabili behar dituzte, eta, egoki denean,



critérios. Los Estados miembros deben utilizar los canales existentes y establecer, cuando proceda, nuevos canales de comunicación específicos con las pymes, incluidos las empresas emergentes, los responsables del despliegue, otros innovadores y, cuando proceda, las autoridades públicas locales, para apoyar a las pymes durante toda su trayectoria de desarrollo ofreciendo orientaciones y respondiendo a las preguntas sobre la aplicación del presente Reglamento. Cuando proceda, estos canales deben trabajar juntos para crear sinergias y garantizar la homogeneidad de sus orientaciones para las pymes, incluidas las empresas emergentes, y los responsables del despliegue. Además, los Estados miembros deben fomentar la participación de las pymes y otras partes interesadas pertinentes en los procesos de desarrollo de la normalización. Asimismo, los organismos notificados deben tener en cuenta las necesidades y los intereses específicos de los proveedores que sean pymes, incluidas las empresas emergentes, cuando establezcan las tasas aplicables a las evaluaciones de la conformidad. La Comisión debe evaluar periódicamente los costes de la certificación y el cumplimiento para las pymes, incluidas las empresas emergentes, a través de consultas transparentes, y debe trabajar con los Estados miembros para reducir dichos costes. Por ejemplo, los costes de traducción ligados a la documentación obligatoria y a la comunicación con las autoridades pueden ser considerables para los proveedores y otros operadores, en particular para los de menor tamaño. En la medida de lo posible, los Estados miembros deben velar por que una de las lenguas en las que acepten que los proveedores presenten la documentación pertinente y que pueda usarse para la comunicación con los operadores sea ampliamente conocida por el mayor número posible de responsables del despliegue transfronterizos. A fin de abordar las necesidades específicas de las pymes, incluidas las empresas emergentes, la Comisión debe proporcionar modelos normalizados para los ámbitos regulados por el presente Reglamento, previa solicitud del Consejo de IA. Además, la Comisión debe complementar los esfuerzos de los Estados miembros proporcionando una plataforma única de información con información fácil de utilizar sobre el presente Reglamento para todos los proveedores y responsables del despliegue, organizando campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento y evaluando y fomentando la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA. Las medianas empresas que hace poco se consideraban pequeñas empresas en el sentido del anexo de la Recomendación 2003/361/CE de la Comisión (44) deben tener acceso a esas medidas de apoyo, ya que dichas nuevas medianas empresas a veces pueden carecer de los recursos jurídicos y la formación necesarios para

komunikazio-kanal zehatzak ireki, harremanetan izateko bai ETEekin —enpresa emergenteak barne—, bai hedapenaren arduradunekin, baita beste eraberritzaile batzuekin eta, behar denean, tokian tokiko agintaritzak publikoekin ere, laguntza emateko ETEei haien garapen-ibilbide guztian barrena, erregelamendu hau aplikatzeko orduan sortzen zaizkien galderei erantzunez eta orientazioa emanez. Kanal horiek, egoki denean, elkarrekin lan egin behar dute sinergiak sortzeko eta horrekin batera bermatzeko homogeneoak direla ETEei —enpresa emergenteak barne— eta hedapenaren arduradunei ematen zaizkien orientabideak. Estatu kideek, bestalde, bultzada eman behar dute ETEek eta beste alderdi interesdun egoki batzuek normalizazioaren garapen-prozesuan parte har dezaten. Era berean, organismo jakinaraziek, adostasunaren ebaluazioari aplikatzekoak zaizkion tasak ezartzen dituztenean, kontuan izan behar dituzte hornitzaile lanetan diharduten ETEen premia eta interes zehatzak —enpresa emergenteak ere barnean direla—. Batzordeak ETEen ziurtatze- eta betetze-kostuak balioztatu behar ditu aldian-aldian —enpresa emergenteak ere barnean direla—, kontsulta gardenak eginez, eta estatu kideekin batera lan egin behar du kostu horiek murrizteko. Esaterako, nahitaezko dokumentazioa kudeatzeko eta agintaritzarekin komunikatzeko itzulpen-kostuak handiak izan daitezke hornitzaileentzat eta beste operadore batzuentzat, batez ere txikiak direnean. Estatu kideek, ahal den neurrian, bermatu behar dute hornitzaileek dokumentazioa aurkezteko balia dezaketen eta operadoreekin komunikatzeko erabil daitekeen hizkuntzetako bat luze-zabal ezaguna dela mugaz gaindi diharduten hedapenaren ahalik eta arduradun gehienen artean. ETEen premia zehatzei aurre egiteko —enpresa emergenteak ere barnean direla—, Batzordeak eredu normalizatuak eskaini behar ditu erregelamendu honetan araututako arloetarako, AA-kontseiluak aurrez hala eskatuta. Batzordeak, gainera, estatu kideen ahalegina osatzeko, informazio-plataforma bakarra eskaini behar du, haren bidez erregelamendu honi buruzko informazio erabilerraza emateko hornitzaileei zein hedapenaren arduradunei; halaber, komunikazio-kanpaina egokiak antolatuko ditu, erregelamendu honetatik sortutako betebeharren gainean sensibiltzatzeko, eta AA-sistemen gaineako kontratazio publikoaren prozeduretan jardunbide egokien bateratasuna ebaluatu eta sustatuko du. Batzordearen 2003/361/EE Gomendioaren (44) eranskinaren arabera duela gutxi arte enpresa txikitzat jotzen ziren enpresa ertainek laguntza-neurri horiek baliatzeko modua izan behar dute; izan ere, enpresa ertain berri horiek, batzuetan, ez daukate erregelamendu hau egokiro ulertu eta bete ahal izateko beharrezkoak diren baliabide juridikoak eta prestakuntza.



garantizar la comprensión y el cumplimiento adecuados del presente Reglamento.

(144) Con el fin de promover y proteger la innovación, la plataforma de IA a la carta y todos los programas y proyectos de financiación de la Unión pertinentes, como el programa Europa Digital u Horizonte Europa, ejecutados por la Comisión y los Estados miembros a escala nacional o de la Unión deben, cuando proceda, contribuir a la consecución de los objetivos del presente Reglamento.

(145) A fin de reducir al mínimo los riesgos para la aplicación derivados de la falta de conocimientos y experiencia en el mercado, y con el objetivo de facilitar que los proveedores, en particular las pymes, incluidas las empresas emergentes, y los organismos notificados cumplan las obligaciones que les impone el presente Reglamento, la plataforma de IA a la carta, los centros europeos de innovación digital y las instalaciones de ensayo y experimentación establecidos por la Comisión y los Estados miembros a escala nacional o de la Unión deben contribuir a la aplicación de este Reglamento. En concreto, la plataforma de IA a la carta, los centros europeos de innovación digital y las instalaciones de ensayo y experimentación son capaces de proporcionar a los proveedores y organismos notificados asistencia técnica y científica dentro de sus respectivas misiones y esferas de competencia.

(146) Además, a la luz del tamaño muy pequeño de algunos operadores y con el fin de garantizar la proporcionalidad en relación con los costes de innovación, conviene permitir que las microempresas cumplan una de las obligaciones más costosas, a saber, la de establecer un sistema de gestión de la calidad, de manera simplificada, lo que reduciría la carga administrativa y los costes para dichas empresas sin afectar al nivel de protección ni a la necesidad de cumplir los requisitos aplicables a los sistemas de IA de alto riesgo. La Comisión debe elaborar directrices para especificar los elementos del sistema de gestión de la calidad que las microempresas deben cumplir de esta manera simplificada.

(147) Resulta adecuado que la Comisión facilite, en la medida de lo posible, el acceso a las instalaciones de ensayo y experimentación a organismos, grupos o laboratorios establecidos o acreditados con arreglo a la legislación de armonización de la Unión pertinente y que realicen tareas en el marco de la evaluación de la conformidad de productos o dispositivos regulados por dicha legislación. Tal es el caso, en particular, en lo que respecta a los paneles de expertos, los laboratorios especializados y los laboratorios de referencia en el ámbito de los productos sanitarios, de conformidad con los Reglamentos (UE) 2017/745 y (UE) 2017/746.

(144) Berrikuntza sustatzeko eta babesteko helburuz, nahierako AA-plataforma eta Batasuneko finantzaketa-programa eta -proiektu egoki guztiak —hala nola Europa Digitala eta Europa Horizonte programak—, Batzordeak eta estatu kideek garatutakoak izanda maila nazionalean zein Batasunaren mailan, laguntza eman behar dute erregelamendu honen helburuak lortzeko, hala dagokienean.

(145) Ahal beste murrizteko ezagutza-faltagatik edo merkatuan esperientzia nahikoa ez izategatik erregelamendua aplikatzean sor daitezkeen arriskuak, eta, horrekin batera, hornitzaileek —bereziki ETEek (enpresa emergenteak barne)— eta organismo jakinaraziek egokiro bete ahal izateko erregelamendu honek ezarritako betebeharrak, beharrezkoa da nahierako AA-plataformak, berrikuntza digitaleko Europako guneek eta Batzordean eta estatu kideetan maila nazionalean zein Batasunaren mailan ezarritako saiakuntza- eta esperimentazio-instalazioek erregelamendu honen aplikazioan parte hartzea. Zehazki, nahierako AA-plataforma, berrikuntza digitaleko Europako guneak eta saiakuntza- eta esperimentazio-instalazioak gai dira laguntza teknikoa eta zientifikoa emateko hornitzaileei eta organismo jakinaraziei, nork bere misio eta eskumen-eremuen barruan.

(146) Gainera, operadore batzuen tamaina hain txikia izanik eta berrikuntza-kostuetan proportzionaltasuna bermatu asmoz, komeni da mikroenpresei aukera ematea betebeharrak garestienetako bat bete ahal izateko; alegia, kalitatea kudeatzeko sistema bat ezarri ahal izateko, modu sinplifikatuan, halako sistemek murriztu egiten baitute enpresa horien administrazio-karga, baita kostuak ere, kalte egin gabe, hala babes-mailari nola arrisku handiko AA-sistemetan aplikatzekoak diren beste betekizunak betetzeko beharrari. Batzordeak gidalerroak prestatu behar ditu kalitatea kudeatzeko sistemak zer osagai dituen zehazteko, mikroenpresek modu sinplifikatu horretan bete ahal izan ditzaten.

(147) Egokia da Batzordeak, ahal duen neurrian, saiakuntza- eta esperimentazio-instalazioetarako sarbidea eman diezaien organismoei, taldeei edo laborategiei, Batasunaren harmonizazioko legeriaren arabera ezarrita edo akreditatuta dauden heinean eta legeria horrek araututako produktu edo gailuen adostasuna ebaluatzeko zereginak betetzen dituzten heinean. Horien artean dira, zehazki, osasun-produktuen arloko aditu-panelak, laborategi espezializatuak eta erreferentziazko laborategiak, bat etorrita (EB) 2017/745 eta (EB) 2017/746 erregelamenduekin.



(148) El presente Reglamento debe establecer un marco de gobernanza que permita tanto coordinar y apoyar su aplicación a escala nacional, como desarrollar capacidades a escala de la Unión e integrar a las partes interesadas en el ámbito de la IA. La aplicación y el cumplimiento efectivos del presente Reglamento requieren un marco de gobernanza que permita coordinar y adquirir conocimientos especializados centrales a escala de la Unión. La Oficina de IA se creó mediante Decisión de la Comisión (45) y tiene como misión desarrollar conocimientos especializados y capacidades de la Unión en el ámbito de la IA y contribuir a la aplicación del Derecho de la Unión en materia de IA. Los Estados miembros deben facilitar las tareas de la Oficina de IA con vistas a apoyar el desarrollo de conocimientos especializados y capacidades a escala de la Unión y a fortalecer el funcionamiento del mercado único digital. Además, debe crearse un Consejo de IA compuesto por representantes de los Estados miembros, un grupo de expertos científicos para integrar a la comunidad científica y un foro consultivo para facilitar las aportaciones de las partes interesadas a la aplicación del presente Reglamento, a escala de la Unión y nacional. El desarrollo de conocimientos especializados y capacidades de la Unión también debe incluir la utilización de los recursos y conocimientos especializados existentes, en particular a través de sinergias con estructuras creadas en el contexto de la aplicación a escala de la Unión de otros actos legislativos y de sinergias con iniciativas conexas a escala de la Unión, como la Empresa Común EuroHPC y las instalaciones de ensayo y experimentación de IA en el marco del programa Europa Digital.

(149) Debe establecerse un Consejo de IA que facilite la aplicación fluida, efectiva y armonizada del presente Reglamento. El Consejo de IA debe reflejar los diversos intereses del ecosistema de la IA y estar formado por representantes de los Estados miembros. El Consejo de IA debe encargarse de diversas tareas de asesoramiento. Entre otras cosas, debe emitir dictámenes, recomendaciones e informes de asesoramiento o contribuir a orientaciones sobre asuntos relacionados con la aplicación de este Reglamento, también en lo que respecta la ejecución, las especificaciones técnicas o las normas existentes en relación con los requisitos previstos en el presente Reglamento, y asesorar a la Comisión y a los Estados miembros, así como a sus autoridades nacionales competentes, en cuestiones específicas vinculadas a la IA. Con el fin de dar cierta flexibilidad a los Estados miembros en la designación de sus representantes en el Consejo de IA, cualquier persona perteneciente a una entidad pública que tenga las competencias y facultades pertinentes para facilitar la coordinación a escala nacional y contribuir al cumplimiento de las funciones

(148) Erregelamendu honek gobernantza-esparru bat ezarri behar du, modua eman dezan egokiro koordinatzeko eta aplikatzeko maila nazionalen, eta Batasunaren mailan gaitasunak garatzeko, eta, horiez gain, AAren arloan interesa duten alderdiak barne hartzeko. Erregelamendu hau modu efektiboan aplikatzeko eta betetzeko, gobernantza-esparru bat behar da, aukera emango duena Batasunaren mailan ezagutza espezializatu zentralak koordinatzeko eta eskuratzeko. AA-bulegoa Batzordearen Erabakiaren (45) bidez sortu zen, helburutzat hartuta Batasunean AAren arloko ezagutza espezializatuak eta gaitasunak garatea eta Batasunak AAren arloan ezarrita duen zuzenbidea aplikatzen laguntzea. Estatu kideek laguntza eman behar dute AA-bulegoak Batasunaren barruko ezagutza espezializatuak eta gaitasunak garatzeko dituen zereginak bete ditzan eta merkatu digital bakarraren funtzionamendua indartu dezan. Gainera, AA-kontseilu bat sortu behar da, eta bertan parte hartuko dute estatu kideetako ordezkariak, aditu zientifikoen talde batek —komunitate zientifikoa ordezkatu dezan— eta kontsulta-foro batek —alderdi interesdunek ekarpenak egin ahal izan diezaizoten erregelamendu honen aplikazioari—, Batasunaren mailan zein maila nazionalen. Batasunaren ezagutza espezializatuak eta gaitasunak garatzeko, beharrezkoa da dagoeneko garatuta dauden baliabideak eta ezagutza espezializatuak erabiltzea, eta, horretarako, bereziki sinergiekin baliatzea: Batasunaren mailan beste lege-egintza batzuk aplikatzean sortutako egiturekin eratutako sinergiak zein Batasunaren mailan arlo honi lotutako ekimenekin eratutako sinergiak, hala nola EuroHPC Enpresa Komuna eta Europa Digitalaren programaren esparruan AArekin saiakuntzak eta esperimenduak egiteko instalazioak.

(149) AA-kontseilu bat ezarri behar da, erregelamendu hau modu arin, eraginkor eta harmonizatuan aplikatu ahal izateko. AA-kontseiluak AAren ekosistemaren interesak islatu behar ditu, eta estatu kideetako ordezkariak osatu behar dute. Askotariko aholkularitzak egin behar ditu AA-kontseiluak. Besteak beste, irizpenak, gomendioak eta aholkularitza-txostenak egin behar ditu, eta orientazioa eman, bai erregelamendu honen aplikazioarekin lotutako gaiei buruz, bai erregelamendu honetan aurreikusitako betekizunen gaineko betearazpenari, zehaztapen teknikoei eta arauari buruz; era berean, AAri lotutako alderdi zehatzen gaineko aholkularitza eman behar die Batzordeari, estatu kideei eta agintaritzak nazional eskudunei. AA-kontseilurako ordezkariak izendatzeko orduan estatu kideei nolabaiteko malgutasuna emate aldera, entitate publiko bateko edozein kide ordezkari izendatu ahal izango da, baldin eta behar diren eskumenak eta ahalmenak baditu maila nazionalen koordinazio-lanak egin ditzan eta laguntza eman dezan AA-kontseiluak bere eginkizunak betetzeko. AA-kontseiluak bi azpitalde iraunkor ezarri behar ditu, merkatua zaintzeko



del Consejo de IA podrá ser designada representante. El Consejo de IA debe establecer dos subgrupos permanentes a fin de proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y las autoridades notificantes sobre cuestiones relacionadas, respectivamente, con la vigilancia del mercado y los organismos notificados. El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020. De conformidad con el artículo 33 de dicho Reglamento, la Comisión debe apoyar las actividades del subgrupo permanente de vigilancia del mercado mediante la realización de evaluaciones o estudios de mercado, en particular con vistas a determinar los aspectos del presente Reglamento que requieran una coordinación específica y urgente entre las autoridades de vigilancia del mercado. El Consejo de IA puede establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. El Consejo de IA también debe cooperar, según proceda, con los organismos, grupos de expertos y redes pertinentes de la Unión activos en el contexto del Derecho de la Unión pertinente, incluidos, en particular, los activos en virtud del Derecho de la Unión pertinente en materia de datos y productos y servicios digitales.

(150) Con vistas a garantizar la participación de las partes interesadas en la ejecución y aplicación del presente Reglamento, debe crearse un foro consultivo para asesorar al Consejo de IA y a la Comisión y proporcionarles conocimientos técnicos. A fin de garantizar una representación variada y equilibrada de las partes interesadas que tenga en cuenta los intereses comerciales y no comerciales y, dentro de la categoría de los intereses comerciales, por lo que se refiere a las pymes y otras empresas, el foro consultivo debe incluir, entre otros, a la industria, las empresas emergentes, las pymes, el mundo académico, la sociedad civil, en particular los interlocutores sociales, así como a la Agencia de los Derechos Fundamentales de la Unión Europea, ENISA, el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI).

(151) Para apoyar la aplicación y el cumplimiento del presente Reglamento, en particular las actividades de supervisión de la Oficina de IA en lo que respecta a los modelos de IA de uso general, debe crearse un grupo de expertos científicos formado por expertos independientes. Los expertos independientes que constituyan el grupo de expertos científicos deben seleccionarse sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA y deben desempeñar sus funciones con imparcialidad y objetividad y garantizar la confidencialidad de la información y los datos obtenidos en el ejercicio de sus

agintaritzek eta agintaritza jakinarazleek lankidetzarako eta trukerako plataforma bat izan dezaten hurrenez hurren merkatuaren zaintzarekin eta organismo jakinaraziekin lotutako gaiak joratzeko. Merkatua zaintzeko azpitalde iraunkorrak administrazio-lankidetzarako talde gisa (ADCO) jardun behar du erregelamendu honetarako, (EB) 2019/1020 Erregelamenduaren 30. artikuluan ezarritakoaren arabera. Erregelamendu horren 33. artikuluekin bat, Batzordeak babesa eman behar die merkatua zaintzeko azpitalde iraunkorren jarduerari, merkatu-ebaluazioak edo -azterlanak eginez bereziki zehazte aldera erregelamendu honetan zein alderdik eskatzen duten merkatua zaintzeko agintaritzen arteko koordinazio espezifikoa eta premiazkoa. AA-kontseiluak beste azpitalde batzuk ezar ditzake, iraunkorrak edo aldi baterakoak, dagokionaren arabera, gai espezifikoak aztertzeko. Era berean, lankidetzan aritu behar du, egoki den moduan, Batasuneko zuzenbidearen arloan diharduten Batasuneko organismo, aditu-talde eta sareekin, barruan direla bereziki Batasuneko zuzenbideak datuen eta produktu eta zerbitzu digitalen arloan zehaztutako eremuan dihardutenak.

(150) Erregelamendu honen betearazpen eta aplikazioan interesa duten alderdiek ere parte hartzen dutela bermatzeko, kontsulta-foro bat sortu behar da, AA-kontseiluari eta Batzordeari aholku emateko eta ezagutza teknikoak eskaintzeko. Interes komertzialak eta ez-komertzialak dituzten alderdi interesdunen ordezkaritza askotarikoa eta orekatua dela bermatzeko eta, interes komertzialeko kategoriaren barruan, ETEak eta beste enpresa batzuk kontuan hartuta, kontsulta-foroak honako eremu hauetako ordezkariak jaso behar ditu, besteak beste: industria, enpresa emergenteak, ETEak, mundu akademikoa, gizarte zibila —bereziki, gizarte-solaskideak—, Oinarritzko Eskubideen Agentzia (ENISA), Europako Normalizazio Komitea (CEN), Normalizazio Elektroteknikoko Europako Komitea (CENELEC) eta Telekomunikazioen Estandarizaziorako Europako Institutua (ETSI).

(151) Erregelamendu hau aplikatzen eta betearazten laguntzeko, bereziki erabilera orokorreko AA-ereduen gainean AA-bulegoak egin beharreko ikuskatze-jarduerak, aditu zientifikoen talde bat sortu behar da, aditu independenteek osatua. Aditu zientifikoen taldea osatuko duten aditu independenteak hautatzeko, Aaren arloko ezagutza zientifiko edo tekniko eguneratuak hartu behar dira oinarritzat, eta adituek inpartzialtasunez eta objektibotasunez bete behar dituzte beren eginkizunak, eta, beren eginkizunak eta jarduerak bete bitartean, eskuratutako informazioaren eta datuen konfidentzialtasuna bermatu behar dute. Erregelamendu



funciones y actividades. A fin de permitir el refuerzo de las capacidades nacionales necesarias para el cumplimiento efectivo del presente Reglamento, los Estados miembros deben poder solicitar el apoyo de los expertos que constituyan el grupo científico para sus actividades de garantía del cumplimiento.

(152) A fin de apoyar una ejecución adecuada en lo que respecta a los sistemas de IA y reforzar las capacidades de los Estados miembros, deben crearse y ponerse a disposición de los Estados miembros estructuras de apoyo a los ensayos de IA de la Unión.

(153) Los Estados miembros desempeñan un papel clave en la aplicación y ejecución del presente Reglamento. En ese sentido, cada Estado miembro debe designar al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes que se encarguen de supervisar su aplicación y ejecución. Los Estados miembros pueden decidir designar cualquier tipo de entidad pública para que desempeñe las tareas de las autoridades nacionales competentes en el sentido del presente Reglamento, de conformidad con sus características y necesidades organizativas nacionales específicas. Con el fin de incrementar la eficiencia organizativa en los Estados miembros y establecer un único punto de contacto oficial con el público y otros homólogos a escala de los Estados miembros y la Unión, cada Estado miembro debe designar una autoridad de vigilancia del mercado que actúe como punto de contacto único.

(154) Las autoridades nacionales competentes deben ejercer sus poderes de manera independiente, imparcial y objetiva, a fin de preservar los principios de objetividad de sus actividades y funciones y garantizar la aplicación y ejecución del presente Reglamento. Los miembros de estas autoridades deben abstenerse de todo acto incompatible con el carácter de sus funciones y estar sujetos a las normas de confidencialidad establecidas en el presente Reglamento.

(155) Todos los proveedores de sistemas de IA de alto riesgo deben contar con un sistema de vigilancia poscomercialización, con vistas a garantizar que puedan tener en cuenta la experiencia con el uso de esos sistemas de cara a mejorar los suyos y el proceso de diseño y desarrollo o que puedan adoptar cualquier medida correctora en el momento oportuno. Cuando proceda, la vigilancia poscomercialización debe incluir un análisis de la interacción con otros sistemas de IA, incluidos otros dispositivos y software. La vigilancia poscomercialización no debe comprender los datos operativos sensibles de los responsables del despliegue de sistemas de IA que sean autoridades garantes del cumplimiento del Derecho. Este sistema es también

hau eraginkortasunez betetzeko behar diren gaitasun nazionalak indartzeko aldera, estatu kideek talde zientifikoa osatzen duten adituen laguntza eskatzeko aukera izan behar dute, erregelamendua betetzen dela bermatzeko jardueretarako.

(152) AA-sistemei dagozkien alderdiak egokiro betearazten laguntzeko eta estatu kideen gaitasunak indartzeko, Batasuneko AA-saiakuntzei sostengua emateko egiturak sortu behar dira eta estatu kideen eskura jarri.

(153) Estatu kideek funtsezko eginkizuna dute erregelamendu hau aplikatzeko eta betearazteko orduan. Horregatik, estatu kide bakoitzak gutxienez agintaritza jakinarazle bat eta merkatua zaintzeko agintaritza bat izendatu behar ditu, agintaritza nazional eskudun modura jardun dezaten erregelamendua egokiro aplikatzen eta betearazten dela ikuskatzeko lanetan. Estatu kideek edozein motatako entitate publikoa izendatu dezakete erregelamendu honi lotuta agintaritza nazional eskudun modura jardun dezan, estatuaren ezaugarrietara eta antolamendu-premia zehatzetara egokituta. Estatu kideen antolamendu-efizientzia handitzeko xedez eta herritarrek eta estatuen mailako zein Batasunaren mailako homologoei harremanetan izateko gune ofizial bakarra ezartzeko asmoz, estatu kide bakoitzak merkatua zaintzeko agintaritza bat izendatu behar du harremanetarako gune bakar gisa jardun dezan.

(154) Agintaritza nazional eskudunek modu independente, inpartzial eta objektiboan baliatu behar dituzte beren ahalak, hartara beren jardun eta eginkizunetan objektibotasun-printzipioak betetzen direla zaintzeko eta erregelamendu hau aplikatzen eta betetzen dela bermatzeko. Agintaritza horietako kideek uko egin behar diete beren eginkizunen nondik norakoekin bateraezinak diren egintza guztiei, eta xehe bete behar dituzte erregelamendu honetan ezarritako konfidentzialtasun-arauak.

(155) Arrisku handiko AA-sistemen hornitzaile guztiek merkaturatu osteko zaintza-sistema bat eduki behar dute. Izan ere, zaintza-sistema horren bidez, arrisku handiko AA-sistemak erabiltzean izandako esperientzia kontuan hartu ahal izango da, hartara hobekuntzak egin ahal izateko bai sistemetan bertan, bai haien diseinu-eta garapen-prozesuetan, edo zuzenketa-neurriak hartu ahal izateko egoki den unean. Merkaturatu osteko zaintzak, hala dagokionean, beste AA-sistema batzuekiko interakzioa ere aztertuko du —beste gailu eta software batzuk ere barne—. AA-sistemen hedapenaren arduradunak zuzenbidea betearazteko agintaritza direnean, haiei dagozkien bereziki babestutako datu operatiboak ez dira merkaturatu



fundamental para garantizar que los posibles riesgos derivados de los sistemas de IA que siguen «aprendiendo» tras su introducción en el mercado o puesta en servicio se aborden de un modo más eficiente y oportuno. En este contexto, procede exigir a los proveedores que también cuenten con un sistema para comunicar a las autoridades pertinentes cualquier incidente grave asociado al uso de sus sistemas de IA, entendido como un incidente o defecto que tenga como consecuencia un fallecimiento o daños graves para la salud, una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas, el incumplimiento de obligaciones derivadas del Derecho de la Unión destinadas a proteger los derechos fundamentales o daños graves a la propiedad o al medio ambiente.

(156) Con el objetivo de garantizar el cumplimiento adecuado y efectivo de los requisitos y obligaciones previstos en el presente Reglamento, que constituye legislación de armonización de la Unión, debe aplicarse en su totalidad el sistema relativo a la vigilancia del mercado y la conformidad de los productos establecido por el Reglamento (UE) 2019/1020. Las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento deben disponer de todos los poderes de ejecución establecidos en el presente Reglamento y en el Reglamento (UE) 2019/1020, y deben ejercer sus poderes y desempeñar sus funciones de manera independiente, imparcial y objetiva. Aunque la mayoría de los sistemas de IA no están sujetos a requisitos ni obligaciones específicos en virtud del presente Reglamento, las autoridades de vigilancia del mercado pueden adoptar medidas en relación con todos los sistemas de IA cuando estos presenten un riesgo de conformidad con el presente Reglamento. Debido a la naturaleza específica de las instituciones, órganos y organismos de la Unión que entran en el ámbito de aplicación del presente Reglamento, procede designar al Supervisor Europeo de Protección de Datos como autoridad de vigilancia del mercado competente para ellos. Esto debe entenderse sin perjuicio de la designación de autoridades nacionales competentes por parte de los Estados miembros. Las actividades de vigilancia del mercado no deben afectar a la capacidad de las entidades supervisadas para llevar a cabo sus tareas de manera independiente, cuando el Derecho de la Unión exija dicha independencia.

(157) El presente Reglamento se entiende sin perjuicio de las competencias, funciones, poderes e independencia de las autoridades u organismos públicos nacionales pertinentes que supervisan la aplicación del Derecho de la Unión que protege los derechos fundamentales, incluidos los organismos de igualdad y las autoridades de protección de datos. Cuando sea necesario para su mandato, dichas autoridades u organismos públicos nacionales también deben tener acceso a cualquier documentación creada

osteko zaintzan sartuko. Sistema hori funtsezkoa da, halaber, bermatzeko merkatuan jarri edo zerbitzuan ipini ostean «ikasten» jarraitzen duten AA-sistemetatik datozen arriskuak modu efiziente eta egokiagoan jorratzen direla. Testuinguru horretan, egoki da hornitzaileei eskatzea sistema bat izan dezaten agintaritzei AA-sistemen erabilerari lotutako edozein gorabehera larri jakinarazteko. Gorabehera larritzat jotzen dira: heriotza edo osasunerako kalte larriak eragiten dituzten gertaerak edo akatsak; azpiegitura kritikoen kudeaketa edo funtzionamendua larriki eta ezin konponduzko moduan aldarazten duten gertaerak; Batasunak oinarritzko eskubideak babesteko ezarritako zuzenbidetik sortutako betebeharren ez-betetzeak, eta jabetzari edota ingurumenari eragindako kalte larriak.

(156) Erregelamendu honetan aurreikusitako betekizunak eta betebeharrak egokiro eta eraginkortasunez betetzen direla bermatzeko, erregelamendu hau Batasunaren harmonizazioko legeria izanik, osorik aplikatu behar da merkatuaren zaintzarako eta produktuen adostasunerako sistema, (EB) 2019/1020 Erregelamenduan ezarritako moduan. Merkatua zaintzeko agintaritzek, erregelamendu honen arabera izendatuta dauden heinean, erregelamendu honetan eta (EB) 2019/1020 Erregelamenduan ezarritako betearazpen-ahalak eduki behar dituzte, eta modu independente, inpartzial eta objektiboan baliatu behar dituzte beren ahalak, eta halaxe bete behar dituzte beren eginkizunak. Nahiz eta erregelamendu honen arabera AA-sistema gehienak ez dauden lotuta betekizun eta betebeharrak zehatzetara, merkatua zaintzeko agintaritzek edozein AA-sistematarako har ditzakete neurriak, dena delako sistema horrek erregelamendu honen arabera arriskuren bat badakar. Erregelamendu honen aplikazio-eremuan sartzen diren Batasuneko instituzio, organo eta organismoen izaera jakina dela eta, egoki da Datuak Babesteko Europako Ikuskatzailea merkatua zaintzeko agintaritzak eskudun izendatzea erakunde horietarako. Hori, nolahi ere, ez da eragozpen izango estatu kideek agintaritzak nazional eskudunak izenda ditzaten. Merkatuko zaintza-jarduerak ez dute eraginik izan behar ikuskatutako entitateek beren jarduerak modu independentean egiteko duten gaitasunean, Batasuneko zuzenbideak independentzia hori exijitzen duenean.

(157) Erregelamendu hau ez da eragozpen izango Batasunaren oinarritzko eskubideak babesten dituen zuzenbidearen aplikazioa ikuskatzen duten agintaritzak edo organismo publiko nazionalen eskumen, eginkizun, ahal eta independentziarako —berdintasun-organismoak eta datuak babesteko agintaritzak ere organismo eta agintaritzak horien barruan daude—. Agintaritzak edo organismo publiko nazional horiek, beren aginpiderako beharrezkoa dutenean, erregelamendu honen arabera sortutako edozein dokumentaziotarako sarbidea izango



en virtud del presente Reglamento. Debe establecerse un procedimiento de salvaguardia específico para garantizar una ejecución adecuada y oportuna frente a sistemas de IA que presenten un riesgo para la salud, la seguridad o los derechos fundamentales. El procedimiento relativo a dichos sistemas de IA que presentan un riesgo debe aplicarse a los sistemas de IA de alto riesgo que presenten un riesgo, a los sistemas prohibidos que hayan sido introducidos en el mercado, puestos en servicio o utilizados contraviniendo las prácticas prohibidas establecidas en el presente Reglamento y a los sistemas de IA que hayan sido comercializados infringiendo los requisitos de transparencia establecidos en el presente Reglamento y que presenten un riesgo.

(158) El Derecho de la Unión en materia de servicios financieros contiene normas y requisitos en materia de gobernanza interna y gestión de riesgos que las entidades financieras reguladas deben cumplir durante la prestación de dichos servicios, y también cuando utilicen sistemas de IA. Para garantizar la aplicación y ejecución coherentes de las obligaciones previstas en el presente Reglamento, así como de las normas y los requisitos oportunos de los actos jurídicos de la Unión relativos a los servicios financieros, se ha de designar a las autoridades competentes de supervisar y ejecutar dichos actos jurídicos, en particular las autoridades competentes definidas en el Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo (46) y las Directivas 2008/48/CE (47), 2009/138/CE (48), 2013/36/UE (49), 2014/17/UE (50) y (UE) 2016/97 (51) del Parlamento Europeo y del Consejo, dentro de sus respectivas competencias, como las autoridades competentes encargadas de supervisar la aplicación del presente Reglamento, también por lo que respecta a las actividades de vigilancia del mercado, en relación con los sistemas de IA proporcionados o utilizados por las entidades financieras reguladas y supervisadas, a menos que los Estados miembros decidan designar a otra autoridad para que desempeñe estas tareas de vigilancia del mercado. Dichas autoridades competentes deben disponer de todos los poderes previstos en el presente Reglamento y en el Reglamento (UE) 2019/1020 para hacer cumplir los requisitos y obligaciones del presente Reglamento, incluidos los poderes para llevar a cabo actividades de vigilancia del mercado *ex post* que pueden integrarse, en su caso, en sus mecanismos y procedimientos de supervisión existentes en virtud del Derecho pertinente de la Unión en materia de servicios financieros. Conviene prever que, cuando actúen como autoridades de vigilancia del mercado en virtud del presente Reglamento, las autoridades nacionales responsables de la supervisión de las entidades de crédito reguladas por la Directiva 2013/36/UE que participen en el Mecanismo Único de Supervisión establecido por el Reglamento (UE) n.º 1024/2013 del Consejo (52) comuniquen sin demora al Banco Central

dute. Babes-prozedura espezifikiko bat ezarri behar da modu egoki eta aproposan jarduteko osasunerako, segurtasunerako edo oinarritzko eskubideetarako arriskua dakarten AA-sistemen aurrean. Arriskua dakarten AA-sistema horien gaineko prozedura sistema hauei aplikatu behar zaie: arriskua dakarten arrisku handiko sistemei, erregelamendu honetan adierazitako jardunbide debekatuei muzin eginda merkatuan jarri, zerbitzuan ipini edo erabilitako sistema debekatuei eta erregelamendu honen arabera gardentasun-betekizunak hautsita merkaturatu diren eta arriskua dakarten AA-sistemei.

(158) Batasunak finantza-zerbitzuen arloan ezarritako zuzenbideak zenbait arau eta betekizun jasotzen ditu barne-gobernantzarako eta arriskuen kudeaketarako; finantza-entitateek beharrezkoa dute arau eta betekizun horiek betetzea zerbitzu horiek ematen dituztenean, baita AA-sistemak erabiltzen dituztenean ere. Finantza-zerbitzuen gainean erregelamendu honetan aurreikusitako betebeharrak eta Batasunean ezarritako egintza juridikoen arauak eta betekizunak modu koherentean aplikatzen eta betearazten direla bermatzeko, egintza juridiko horiek ikuskatzeko eta betearazteko agintaritza eskudunak izendatu behar dira, bereziki arau hauetan zehaztutako agintaritza eskudunak: Europako Parlamentuaren eta Kontseiluaren (EB) 575/2013 Erregelamenduan (46) eta Europako Parlamentuaren eta Kontseiluaren 2008/48/EE (47), 2009/138/EE (48), 2013/36/EB (49), 2014/17/EB (50) eta (EB) 2016/97 zuzentarauetan (51), bakoitzak bere eskumenen barruan, erregelamendu honen aplikazioa ikuskatzeko ardura duten agintaritza eskudun izanik, eta haien ardurapean izango dira, halaber, merkatua zaintzeko jarduerak, araututako eta ikuskatutako finantza-entitateek emandako edo erabilitako AA-sistemei lotuta, salbu eta estatu kideek erabakitzen badute beste agintaritza bat izendatzea merkatua zaintzeko betekizun horiek betetzeko. Agintaritza eskudun horiek erregelamendu honetan eta (EB) 2019/1020 Erregelamenduan aurreikusitako ahal guztiak izan behar dituzte erregelamendu honetako betekizunak eta betebeharrak betearazteko; hala, ahal horien barruan egongo dira *ex post* merkatua zaintzeko jarduerak, finantza-zerbitzuen arloan Batasunak xedatutako zuzenbidearen arabera ikuskatze-mekanismo eta -prozeduren barruan sar daitezkeen heinean. Komeni da aurreikustea ezen 2013/36/EB Zuzentzarauan araututako kreditu-entitateak ikuskatzeaz arduratzen diren agintaritza nazionalak —Kontseiluaren (EB) 1024/2013 Erregelamenduan (52) ezarritako Gainbegiratzeko Mekanismo Bakarrean parte hartzen dutenak—, erregelamendu honen arabera merkatua zaintzeko agintaritza modura dihardutenean, atzerapenik gabe jakinarazi behar diotela Europako



Europeo toda información obtenida en el transcurso de sus actividades de vigilancia del mercado que pueda ser de interés para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento. Con vistas a aumentar la coherencia entre el presente Reglamento y las normas aplicables a las entidades de crédito reguladas por la Directiva 2013/36/UE, conviene igualmente integrar algunas de las obligaciones procedimentales de los proveedores relativas a la gestión de riesgos, la vigilancia poscomercialización y la documentación en las obligaciones y los procedimientos vigentes con arreglo a la Directiva 2013/36/UE. Para evitar solapamientos, también se deben contemplar excepciones limitadas en relación con el sistema de gestión de la calidad de los proveedores y la obligación de vigilancia impuesta a los responsables del despliegue de sistemas de IA de alto riesgo, en la medida en que estos se apliquen a las entidades de crédito reguladas por la Directiva 2013/36/UE. El mismo régimen debe aplicarse a las empresas de seguros y reaseguros y a las sociedades de cartera de seguros reguladas por la Directiva 2009/138/CE, a los intermediarios de seguros regulados por la Directiva (UE) 2016/97 y a otros tipos de entidades financieras sujetas a requisitos sobre gobernanza, sistemas o procesos internos establecidos con arreglo al Derecho pertinente de la Unión en materia de servicios financieros a fin de garantizar la coherencia y la igualdad de trato en el sector financiero.

(159) Cada autoridad de vigilancia del mercado para los sistemas de IA de alto riesgo en el ámbito de la biometría enumerados en un anexo del presente Reglamento, en la medida en que dichos sistemas se utilicen con fines de garantía del cumplimiento del Derecho, de migración, asilo y gestión del control fronterizo, o de la administración de justicia y los procesos democráticos, debe disponer de facultades de investigación y correctoras efectivas, incluida al menos la facultad de obtener acceso a todos los datos personales que se estén tratando y a toda la información necesaria para el desempeño de sus funciones. Las autoridades de vigilancia del mercado deben poder ejercer sus poderes actuando con total independencia. Cualquier limitación de su acceso a datos operativos sensibles en virtud del presente Reglamento debe entenderse sin perjuicio de los poderes que les confiere la Directiva (UE) 2016/680. Ninguna exclusión de la divulgación de datos a las autoridades nacionales de protección de datos en virtud del presente Reglamento debe afectar a los poderes actuales o futuros de dichas autoridades que trasciendan el ámbito de aplicación del presente Reglamento.

(160) Las autoridades de vigilancia del mercado y la Comisión deben poder proponer actividades conjuntas, incluidas investigaciones conjuntas, que deben llevar a cabo las autoridades de vigilancia del mercado o las

Banku Zentralari merkatua zaintzeko jardueretan eskuratutako informazio guztia, interesgarria bada Europako Banku Zentralaren zuhurtziazko gainbegiratze-eginkizunetarako, zeinak (EB) 1024/2013 Erregelamenduan baitaude zehatuta. Erregelamendu honen eta 2013/36/EB Zuzentarauan araututako kreditu-entitateei aplikatu beharreko arauen arteko koherentzia handitze aldera, komenigarria da, halaber, hornitzaileen prozedura-betebehar batzuk txertatzea, zehazki gai hauei dagokienez: arriskuen kudeaketa, merkaturatu osteko zaintza eta indarrean dauden betebehar eta prozedurak bat etorrita 2013/36/EB Zuzentaruarekin. Gainjartzerik ez gertatzeko, salbuespen mugatu batzuk ere ezarri behar dira hornitzaileen kalitate-kudeaketako sistemari eta arrisku handiko AA-sistemen hedapenaren arduradunei ezarritako zaintza-betebeharrari dagokienez, AA-sistema horiek 2013/36/EB Zuzentarauan araututako kreditu-entitateei aplikatzen zaien heinean. Araubide bera aplikatu behar zaie 2009/138/EE Zuzentaruak araututako aseguru- eta berraseguru-enpresei eta aseguru-zorroko sozietateei, (EB) 2016/97 Zuzentaruak araututako aseguru-bitartekariei eta bestelako finantza-entitate batzuei, entitate horiek lotuta dauden heinean Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera ezarritako barne-gobernantza, -sistema edo -prozesuei buruzko betekizunetara finantza-sektorean koherentzia eta tratu-berdintasuna bermatzeko.

(159) Erregelamendu honen eranskin batean zerrendatutako biometriaren arloko arrisku handiko AA-sistemen kasuan —betiere sistema horiek zuzenbidea betearazteko, migrazioarako, asiloarako eta muga-kontrola kudeatzeko erabiltzen diren neurrian edo justizia-administrazioarako eta prozesu demokratikoetarako erabiltzen diren neurrian—, merkatua zaintzeko agintaritza bakoitzak ikerketarako eta zuzenketarako ahalmen efektiboak eduki behar ditu, eta ahalmen horien artean egongo da, gutxienez, tratatzen ari diren datu pertsonal guztietara eta beren eginkizunak betetzeko beharrezkoa duten informazio guztira sarbidea izateko ahalmena. Merkatua zaintzeko agintaritzek beren ahalak independentzia osoz betearazteko gaitasuna izan behar dute. Erregelamendu honen arabera bereziki babestutako datu operatiboetara sarbidea izateko mugek ez diete kalterik egingo (EB) 2016/680 Zuzentaruak ematen dizkien ahalei. Erregelamendu honen arabera datuak babesteko agintaritza nazionalak datuak jakinarazteko eskklusio bakar batek ere ezin die eragin agintaritza horien nean uneko zein etorkizuneko ahalei, erregelamendu honen aplikazio-eremutik landa.

(160) Bi estatu kide edo gehiagotan arrisku larria dakarten arrisku handiko AA-sistemen kategoria espezifikoek dagokienez erregelamendu hau beteko dela sustatzeko, ez-betetzeak detektatzeko eta haren



autoridades de vigilancia del mercado junto con la Comisión, con el objetivo de fomentar el cumplimiento, detectar incumplimientos, sensibilizar y ofrecer orientaciones en relación con el presente Reglamento con respecto a las categorías específicas de sistemas de IA de alto riesgo que presentan un riesgo grave en dos o más Estados miembros. Tales actividades conjuntas para fomentar el cumplimiento deben llevarse a cabo de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de IA debe prestar apoyo de coordinación a las investigaciones conjuntas.

(161) Es necesario aclarar las responsabilidades y competencias a escala de la Unión y nacional en lo que respecta a los sistemas de IA que se basan en modelos de IA de uso general. Para evitar el solapamiento de competencias, cuando un sistema de IA se base en un modelo de IA de uso general y el modelo y el sistema sean suministrados por el mismo proveedor, la supervisión debe llevarse a cabo a escala de la Unión a través de la Oficina de IA, que debe tener a estos efectos las facultades de una autoridad de vigilancia del mercado en el sentido de lo dispuesto en el Reglamento (UE) 2019/1020. En todos los demás casos, serán responsables de la supervisión de los sistemas de IA las autoridades nacionales de vigilancia del mercado. No obstante, en el caso de los sistemas de IA de uso general que puedan ser utilizados directamente por los responsables del despliegue con al menos un fin clasificado como de alto riesgo, las autoridades de vigilancia del mercado deben cooperar con la Oficina de IA para llevar a cabo evaluaciones de la conformidad e informar de ello al Consejo de IA y a otras autoridades de vigilancia del mercado. Además, las autoridades de vigilancia del mercado deben poder solicitar la asistencia de la Oficina de IA cuando la autoridad de vigilancia del mercado no pueda concluir una investigación sobre un sistema de IA de alto riesgo debido a su incapacidad para acceder a determinada información relacionada con el modelo de IA de uso general en el que se basa el sistema de IA de alto riesgo. En tales casos, debe aplicarse *mutatis mutandis* el procedimiento de asistencia mutua transfronteriza previsto en el capítulo VI del Reglamento (UE) 2019/1020.

(162) Para aprovechar al máximo la centralización de conocimientos especializados y las sinergias que se generan a escala de la Unión, deben atribuirse a la Comisión las competencias de supervisión y de control del cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general. La Oficina de IA debe poder llevar a cabo todas las acciones necesarias para supervisar la aplicación efectiva del presente Reglamento en lo que respecta a los modelos de IA de uso general. Debe poder investigar posibles infracciones de las normas relativas a los proveedores de modelos de IA de uso general, tanto por iniciativa propia, a raíz

inguruan sentsibilizatzeko eta orientabideak emateko xedez, merkatua zaintzeko agintaritzek eta Batzordeak aukera izan behar dute baterako jarduerak proposatzeko —baterako ikerketak barne—, merkatua zaintzeko agintaritzek beren kabuz edo Batzordearekin batera gauzatu ditzaten. Erregelamendua betetzea sustatzeko baterako jarduera horiek gauzatzeko orduan, 2019/1020 (EB) Erregelamenduaren 9. artikulua bete behar da. AA-bulegoak koordinazio-laguntza eman behar du baterako ikerketak egiteko.

(161) Beharrezkoa da argitzea zer erantzukizun eta eskumen izango dituzten Batasunak eta estatu kideek erabilera orokorreko AA-ereduetan oinarritzen diren AA-sistemen gainean. Eskumenak gainjarri ez daitezten, AA-sistema bat erabilera orokorreko AA-eredu batean oinarritzen denean eta bai eredia, bai sistema hornitzaile berak hornitzen dituenean, ikuskapena Batasunak egin behar du AA-bulegoaren bitartez; horretarako, merkatua zaintzeko agintaritzaren ahalmenak izan behar ditu AA-bulegoak, 2019/1020 (EB) Erregelamenduan xedatutakoaren ildotik. Gainerako kasu guztietan, merkatua zaintzeko agintaritza nazionalak izango dira AA-sistemak ikuskatzeko arduradunak. Dena dela, hedapenaren arduradunek zuzenean erabiltzeko modukoak diren erabilera orokorreko AA-sistemen kasuan, arrisku handikotzat sailkatutako gutxienez helburu bat duten heinean, merkatua zaintzeko agintaritzek AA-bulegoarekin lankidetzan jardun behar dute adostasuna ebaluatzeko eta horren berri emateko bai AA-kontseiluari, bai merkatua zaintzeko beste agintaritza batzuei. Gainera, merkatua zaintzeko agintaritzek AA-bulegoaren laguntza eskatzeko aukera izan behar dute, ezinezkoa bazaie arrisku handiko AA-sistema baten gaineko ikerketa burutzea ezin dutelako eskuratu arrisku handiko AA-sistemaren oinarri den erabilera orokorreko AA-ereduari lotutako informazio zehatzen bat. Halakoetan, *mutatis mutandis* aplikatu behar da (EB) 2019/1020 Erregelamenduaren VI. kapituluaren aurreikusitako mugaz gaindiko elkarrekiko laguntza prozedura.

(162) Batasunean sortutako ezagutza espezializatuen zentralizazioari eta sinergiari ahalik eta etekin handiena ateratzeko, Batzordeari esleitu behar zaizkio erabilera orokorreko AA-ereduen hornitzaileek beren betebeharrak betetzen dituzten ikuskatzeko eta kontrolatzeko eskumenak. AA-bulegoak modua izan behar du behar diren ekintza guztiak egin ahal izateko, erabilera orokorreko AA-ereduei dagokienez erregelamendu hau egokiro aplikatzen dela ikuskatze aldera. Hala, modua izan behar du erabilera orokorreko AA-ereduen hornitzaileei dagozkien arauetan arau-hausterik gertatu den ikertzeko, bai bere ekimenez —



de los resultados de sus actividades de supervisión, como a petición de las autoridades de vigilancia del mercado, de conformidad con las condiciones establecidas en el presente Reglamento. Para promover la eficacia de la supervisión, la Oficina de IA debe prever la posibilidad de que los proveedores posteriores presenten reclamaciones sobre posibles infracciones de las normas relativas a los proveedores de sistemas y modelos de IA de uso general.

(163) Con el fin de complementar los sistemas de gobernanza de los modelos de IA de uso general, el grupo de expertos científicos debe contribuir a las actividades de supervisión de la Oficina de IA y, en determinados casos, puede proporcionar alertas cualificadas a la Oficina de IA que activen actuaciones consecutivas, como investigaciones. Así debe ocurrir cuando el grupo de expertos científicos tenga motivos para sospechar que un modelo de IA de uso general presenta un riesgo concreto e identificable a escala de la Unión. También debe ser este el caso cuando el grupo de expertos científicos tenga motivos para sospechar que un modelo de IA de uso general cumple los criterios que llevarían a clasificarlo como modelo de IA de uso general con riesgo sistémico. A fin de facilitar al grupo de expertos científicos la información necesaria para el desempeño de esas funciones, debe existir un mecanismo que permita al grupo de expertos científicos pedir a la Comisión que solicite documentación o información a un proveedor.

(164) La Oficina de IA debe poder adoptar las medidas necesarias para supervisar la aplicación efectiva y el cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general establecidas en el presente Reglamento. La Oficina de IA debe poder investigar posibles infracciones de conformidad con las competencias previstas en el presente Reglamento, por ejemplo, solicitando documentación e información, realizando evaluaciones y solicitando la adopción de medidas a los proveedores de modelos de IA de uso general. En la realización de las evaluaciones, para poder contar con conocimientos especializados independientes, la Oficina de IA debe poder recurrir a expertos independientes para que lleven a cabo las evaluaciones en su nombre. Se debe poder exigir el cumplimiento de las obligaciones mediante, entre otras cosas, solicitudes de adopción de medidas adecuadas, entre las que se incluyen medidas de reducción del riesgo en caso de que se detecten riesgos sistémicos, así como la restricción de la comercialización, la retirada o la recuperación del modelo. Como salvaguardia, cuando sea necesario, además de los derechos procedimentales previstos en el presente Reglamento, los proveedores de modelos de IA de uso general deben tener los derechos procedimentales previstos en el artículo 18 del Reglamento (UE) 2019/1020, que deben aplicarse *mutatis mutandis*, sin perjuicio de los derechos

ikuskatze-lanetako emaitzetan oinarrituta—, bai merkatua zaintzeko agintaritzen eskariz, erregelamendu honetan ezarritako baldintzekin bat etorrita. Ikuskatze-lana eraginkorra izateko, AA-bulegoak aurreikusi behar du ondorengo hornitzaileek erreklamazioak aurkeztu ahal izatea erabilera orokorreko AA-sistema eta -ereduen hornitzaileei dagozkien arauen gaineko balizko arau-hausteei buruz.

(163) Erabilera orokorreko AA-ereduen gobernantza-sistemak osatze aldera, aditu zientifikoen taldeak laguntza eman behar du AA-bulegoaren ikuskapen-jardueretarako, eta, kasu jakin batzuetan, alerta kualifikatuak eman diezazkioke AA-bulegoari, alerten araberako jarduketak abiarazteko —ikerketak, adibidez—. Halaxe gertatu behar da aditu zientifikoen taldeak arrazoiak dituenean susmatzeko erabilera orokorreko AA-eredu batek arrisku zehatz eta identifikagarri bat duela Batasunaren mailan. Halaxe izan behar da, halaber, aditu zientifikoen taldeak arrazoiak dituenean susmatzeko erabilera orokorreko AA-eredu batek bete egiten dituela arrisku sistemikoa dakarren erabilera orokorreko AA-eredutzat sailkatzeko irizpideak. Aditu zientifikoen taldeak eginkizun horiek betetzeko behar duen informazioa izan dezan, beharrezkoa da mekanismo bat egotea aditu zientifikoen taldeak Batzordeari eskaria egin ahal izan diezaion Batzordeak hornitzaileari dokumentazioa eta informazio hori galdegiteko.

(164) AA-bulegoak behar diren neurriak hartu ahal izango ditu ikuskatzeko egokiro aplikatzen eta betetzen direla erabilera orokorreko AA-ereduen hornitzaileek erregelamendu honen arabera dituzten betebeharrak. AA-bulegoak modua izan behar du arau-haustek ikertzeko, bat etorrita erregelamendu honetan aurreikusitako eskumenekin; esate baterako, dokumentazioa eta informazioa eskatuz, ebaluazioak eginez eta erabilera orokorreko AA-ereduen hornitzaileei neurriak har ditzaten eskatuz. Ebaluazioak egiteko orduan, ezagutza espezializatu independenteak eskuratu ahal izateko, AA-bulegoak aditu independenteetara jo ahal izateko aukera izan behar du, ebaluazioak haren izenean egin ditzan. Betebeharrak betetzea eskatu ahal izango da, besteak beste eskariak eginez neurri egokiak har daitezen: adibidez, arriskuak murrizteko neurriak, arrisku sistemikoak hautemanez gero, edota ereduaren merkaturatzea mugatzeko edo erdua merkatutik kentzeko edo berreskuratzeko neurriak. Babes modura, beharrezkoa denean, erregelamendu honetan aurreikusitako eskubideez gain, erabilera orokorreko AA-ereduen hornitzaileek (EB) 2019/1020 Erregelamenduaren 18. artikuluan aurreikusitako eskubide prozesalak eduki behar dituzte, eta eskubide horiek *mutatis mutandis* aplikatu behar



procesales más específicos previstos en el presente Reglamento.

(165) El desarrollo de sistemas de IA que no sean sistemas de IA de alto riesgo conforme a los requisitos establecidos en el presente Reglamento puede dar lugar a la adopción más amplia de una IA ética y fiable en la Unión. Se debe alentar a los proveedores de sistemas de IA que no son de alto riesgo a crear códigos de conducta, entre los que se incluyen los correspondientes mecanismos de gobernanza, destinados a impulsar la aplicación voluntaria de la totalidad o parte de los requisitos aplicables a los sistemas de IA de alto riesgo, adaptados teniendo en cuenta la finalidad prevista de los sistemas y el menor riesgo planteado y teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector, como las tarjetas de modelo y de datos Asimismo, se debe animar a los proveedores y, en su caso, a los responsables del despliegue de todos los sistemas de IA, ya sean o no de alto riesgo, y de los modelos de IA, a aplicar, con carácter voluntario, requisitos adicionales relativos, por ejemplo, a los elementos de las Directrices éticas de la Unión para una IA fiable, la sostenibilidad medioambiental, medidas de alfabetización en materia de IA, la inclusividad y la diversidad en el diseño y el desarrollo de los sistemas de IA, lo que incluye tener en cuenta a las personas vulnerables y la accesibilidad de las personas con discapacidad, la participación de las partes interesadas, con la participación, según proceda, de las partes interesadas pertinentes, como las organizaciones empresariales y de la sociedad civil, el mundo académico, los organismos de investigación, los sindicatos y las organizaciones de protección de los consumidores, en el diseño y el desarrollo de los sistemas de IA, y la diversidad de los equipos de desarrollo, también por lo que respecta a la paridad de género. Para garantizar la efectividad de los códigos de conducta voluntarios, estos deben basarse en objetivos claros e indicadores clave del rendimiento que permitan medir la consecución de dichos objetivos. También deben desarrollarse de manera inclusiva, según proceda, con la participación de las partes interesadas pertinentes, como las organizaciones empresariales y de la sociedad civil, el mundo académico, los organismos de investigación, los sindicatos y las organizaciones de protección de los consumidores. La Comisión podría formular iniciativas, también de carácter sectorial, encaminadas a facilitar la disminución de los obstáculos técnicos que dificultan el intercambio transfronterizo de datos para el desarrollo de la IA, también en relación con la infraestructura de acceso a los datos y la interoperabilidad semántica y técnica de distintos tipos de datos.

(166) Es importante que los sistemas de IA asociados a productos que el presente Reglamento no considera de alto riesgo y que, por lo tanto, no están obligados a cumplir los requisitos establecidos para los sistemas de

dira, hargatik erregelamendu honetan aurreikusitako eskubide prozesal zehatzagoak eragotzi gabe.

(165) Erregelamendu honetan ezarritako betekizunen arabera arrisku handiko AA-sistemak ez diren AA-sistemak garatzeak Batasunean AA etiko eta fidagarriago bat luze-zabalago hartzea ekar dezake. Arrisku handikoak ez diren AA-sistemen hornitzaileak jokabide-kodeak hartzera bultzatu behar dira. Jokabide-kode horien artean daude, besteak beste, sistemetarako gobernantza-mekanismoak, arrisku handiko AA-sistemei aplikatzekoak zaizkien betekizunak osorik edo parte batez borondatez aplikatzera bideratutakoak, egokiro moldatuta kontuan hartuz zer helburu aurreikusi daukaten sistemak eta zer-nolakoa den planteatutako arrisku txikiago hori, bai, halaber, zer soluzio tekniko dauden erabilgarri eta zein diren sektorearen jardunbide egokienak, hala nola eredu- eta datu-txartelak. Era berean, AA-sistema guztien kasuan —arrisku handikoak izan zein ez—, haien hornitzaileak bultzatu behar dira, eta, egoki bada, hedapenaren arduradunak ere bai, beren borondatez beste betekizun osagarri batzuk ere har ditzaten, arlo hauetan adibidez: AA fidagarria izateko Batasunak ezarritako gidalerro etikoak ezartzea, ingurumen-jasangarritasuna zaintzea, AAren arloko alfabetatzea, AA-sistemak diseinatzeko eta garatzeko prozesuetan inklusibitatea eta aniztasuna aintzat hartzea —pertsona kalteberak eta desgaitasuna duten pertsonen irisgarritasuna aintzat hartuta—, AA-sistemak diseinatzeko eta garatzeko prozesuetan alderdi interesdunek parte hartzea —hor dira enpresaren eremuko zein gizarte zibileko antolakundeak, mundu akademikoa, ikerketa-organismoak, sindikatuak eta kontsumitzaileak babesteko antolakundeak—, eta garapen-taldeetan aniztasuna bermatzea, genero-parekotasuna ere barnean dela. Borondatezko jokabide-kodeen eraginkortasuna bermatzeko, jokabide-kode horien helburuek argiak izan behar dute eta errendimendua azaltzeko giltzarri izan, haien bidez helburuen lorpen-maila zehazteko. Jokabide-kodeak, gisa bera, era inklusiboan garatu behar dira; hala, egoki diren alderdi interesdunek parte hartu behar dute, hots enpresaren eremuko zein gizarte zibileko antolakundeak, mundu akademikoa, ikerketa-organismoak, sindikatuak eta kontsumitzaileak babesteko antolakundeak. Batzordeak ekimenak era litzake —izaera sektorialekoak barne— AA garatzeko datuak mugaz gaindi trukatzeko traba teknikoak arintzen laguntzeko, barnean hartuta datuetara irispidea izateko azpiegitura eta datu moten arteko elkarreragingarritasun semantikoa eta teknikoa.

(166) Garrantzitsua da erregelamendu honek arrisku handikotzat jotzen ez dituen AA-sistemak, arrisku handiko AA-sistemetarako ezarritako betekizunak betetzera behartuta egon ez arren, seguruak izatea



IA de alto riesgo sean, no obstante, seguros una vez introducidos en el mercado o puestos en servicio. Para contribuir a este objetivo, se aplicaría, como red de seguridad, el Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo (53).

(167) Todas las partes implicadas en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos que obtengan en el ejercicio de sus funciones, de conformidad con el Derecho de la Unión o nacional, con vistas a garantizar una cooperación fiable y constructiva entre las autoridades competentes a escala de la Unión y nacional. Deben desempeñar sus funciones y actividades de manera que se protejan, en particular, los derechos de propiedad intelectual e industrial, la información empresarial confidencial y los secretos comerciales, la aplicación eficaz del presente Reglamento, los intereses de seguridad pública y nacional, la integridad de los procedimientos penales y administrativos y la integridad de la información clasificada.

(168) Se debe poder exigir el cumplimiento del presente Reglamento mediante la imposición de sanciones y otras medidas de ejecución. Los Estados miembros deben tomar todas las medidas necesarias para garantizar que se apliquen las disposiciones del presente Reglamento, también estableciendo sanciones efectivas, proporcionadas y disuasorias para las infracciones, y para respetar el principio de *non bis in idem*. A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, deben establecerse los límites máximos para la imposición de las multas administrativas en el caso de ciertas infracciones concretas. A la hora de determinar la cuantía de las multas, los Estados miembros deben tener en cuenta, en cada caso concreto, todas las circunstancias pertinentes de la situación de que se trate, considerando especialmente la naturaleza, gravedad y duración de la infracción y de sus consecuencias, así como el tamaño del proveedor, en particular si este es una pyme o una empresa emergente. El Supervisor Europeo de Protección de Datos debe estar facultado para imponer multas a las instituciones, los órganos y los organismos de la Unión incluidos en el ámbito de aplicación del presente Reglamento.

(169) Se debe poder exigir el cumplimiento de las obligaciones impuestas en virtud del presente Reglamento a los proveedores de modelos de IA de uso general mediante, entre otras cosas, la imposición de multas. A tal fin, también deben establecerse multas de una cuantía apropiada en caso de incumplimiento de dichas obligaciones, lo que incluye el incumplimiento de las medidas solicitadas por la Comisión de conformidad con el presente Reglamento, con sujeción a los plazos

merkaturan jarritakoan edo zerbitzuan ipinitakoan. Helburu hori lortu ahal izateko, Europako Parlamentuaren eta Kontseiluaren (EB) 2023/988 Erregelamendua (53) aplikatuko litzateke segurtasun-sare modura.

(167) Erregelamendu hau aplikatzeko zereginetan parte hartzen duten alderdi guztiek beren jardunean lortutako informazioaren eta datuen isilpekotasuna errespetatu behar dute, bat etorrita Batasuneko zuzenbidearekin edo zuzenbide nazionalarekin; helburua baita agintaritza eskudunen arteko lankidetzaz fidagarri eta konstruktiboa bermatzea. Beren zereginak eta jarduerak garatzeko orduan, bereziki babestu behar dituzte jabetza intelektualaren eta industrialaren eskubideak, enpresa-informazio konfidentziala eta merkataritza-sekretuak, erregelamendu honen aplikazio eraginkorra, segurtasun publiko eta nazionalaren interesak, prozedura penal eta administratiboen integritatea eta informazio sailkatuaren integritatea.

(168) Erregelamendu hau betetzea exijitu ahal izateko bidea eman behar da, zehapenak eta beste betearazpen-neurri batzuk ezarri. Estatu kideek behar diren neurriak hartu behar dituzte erregelamendu honen xedapenak aplikatzeko direla bermatzeko, eta zehapen eraginkor, proportzionatu eta disuasiozkoak ezarri behar dituzte arau-hausteei erantzuteko eta, aldi berean, *non bis in idem* printzipioa errespetatzeko. Erregelamendu hau urratzeagatik ezarritako administrazio-zehapenak indartzeko eta harmonizatzeko, administrazio-isunak jartzeko gehieneko mugak ezarri behar dira arau-hauste jakin batzuetarako. Isunen zenbatekoa zehazteko, estatu kideek egoera zehatz bakoitzari dagozkion inguruabar guztiak kontuan hartu behar dituzte, berezi-bereziki arau-haustearen eta haren ondorioen izaera, larritasuna eta iraupena, baita hornitzailearen tamaina ere, batik bat ETEa edo enpresa emergentea bada. Datuak Babesteko Europako Ikuskatzaileak ahalmena izan behar du isunak ezartzeko erregelamendu honen aplikazio-eremuan sartzen diren Batasuneko instituzio, organo eta organismoak.

(169) Erregelamendu honen arabera erabilera orokorreko AA-ereduen hornitzaileei dagozkien betebeharrak bete daitezkeen exijitzeko modua egon behar da, besteak beste isunak ezarri. Betebeharrak ez betetzeagatik ezartzen diren isunek zenbateko egokia izan behar dute, eta betebeharrak horien barruan egongo dira erregelamendu honekin bat etorrita Batzordeak eskatutako neurriak betetzea. Halakoetan, preskripzio-epe egokiak jarriko dira, proportzionaltasun-



de prescripción pertinentes de conformidad con el principio de proporcionalidad. Todas las decisiones adoptadas por la Comisión en virtud del presente Reglamento están sujetas al control del Tribunal de Justicia de la Unión Europea, de conformidad con lo dispuesto en el TFUE, incluida la competencia jurisdiccional plena del Tribunal de Justicia en materia de sanciones con arreglo al artículo 261 del TFUE.

(170) El Derecho de la Unión y nacional ya prevén vías de recurso efectivas para las personas físicas y jurídicas cuyos derechos y libertades se vean perjudicados por el uso de sistemas de IA. Sin perjuicio de dichas vías de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha producido una infracción del presente Reglamento debe tener derecho a presentar una reclamación ante la autoridad de vigilancia del mercado pertinente.

(171) Las personas afectadas deben tener derecho a obtener una explicación cuando la decisión de un responsable del despliegue se base principalmente en los resultados de salida de determinados sistemas de IA de alto riesgo que entran dentro del ámbito de aplicación del presente Reglamento y cuando dicha decisión produzca efectos jurídicos o afecte significativamente de modo similar a dichas personas, de manera que consideren que tiene un efecto negativo en su salud, su seguridad o sus derechos fundamentales. Dicha explicación debe ser clara y significativa y servir de base para que las personas afectadas puedan ejercer sus derechos. El derecho a obtener una explicación no debe aplicarse a la utilización de sistemas de IA para los que se deriven excepciones o restricciones con arreglo al Derecho nacional o de la Unión, y solo debe aplicarse en la medida en que este derecho no esté ya previsto en el Derecho de la Unión.

(172) Las personas que informen sobre infracciones del presente Reglamento deben quedar protegidas por el Derecho de la Unión. Así pues, cuando se informe sobre infracciones del presente Reglamento y en lo que respecta a la protección de las personas que informen sobre dichas infracciones debe aplicarse la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo (54).

(173) A fin de garantizar que el marco reglamentario pueda adaptarse cuando sea necesario, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE de modo que pueda modificar las condiciones en las que un sistema de IA no debe considerarse un sistema de alto riesgo, la lista de sistemas de IA de alto riesgo, las disposiciones relativas a la documentación técnica, el contenido de la declaración UE de conformidad, las disposiciones relativas a los procedimientos de evaluación de la

printzipioarekin bat. Batzordeak erregelamendu honen arabera hartutako erabaki guztiak Europar Batasuneko Justizia Auzitegiaren kontrolpean egongo dira, EBFTn xedatutakoari jarraikiz, barnean hartuta Justizia Auzitegiak zehapenen arloan EBFTren 261. artikuluearekin bat etorrita duen eskumen jurisdikzional osoa.

(170) Batasuneko zuzenbideak eta zuzenbide nazionalak jada aurreikusiak dituzte pertsona fisiko zein juridikoentzako errekurso-bideak, AA-sistemen erabilerak haien eskubide eta askatasunei kalte egiten dietenerako. Errekurtso-bide horiek gorabehera, pertsona fisiko edo juridiko batek arrazoren bat badu pentsatzeko erregelamendu honetan xedatutakoa urratu dela, eskubidea izan behar du erreklamazioak aurkezteko merkatua zaintzeko dagokion agintaritzan.

(171) Ukitutako pertsonak azalpen bat jasotzeko eskubidea izan behar dute, baldin eta hedapenaren arduradunak erregelamendu honen aplikazio-eremuan sartzen diren arrisku handiko AA-sistema jakinen irteera-emaizak baliatzen baditu erabakiak hartzeko oinarri nagusizat, eta erabaki horiek eragin juridikoak badituzte edo antzerako eragina badute ukitutako pertsona horiengan modu nabarmenean, eta, ondorioz, irizten bada eragin kaltegarria dutela haien osasunean, segurtasunean eta oinarritzko eskubideetan. Azalpenak argia eta adierazgarria izan behar du, eta baliagarria izan behar du ukitutako pertsonak haien eskubideak erabili ahal izan ditzaten. Azalpen bat jasotzeko eskubidea ez zaio aplikatu behar AA-sistemen erabilerari, baldin eta sistema horiei salbuespenak edo murrizketak aplikatzen bazaizkie Batasuneko zuzenbidearen edo zuzenbide nazionalaren arabera, eta Batasuneko zuzenbidean aurrez aurreikusita ez badago bakarrik aplikatu behar da.

(172) Batasuneko zuzenbideak babesa eman behar die erregelamendu honen arau-hausteei buruz informatzen duten pertsonen. Horrela, bada, jakinarazten denean erregelamendu hau urratu dela, Europako Parlamentuaren eta Kontseiluaren (EB) 2019/1937 Zuzentaraua (54) aplikatu behar da, arau-hauste horien berri eman duten pertsonak babeste aldera.

(173) Bermatu ahal izateko beharrezkoa denean erregelamendu-esparrua egokitu ahal izango dela, Batzordeari eskuordetu behar zaizkio EBFTren 290. artikuluari jarraikiz egintzak egiteko ahalak, aldaketak egin ahal izan ditzan alderdi hauetan guztietan: AA-sistema bat arrisku handikotzat ez jotzeko baldintzetan, arrisku handiko AA-sistemen zerrendan, dokumentazio teknikoari buruzko xedapenetan, EB adostasun-adierazpenaren edukian, adostasuna ebaluatzeko prozeduren gaineko xedapenetan, kalitatea kudeatzeko



conformidad, las disposiciones que establecen a qué sistemas de IA de alto riesgo debe aplicarse el procedimiento de evaluación de la conformidad basado en la evaluación del sistema de gestión de la calidad y en la evaluación de la documentación técnica, el umbral, los parámetros de referencia y los indicadores, lo que incluye la posibilidad de complementar dichos parámetros de referencia e indicadores, de las normas de clasificación de los modelos de IA de uso general con riesgo sistémico, los criterios para clasificar un modelo como modelo de IA de uso general con riesgo sistémico, la documentación técnica para los proveedores de modelos de IA de uso general y la información sobre transparencia para los proveedores de modelos de IA de uso general. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación (55). En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(174) Habida cuenta de los rápidos avances tecnológicos y de los conocimientos técnicos necesarios para la aplicación efectiva del presente Reglamento, la Comisión debe evaluar y revisar el presente Reglamento a más tardar el 2 de agosto de 2029 y posteriormente cada cuatro años e informar al Parlamento Europeo y al Consejo. Además, teniendo en cuenta las implicaciones por lo que respecta al ámbito de aplicación del presente Reglamento, la Comisión debe llevar a cabo una evaluación de la necesidad de modificar la lista de sistemas de IA de alto riesgo y la lista de prácticas prohibidas una vez al año. Asimismo, a más tardar el 2 de agosto de 2028 y posteriormente cada cuatro años, la Comisión debe evaluar y comunicar al Parlamento Europeo y al Consejo la necesidad de modificar la lista de ámbitos de alto riesgo que figura en el anexo del presente Reglamento, los sistemas de IA incluidos en el ámbito de aplicación de las obligaciones de transparencia, la eficacia del sistema de supervisión y gobernanza y los avances en el desarrollo de documentos de normalización sobre el desarrollo eficiente desde el punto de vista energético de modelos de IA de uso general, incluida la necesidad de medidas o acciones adicionales. Por último, a más tardar el 2 de agosto de 2028 y posteriormente cada tres años, la Comisión debe evaluar la repercusión y la eficacia de los códigos de conducta voluntarios para fomentar la aplicación de los requisitos establecidos para los sistemas de IA de alto riesgo a los sistemas de IA que

sistemaren ebaluazioa eta dokumentazio teknikoaren ebaluazioa oinarritzat dituen adostasuna ebaluatzeko prozedura arrisku handiko zer AA-sistematan aplikatu behar den zehazten duten xedapenetan, arrisku sistemikoa dakarten erabilera orokorreko AA-ereduak sailkatzeko arauetako atalasean, erreferentzia-parametroetan eta adierazleetan —barnean hartuta erreferentzia-parametro eta adierazle horiek osatu ahal izatea—, bai, halaber, eredu bat arrisku sistemikoa dakarren erabilera orokorreko AA-eredutzat sailkatzeko irizpideetan, erabilera orokorreko AA-ereduen hornitzaileentzako dokumentazio teknikoan eta erabilera orokorreko AA-ereduen hornitzaileei zuzendutako gardentasunari buruzko informazioan. Bereziki garrantzitsua da Batzordeak behar diren kontsultak egitea prestaketa-fasean, bereziki adituekin, eta, kontsulta horiek egiteko orduan, legeria hobetzeari buruzko 2016ko apirilaren 13ko erakundearteko Akordioan (55) ezarritako printzipioak betetzea. Zehazki, egintza eskuordetuak prestatzeko orduan parte-hartze ekitatiboa bermatzeko, estatu kideetako adituek dokumentazioa jasotzen dutenean, aldi berean jasotzen dute Europako Parlamentuak eta Kontseiluak ere dokumentazio guztia, eta erakunde horietako adituek sistematikoki dute sarbidea Batzordeko aditu-taldeek egintza eskuordetuak prestatzeko egiten dituzten bileretara.

(174) Erregelamendu hau egokiro aplikatzeko behar diren aurrerabide teknologikoak eta ezagutza teknikoak kontuan hartuta, Batzordeak, beranduenez, 2029ko abuztuaren 2an ebaluatu eta berrikusi behar du erregelamendu hau, eta, horren ostean, lau urterik behin, eta Europako Parlamentuari eta Kontseiluari horren berri eman. Gainera, gogoan izanda Erregelamenduaren aplikazio-eremuak dituen berezitasunak, Batzordeak ebaluazio bat egin behar du urtean behin aztertzeko ea beharrezkoa den aldaketak egitea arrisku handiko AA-sistemen zerrendan eta jardunbide debekatuen zerrendan. Gisa bera, beranduenez 2028ko abuztuaren 2an eta hortik aurrera lau urterik behin, Batzordeak ebaluazio bat egin behar du —eta Europako Parlamentuari eta Kontseiluari jakinarazi— zehazteko beharrezkoa ote den aldaketak egitea erregelamendu honen eranskinean jasotako arrisku handiko eremuen zerrendan, gardentasun-betebeharren aplikazio-eremuan jasotako AA-sistemetan, ikuskapen- eta gobernantza-sistemaren eraginkortasunean eta erabilera orokorreko AA-ereduak ikuspegi energetikotik eraginkortasunez garatzeari buruzko normalizazio-dokumentuak eratzeke egindako aurrerapenetan, neurri edo ekintza osagarrien premia ere aztertuta. Azkenik, beranduenez 2028ko abuztuaren 2an, eta hortik aurrera hiru urterik behin, Batzordeak ebaluazio bat egin beharko du zehazteko ea borondatezko jokabide-kodeek zer-nolako eragina eta eraginkortasuna duten arrisku handikoak ez diren AA-sistemei arrisku handiko sistemetarako ezarritako



no sean sistemas de IA de alto riesgo y, posiblemente, otros requisitos adicionales para dichos sistemas de IA.

(175) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo (56).

(176) Dado que el objetivo del presente Reglamento, a saber, mejorar el funcionamiento del mercado interior y promover la adopción de una IA centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a sus dimensiones y efectos, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(177) A fin de garantizar la seguridad jurídica, garantizar un período de adaptación adecuado para los operadores y evitar perturbaciones del mercado, también garantizando la continuidad del uso de los sistemas de IA, es conveniente que el presente Reglamento se aplique a los sistemas de IA de alto riesgo que se hayan introducido en el mercado o se hayan puesto en servicio antes de la fecha general de aplicación del Reglamento únicamente si, a partir de esa fecha, dichos sistemas se ven sometidos a cambios significativos en su diseño o su finalidad prevista. Conviene aclarar que, a este respecto, el concepto de «cambio significativo» debe entenderse como equivalente en sustancia al de «modificación sustancial», que se utiliza únicamente con respecto a los sistemas de IA de alto riesgo de conformidad con el presente Reglamento. Con carácter excepcional y a efectos de la rendición pública de cuentas, los operadores de sistemas de IA que sean componentes de sistemas informáticos de gran magnitud establecidos por los actos jurídicos enumerados en un anexo del presente Reglamento y los operadores de sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas deben adoptar, respectivamente, las medidas necesarias para cumplir los requisitos del

betekizunak aplikatzea sustatzeko, baita, segur aski, halako AA-sistemetakako ezarritako beste betekizun osagarri batzuk aplikatzea sustatzeko ere.

(175) Erregelamendu hau baldintza uniformeetan egikaritzen dela bermatzeko, egikaritze-eskumenak eman behar zaizkio Batzordeari. Eskumen horiek Europako Parlamentuaren eta Kontseiluaren (EB) 182/2011 Erregelamenduari (56) jarraituz egikaritu behar dira.

(176) Erregelamendu honen helburua kontuan hartuta —alegia, barne-merkatuaren funtzionamendua hobetzea eta gizakian oinarritutako AA fidagarri bat har dadin sustatzea, eta, aldi berean, bermatzea Batasunean AA-sistemen eragin kaltegarrien aurrean zorrotz zaintzen direla osasuna, segurtasuna eta Gutunean ezarritako oinarritzko eskubideak, barnean hartuta demokrazia, zuzenbide-estatua eta ingurumenaren babesa, eta, horrekin guztiarekin batera, berrikuntza ere bultzatzea—, estatu kideak ezin dira horretara guztira behar bezala iritsi; aitzitik, erregelamendu horren helburuaren neurria eta eraginak kontuan hartuta, helburua hobeto lor daiteke Batasunaren mailan jardunda; izan ere, Batasunak neurri egokiak har ditzake, EBTren 5. artikuluan ezarritako subsidiariorotasun-printzipioarekin bat etorrita. Artikulu horretan bertan jasota dagoen proportzionaltasun-printzipioaren arabera, erregelamendu hau ez da helburua lortzeko beharrezkoa den neurriaz gainekoa.

(177) Segurtasun juridikoa bermatzeko, operadoreentzako egokitze-aldi aproposa bermatzeko eta merkatuan gorabeherak saihesteko, eta, aldi berean, AA-sistemak erabiltzen jarraitzen direla bermatzeko, komenigarria da erregelamendu hau aplikatzen hasteko data orokorraren aurretik merkatuan jarri diren edo zerbitzuan ipini diren arrisku handiko AA-sistemetan ere aplikatzea, betiere baldin eta data horretatik aurrera sistema horien diseinuan edo helburu aurreikusian aldaketa nabarmenak egin behar badira. Ohartarazi behar da «aldaketa nabarmena», izatez, «funtsezko aldaketaren» baliokidetzat ulertu behar dela, zeina erregelamendu honen arabera arrisku handikoak diren AA-sistemen kasuan bakarrik erabiltzen baita. Salbuespen modura eta kontu-emate publikoari begira, bai AA-sistemen operadoreek —sistema horiek erregelamendu honetako eranskin batean zerrendatutako egintza juridikoek ezarritako magnitude handiko sistema informatikoen osagai diren heinean—, bai agintaritza publikoen erabilerarako arrisku handiko AA-sistemen operadoreek behar diren neurriak hartu behar dituzte, hurrenez hurren, erregelamendu honetako betekizunak betetzeko 2030. urtearen amaiera baino lehen eta, beranduenez, 2030eko abuztuaren 2a baino lehen.



presente Reglamento antes del final de 2030 y, a más tardar el 2 de agosto de 2030.

(178) Se anima a los proveedores de sistemas de IA de alto riesgo a que empiecen a cumplir, de forma voluntaria, las obligaciones pertinentes del presente Reglamento ya durante el período transitorio.

(179) El presente Reglamento debe aplicarse a partir del 2 de agosto de 2026. No obstante, teniendo en cuenta el riesgo inaceptable asociado a determinadas formas de uso de la IA, las prohibiciones, así como las disposiciones generales del presente Reglamento, deben aplicarse ya desde el 2 de febrero de 2025. Aunque dichas prohibiciones no surtan pleno efecto hasta después del establecimiento de la gobernanza y la aplicación del presente Reglamento, es importante anticipar la aplicación de las prohibiciones para tener en cuenta los riesgos inaceptables y adaptar otros procedimientos, por ejemplo, en el ámbito del Derecho civil. Además, la infraestructura relacionada con la gobernanza y el sistema de evaluación de la conformidad deben estar operativos antes de esa fecha, por lo que las disposiciones relativas a los organismos notificados y la estructura de gobernanza deben ser aplicables a partir del 2 de agosto de 2026. Dada la rápida evolución tecnológica y el elevado ritmo de adopción de modelos de IA de uso general, las obligaciones de los proveedores de modelos de IA de uso general deben aplicarse desde el 2 de agosto de 2025. Los códigos de buenas prácticas deben estar finalizados a más tardar el 2 de mayo de 2025 al objeto de permitir a los proveedores demostrar el cumplimiento de sus obligaciones dentro del plazo previsto. La Oficina de IA debe velar por que las normas y los procedimientos de clasificación estén actualizados con arreglo a los avances tecnológicos. Asimismo, los Estados miembros deben establecer y poner en conocimiento de la Comisión las normas referentes a las sanciones, incluidas las multas administrativas, y asegurarse de que para la fecha de aplicación del presente Reglamento se apliquen de manera adecuada y efectiva. Por lo tanto, las disposiciones relativas a las sanciones deben aplicarse a partir del 2 de agosto de 2025.

(180) El Supervisor Europeo de Protección de Datos y el Comité Europeo de Protección de Datos, a los que se consultó de conformidad con el artículo 42, apartados 1 y 2, del Reglamento (UE) 2018/1725, emitieron su dictamen conjunto el 18 de junio de 2021.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

(178) Bultza egiten zaie arrisku handiko AA-sistemen hornitzaileei trantsizio-aldian jada erregelamendu honetatik dagozkien betebeharrak betetzen has daitezen beren borondatez.

(179) Erregelamendu hau 2026ko abuztuaren 2tik aurrera aplikatu behar da. Dena dela, kontuan hartuta AAren erabilera-modu batzuei lotutako arriskua ezin onartuzkoa dela, erregelamendu honen debekuak eta xedapen orokorrak 2025eko otsailaren 2tik aurrera aplikatu behar dira jada. Nahiz eta debeku horiek ondoriorik eragin ez harik eta erregelamendu honen gobernantza eta aplikazioa ezarri arte, garrantzitsua da debekuak aurrez aplikatzen hastea, arrisku onartezinak kontuan hartzeko eta beste prozedura batzuk — adibidez, zuzenbide zibilaren arlokoak — abian jartzeko. Gainera, gobernantzarekin lotutako azpiegiturek eta adostasuna ebaluatzeko sistemek abian egon behar dute data horren aurretik; beraz, organismo jakinaraziei eta gobernantza-egiturari lotutako xedapenek 2026ko abuztuaren 2tik aurrera aplikatzeko moduan egon behar dute. Bilakaera teknologikoa hain azkarra izanik eta erabilera orokorreko AA-ereduak hartzeko erritmoa hain bizia, 2025eko abuztuaren 2tik aurrera aplikatu behar dira erabilera orokorreko AA-ereduen hornitzaileen betebeharrak. Jardunbide egokien kodeek, beranduenez, 2025eko maiatzaren 2rako egon behar dute amaituta, hornitzaileek beren betebeharrak epe barruan bete dituztela egiaztatu ahal izan dezaten. AA-bulegoak berariaz zaindu behar du sailkapen-arauak eta -prozedurak aurrerapen teknologikoei jarrikiz eguneratuta daudela. Era berean, estatu kideek zehapenei dagozkien arauak ezarri eta Batzordeari jakinarazi behar dizkiote (isun administratiboak ere zehapenen barruan sartzen dira), eta ziurtatu behar dute erregelamendu hau aplikatzen hasten den datarako egokiro eta eraginkortasunez ezartzen direla. Horrela, bada, zehapenei dagozkien xedapenak 2025eko abuztuaren 2tik aurrera aplikatu behar dira.

(180) Datuak Babesteko Europako Ikuskatzaileak eta Datuak Babesteko Europako Komiteak 2021eko ekainaren 18an eman zuten irizpena —bi-biei egin baitzitzaien kontsulta, (EB) 2018/1725 Erregelamenduaren 42. artikulua 1. eta 2. paragrafoekin bat etorrira—.

ERREGELAMENDU HAU EMAN DUTE:

I. KAPITULUA



DISPOSICIONES GENERALES

Artículo 1.— Objeto

1. El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación.
2. El presente Reglamento establece:
 - a) normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión;
 - b) prohibiciones de determinadas prácticas de IA;
 - c) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;
 - d) normas armonizadas de transparencia aplicables a determinados sistemas de IA;
 - e) normas armonizadas para la introducción en el mercado de modelos de IA de uso general;
 - f) normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento;
 - g) medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes.

Artículo 2.— Ámbito de aplicación

1. El presente Reglamento se aplicará a:
 - a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la Unión, con independencia de si dichos proveedores están establecidos o ubicados en la Unión o en un tercer país;
 - b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión;

XEDAPEN OROKORRAK

1. artikulua.— Xedea

1. Erregelamendu honen xedea da barne-merkatuaren funtzionamendua hobetzea eta gizakian oinarritutako adimen artifizial (AA) fidagarria garatzea, aldi berean, babes-maila handia bermatuta, bai osasunaren eta segurtasunaren arloetan, bai Gutunean jasotako oinarritzko eskubideen eremuan —haien barruan direla demokrazia, zuzenbide-estatua eta ingurumenaren babesa— Batasuna AA-sistemen ondorio kaltegarrietatik babesteko, eta, horrekin guztiarekin batera, berrikuntzarako laguntza ematea.
2. Erregelamendu honek alderdi hauek ezartzen ditu:
 - a) Batasunean AA-sistemak merkatuan jartzeko, zerbitzuan ipintzeko eta erabiltzeko arau harmonizatuak.
 - b) AA-jardunbide jakin batzuetarako debekuak.
 - c) Arrisku handiko AA-sistemarako betekizun zehatzak eta sistema horien operadoreentzako betebeharrak.
 - d) AA-sistema jakin batzuei aplikatzekoak zaizkien gardentasuneko arau harmonizatuak.
 - e) Erabilera orokorreko AA-ereduak merkatuan jartzeko arau harmonizatuak.
 - f) Merkatuaren jarraipenari, merkatuaren zaintzari, gobernantzari eta betearazteari buruzko arauak.
 - g) Berrikuntzari laguntzeko neurriak, arreta berezia emanda ETEei —enpresa emergenteak ere barne—.

2. artikulua.— Aplikazio-eremua

1. Hauek izango dira erregelamenduaren aplikazio-eremua:
 - a) Batasunean AA-sistema bat merkatuan jartzen edo zerbitzuan ipintzen duten hornitzaileak edo erabilera orokorreko AA-ereduak merkatuan jartzen dituztenak —hornitzaile horiek Batasunean ezarrita edo kokatuta egon zein hirugarren herrialde batean egon—.
 - b) AA-sistemen hedapenaren arduradunak, Batasunean ezarrita edo kokatuta badaude.



c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión;

d) los importadores y distribuidores de sistemas de IA;

e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca;

f) los representantes autorizados de los proveedores que no estén establecidos en la Unión;

g) las personas afectadas que estén ubicadas en la Unión.

2. A los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 1, y relativos a productos regulados por los actos legislativos de armonización de la Unión enumerados en la sección B del anexo I, únicamente se les aplicará el artículo 6, apartado 1, y los artículos 102 a 109 y el artículo 112. El artículo 57 se aplicará únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo en virtud del presente Reglamento se hayan integrado en dichos actos legislativos de armonización de la Unión.

3. El presente Reglamento no se aplicará a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afectará a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado el desempeño de tareas en relación con dichas competencias.

El presente Reglamento no se aplicará a los sistemas de IA que, y en la medida en que, se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

El presente Reglamento no se aplicará a los sistemas de IA que no se introduzcan en el mercado o no se pongan en servicio en la Unión en los casos en que sus resultados de salida se utilicen en la Unión exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

4. El presente Reglamento no se aplicará a las autoridades públicas de terceros países ni a las

c) AA-sistemen hedapenaren arduradunak, hirugarren herrialde batean ezarrita edo kokatuta egonda ere AA-sistemak sortutako irteera-emaizak Batasunean erabiltzen badira.

d) AA-sistemen inportatzaileak eta banatzaileak.

e) Produktuen fabrikatzaileak, baldin eta produktuarekin batera AA-sistema bat merkatuan jartzen edo zerbitzuan ipintzen badute, beren izen eta markarekin.

f) Batasunean ezarrita ez dauden hornitzaileen ordezkari baimenduak.

g) Ukitutako pertsonak, Batasunean kokatuta dauden heinean.

2. Erregelamenduaren 6.1 artikulua arabera arrisku handiko AA-sistema modura sailkatutako AA-sistemei, l. eranskinen B atalean zerrendatutako Batasunaren harmonizazioko lege-egintzek araututako produktuekin lotuta dauden heinean, artikulua hauek bakarrik aplikatuko zaizkie: 6.1 artikulua, 102.etik 109.era bitartekoak eta 112. artikulua. Bestalde, 57. artikulua egoera honetan bakarrik aplikatuko da: erregelamendu honen arabera arrisku handikoak diren AA-sistemetak betekizunak Batasunaren harmonizazioko lege-egintza horietan txertatu badira.

3. Erregelamendu hau ez zaie aplikatuko Batasuneko zuzenbidearen aplikazio-eremutik kanpo geratzen diren eremuei, eta sekula ez die eragingo estatu kideek segurtasun nazionalaren arloan dituzten eskumenei, estatu kideek zeinahi entitate motari agintzen diotela ere eskumen horien inguruko zereginak betetzea.

AA-sistemak erregelamendu honen aplikazio-eremutik kanpo geratuko dira, baldin eta sistema horiek moldatuta zein ez merkatuan jartzeko, zerbitzuan ipintzeko edo erabiltzeko helburu bakarrak helburu militarrek, defentsakoak edo segurtasun nazionalekoak badira erabat, edozein dela ere jardura horiek egiten dituen entitate mota.

Batasuneko merkatuan jartzen edo zerbitzuan ipintzen ez diren AA-sistemak erregelamendu honen aplikazio-eremutik kanpo geratuko dira, baldin eta haien irteera-emaizak Batasunean erabiltzeko helburu bakarrak helburu militarrek, defentsakoak edo segurtasun nazionalekoak badira, edozein dela ere jardura horiek egiten dituen entitate mota.

4. Erregelamendu hau ez zaie aplikatuko, ez hirugarren herrialdeetako agintaritzak publikoei, ez



organizaciones internacionales que entren dentro del ámbito de aplicación de este Reglamento conforme al apartado 1 cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de acuerdos o de la cooperación internacionales con fines de garantía del cumplimiento del Derecho y cooperación judicial con la Unión o con uno o varios Estados miembros, siempre que tal tercer país u organización internacional ofrezca garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas.

5. El presente Reglamento no afectará a la aplicación de las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios que figuran en el capítulo II del Reglamento (UE) 2022/2065.

6. El presente Reglamento no se aplicará a los sistemas o modelos de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad.

7. El Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. El presente Reglamento no afectará a los Reglamentos (UE) 2016/679 o (UE) 2018/1725 ni a las Directivas 2002/58/CE o (UE) 2016/680, sin perjuicio del artículo 10, apartado 5, y el artículo 59 del presente Reglamento.

8. El presente Reglamento no se aplicará a ninguna actividad de investigación, prueba o desarrollo relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio. Estas actividades se llevarán a cabo de conformidad con el Derecho de la Unión aplicable. Las pruebas en condiciones reales no estarán cubiertas por esa exclusión.

9. El presente Reglamento se entenderá sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relativos a la protección de los consumidores y a la seguridad de los productos.

10. El presente Reglamento no se aplicará a las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional.

11. El presente Reglamento no impedirá que la Unión o los Estados miembros mantengan o introduzcan disposiciones legales, reglamentarias o administrativas que sean más favorables a los trabajadores en lo que

nazioarteko antolakundeei, baldin eta 1. atalaren arabera erregelamendu honen aplikazio-eremuan sartu arren agintaritza edo antolakunde horiek nazioarteko lankidetzaz edo akordio jakin batzuen esparruan erabiltzen badituzte AA-sistemak, betiere akordio edo lankidetzaz horien helburua zuzenbidea betearaztea eta Batasunarekin edo estatu kide batekin edo batzuekin lankidetzaz judiziala ezartzea bada eta hirugarren herrialde edo nazioarteko antolakunde horrek nahikoa berme eskaintzen badu pertsonen oinarritzko eskubideak eta askatasunak babesteko.

5. Erregelamendu honek ez dio eragingo (EB) 2022/2065 Erregelamenduaren II. kapituluari jasotako bitarteko zerbitzuen emailen erantzukizunari buruzko xedapenen aplikazioari.

6. Erregelamendu hau ez zaie aplikatutako AA-sistema edo -ereduei —haien irteera-emaitzak ere barne—, baldin eta sistema horiek garatzeko eta zerbitzuan ipintzeko helburu bakarria ikerketa eta garapen zientifikoa bada.

7. Erregelamendu honetan ezarritako eskubide eta betebeharren arloan tratatutako datu pertsonalei dagokienez, Batasunak datu pertsonalak, intimitatea eta komunikazioen konfidentzialtasuna babesteko ezarritako zuzenbidea aplikatuko da. Erregelamendu honek ez du eraginik izango (EB) 2016/679 eta (EB) 2018/1725 erregelamenduetan, ez eta 2002/58/EE eta (EB) 2016/680 zuzentarauetan ere, hargatik eragotzi gabe erregelamendu honen 10.5 eta 59. artikulua.

8. Erregelamendu hau ez zaio aplikatuko merkatuan jarri edo zerbitzuan ipini aurreko AA-sistemen edo -ereduen ikerketa, proba edo garapeneko inolako jarduerari. Hala, aplikatzeko zaien Batasuneko zuzenbidearen arabera egingo dira jarduerak horiek. Baldintza errealeko probak, baina, ez dira salbuespen horretan sartuko.

9. Erregelamendu honek ez ditu eragotziko kontsumitzaileak babesteko eta produktuen segurtasuna bermatzeko Batasunak xedatutako beste egintza juridiko batzuetan ezarritako arauak.

10. Erregelamendu hau ez zaie aplikatuko hedapenaren arduradunen betebeharrari, baldin eta hedapenaren arduradun horiek AA-sistemak jardun guztiz pertsonal eta ez-profesionalerako bakarrik darabiltzaten pertsona fisikoak badira.

11. Erregelamendu honek ez du eragotziko Batasunak edo estatu kideek lege-, arau- edo administrazio-xedapenak mantentzea edo gehitzea, xedapen horiek langileentzako mesedegarriak diren heinean



atañe a la protección de sus derechos respecto al uso de sistemas de IA por parte de los empleadores ni que fomenten o permitan la aplicación de convenios colectivos que sean más favorables a los trabajadores.

12. El presente Reglamento no se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto, a menos que se introduzcan en el mercado o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 o del artículo 50.

Artículo 3.– Definiciones

A los efectos del presente Reglamento, se entenderá por:

- 1) «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;
- 2) «riesgo»: la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio;
- 3) «proveedor»: una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente;
- 4) «responsable del despliegue»: una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional;
- 5) «representante autorizado»: una persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor;
- 6) «importador»: una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado

enplegatzaileek AA-sistemak erabiltzen dituztenean langileen eskubideak babestu ahal izateko; era berean, ez du eragotziko langileentzako mesedegarriagoak diren hitzarmen kolektiboak sustatzea edo baimentzea.

12. Erregelamendu hau ez zaie aplikatuko lizentzia libre eta kode ireki baten arabera jendarteratzen diren AA-ereduen hornitzaileei, salbu eta arrisku handiko AA-sistema modura edo 5. artikulua edo 50. artikulua erabiltzeko eremuko AA-sistema modura jartzen badira merkatuan edo ipintzen badira zerbitzuan.

3. artikulua.– Definizioak

Erregelamendu honen baitan, esanahi hau izango dute termino hauek:

- 1) «AA-sistema»: Makina batean oinarritutako sistema, autonomia-maila batekin baino gehiagorekin funtzionatzeko diseinatuta dagoena eta hedatu ondoren egokitze-gaitasuna izan dezakeena. Helburu esplizitu zein inplizituetarako, jasotzen duen sarrera-informaziotik abiatuta inferitzen du nola eman irteera-emaizak, hala nola iragarpenak, edukiak, gomendioak eta erabakiak, zeinak ingurune fisiko edo birtualetan izan baitezakete eragina.
- 2) «Arriskua»: Kaltea gertatzeko probabilitatearen eta kalte horren larritasunaren arteko konbinazioa.
- 3) «Hornitzailea»: Pertsona fisiko edo juridiko bat, agintaritza publiko bat edo organo edo organismo bat, zeinak AA-sistema bat edo erabilera orokorreko AA-eredu bat garatzen baitu edo zeinarentzat AA-sistema bat edo erabilera orokorreko AA-eredu bat garatzen baita, gero merkatuan jartzeko edo AA-sistema zerbitzuan ipintzeko bere izen edo markarekin, aurrez ordainduta edo doan.
- 4) «Hedapenaren arduraduna»: Pertsona fisiko edo juridiko bat, agintaritza publiko bat edo organo edo organismo bat, bere agintepean AA-sistema bat erabiltzen duena; kanpoan geratzen da izaera ez-profesionaleko jarduera pertsonal baterako erabilera.
- 5) «Ordezkaritza baimendua»: Batasunean kokatutako edo ezarritako pertsona fisiko edo juridiko bat, idatziz jaso eta onartu duena AA-sistema baten edo erabilera orokorreko AA-eredu baten hornitzaile batek egindako mandatua, erregelamendu honetan ezarritako betebeharrak eta prozedurak bete eta gauzatu ditzan hornitzaile horren ordezkaritza modura.
- 6) «Inportatzailea»: Batasunean kokatutako edo ezarritako pertsona fisiko edo juridiko bat, merkatuan jartzen duena hiru garren herrialde batean ezarritako



un sistema de IA que lleve el nombre o la marca de una persona física o jurídica establecida en un tercer país;

7) «distribuidor»: una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión;

8) «operador»: un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor;

9) «introducción en el mercado»: la primera comercialización en el mercado de la Unión de un sistema de IA o de un modelo de IA de uso general;

10) «comercialización»: el suministro de un sistema de IA o de un modelo de IA de uso general para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, previo pago o gratuitamente;

11) «puesta en servicio»: el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista;

12) «finalidad prevista»: el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica;

13) «uso indebido razonablemente previsible»: la utilización de un sistema de IA de un modo que no corresponde a su finalidad prevista, pero que puede derivarse de un comportamiento humano o una interacción con otros sistemas, incluidos otros sistemas de IA, razonablemente previsible;

14) «componente de seguridad»: un componente de un producto o un sistema de IA que cumple una función de seguridad para dicho producto o sistema de IA, o cuyo fallo o defecto de funcionamiento pone en peligro la salud y la seguridad de las personas o los bienes;

15) «instrucciones de uso»: la información facilitada por el proveedor para informar al responsable del despliegue, en particular, de la finalidad prevista y de la correcta utilización de un sistema de IA;

16) «recuperación de un sistema de IA»: toda medida encaminada a conseguir la devolución al proveedor de un sistema de IA puesto a disposición de los

pertsona físico edo juridiko baten izen edo markako AA-sistema bat.

7) «Banatzailea»: Hornidura-kateko kide den pertsona físico edo juridiko bat, hornitzaileaz edo inportatzaileaz bestelakoa, AA-sistema bat Batasunean merkaturatzen duena.

8) «Operadorea»: Hornitzailea, produktuaren fabrikatzailea, hedapenaren arduraduna, ordezkari baimendua, inportatzailea edo banatzailea.

9) «Merkatuan jartzea»: AA-sistema bat edo erabilera orokorreko AA-eredu bat Batasunean lehenengoz merkaturatzea.

10) «Merkaturatzea»: AA-sistema batez edo erabilera orokorreko AA-eredu batez hornitzea, Batasuneko merkatuan banatzeko edo erabiltzeko, jarduera komertzial baten barruan, aldez aurretik ordainduta edo doan.

11) «Zerbitzuan ipintzea»: Hedapenaren arduraduna zuzenean hornitzea AA-sistema batez, sistema lehenengo aldiz erabiltzeko edo Batasunean erabilera propioa egiteko helburu aurreikusirako.

12) «Helburu aurreikusia»: Hornitzaile batek AA-sistema bat sortu dueneko erabilera, barnean hartuta hala testuinguru eta erabilera-baldintza zehatzak —bat etorrita erabilera-jarraibideetan, materialetan eta sustapen eta salmentako adierazpenetan hornitzaileak emandako informazioarekin— nola dokumentazio teknikoa.

13) «Arrazoiz aurreikus daitekeen erabilera desgokia»: AA-sistema baten helburu aurreikusiarekin bat ez datorren erabilera. Erabilera hori arrazoiz aurreikusgarria den giza portaeraren ondorio izan daiteke edo arrazoiz aurreikusgarria den beste sistema batzuekiko elkarrekintzaren ondorio —beste AA-sistema batzuekiko elkarrekintza barne—.

14) «Segurtasun-osagaia»: Produktu edo AA-sistema baten osagaia, segurtasun-eginkizun bat betetzen duena produktu edo AA-sistema horretan, edo funtzionamendu-hutsegite edo -akatsa edukiz gero arriskuan jartzen duena bai pertsonen osasuna eta segurtasuna, bai ondasunena.

15) «Erabilera-jarraibideak»: Hornitzaileak emandako informazioa, hedapenaren arduradunari aditzera emateko bereziki zein diren AA-sistema baten helburu aurreikusia eta erabilera zuzena.

16) «AA-sistema bat berreskuratzea»: Hedapenaren arduradunaren esku jarritako AA-sistema bat hornitzaileari



responsables del despliegue, a inutilizarlo o a desactivar su uso;

17) «retirada de un sistema de IA»: toda medida destinada a impedir la comercialización de un sistema de IA que se encuentra en la cadena de suministro;

18) «funcionamiento de un sistema de IA»: la capacidad de un sistema de IA para alcanzar su finalidad prevista;

19) «autoridad notificante»: la autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión;

20) «evaluación de la conformidad»: el proceso por el que se demuestra si se han cumplido los requisitos establecidos en el capítulo III, sección 2, en relación con un sistema de IA de alto riesgo;

21) «organismo de evaluación de la conformidad»: un organismo que desempeña actividades de evaluación de la conformidad de terceros, como el ensayo, la certificación y la inspección;

22) «organismo notificado»: un organismo de evaluación de la conformidad notificado con arreglo al presente Reglamento y a otros actos pertinentes de la legislación de armonización de la Unión;

23) «modificación sustancial»: un cambio en un sistema de IA tras su introducción en el mercado o puesta en servicio que no haya sido previsto o proyectado en la evaluación de la conformidad inicial realizada por el proveedor y a consecuencia del cual se vea afectado el cumplimiento por parte del sistema de IA de los requisitos establecidos en el capítulo III, sección 2, o que dé lugar a una modificación de la finalidad prevista para la que se haya evaluado el sistema de IA de que se trate;

24) «mercado CE»: un mercado con el que un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el capítulo III, sección 2, y con otros actos aplicables de la legislación de armonización de la Unión que prevén su colocación;

25) «sistema de vigilancia poscomercialización»: todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recoger y examinar la experiencia obtenida con el uso de sistemas de IA que introducen en el mercado o ponen en servicio, con objeto de detectar la posible necesidad de aplicar

itzularazteko, erabilezin uzteko edo desaktibatzeke neurriak hartzea.

17) «AA-sistema bat erretiratzea»: Hornidura-katean dagoen AA-sistema bat ez merkaturatzeko neurriak hartzea.

18) «AA-sistema baten funtzionamendua»: AA-sistema batek bere helburu aurreikusia lortzeko duen gaitasuna.

19) «Agintaritza jakinarazlea»: Agintaritza nazionala, adostasuna ebaluatzeke organismoen ebaluazio, izendapen eta jakinarazpenerako behar diren prozedurak ezartzeaz eta gauzatzeaz eta organismoak berak ikuskatzeaz arduratzen dena.

20) «Adostasuna ebaluatzea»: Arrisku handiko AA-sistema baten gainean III. kapituluko 2. atalean ezarritako betekizunak bete diren egiaztatzea.

21) «Adostasuna ebaluatzeke organismoa»: Hirugarrenen adostasuna ebaluatzeke jarduerak betetzen dituen organismoa. Jarduera horien artean daude saiakuntza, ziurtapena eta ikuskapena.

22) «Organismo jakinarazia»: Adostasuna ebaluatzeke organismo bat, erregelamendu honen arabera eta Batasunaren harmonizazioko legeriaren beste egintza batzuen arabera jakinarazia.

23) «Funtsezko aldaketa»: AA-sisteman egindako aldakuntza, merkatuan jarri edo zerbitzuan ipini ostekoa, hornitzaileak egindako hasierako adostasunaren ebaluazioan aurreikusi edo proiektatu gabea. Aldaketa horrek AA-sistemari eragiten dio III. kapituluko 2. atalean ezarritako betekizunak betetzeko orduan, edo aldakuntza bat dakar AA-sistemaren ebaluazioaren xede izandako helburu aurreikusian.

24) «CE marka»: Hornitzaile batek erabiltzen duen marka adierazteko AA-sistema bat ados datorrela III. kapituluko 2. atalean ezarritako betekizunekin eta Batasunaren harmonizazioko legeriatik aplikatzekoak diren egintza batzuekin, haren ezarpena aurreikusten duten heinean.

25) «Merkaturatu osteko zaintza-sistema»: AA-sistemen hornitzaileek egiten dituzten jarduera guztiak, merkatuan jartzen edo zerbitzuan ipintzen dituzten AA-sistemen erabilerarekin lortutako esperientzia biltzeko eta aztertzeke, beharrezkoa den edozein neurri



inmediatamente cualquier tipo de medida correctora o preventiva que resulte necesaria;

26) «autoridad de vigilancia del mercado»: la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020;

27) «norma armonizada»: una norma armonizada tal como se define en el artículo 2, punto 1, letra c), del Reglamento (UE) n.o 1025/2012;

28) «especificación común»: un conjunto de especificaciones técnicas tal como se definen en el artículo 2, punto 4, del Reglamento (UE) n.o 1025/2012 que proporciona medios para cumplir determinados requisitos establecidos en virtud del presente Reglamento;

29) «datos de entrenamiento»: los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables;

30) «datos de validación»: los datos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje para, entre otras cosas, evitar el subajuste o el sobreajuste;

31) «conjunto de datos de validación»: un conjunto de datos independiente o una parte del conjunto de datos de entrenamiento, obtenida mediante una división fija o variable;

32) «datos de prueba»: los datos usados para proporcionar una evaluación independiente del sistema de IA, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio;

33) «datos de entrada»: los datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce un resultado de salida;

34) «datos biométricos»: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos;

35) «identificación biométrica»: el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos;

zuzentzaile edo prebentibo berehala aplikatzeko premiarik dagoen detektatze aldera.

26) «Merkatua zaintzeko agintaritza»: Agintaritza nazionala, (EB) 2019/1020 Erregelamenduan aurreikusitako jarduerak gauzatzen eta neurriak hartzen dituen.

27) «Arau harmonizatua»: Arau harmonizatua, (EB) 1025/2012 Erregelamenduaren 2.1 artikuluko c) letran definitutako moduan.

28) «Zehaztapen komuna»: (EB) 1025/2012 Erregelamenduaren 2.4 artikuluan definitzen diren zehaztapen teknikoaren multzoa, erregelamendu honen arabera ezarritako betekizun jakin batzuk betetzeko bitartekoak ematen dituen.

29) «Entrenamendu-datuak»: AA-sistema baten parametro entrenagarriak doitu hura entrenatzeko erabilitako datuak.

30) «Balioztatze-datuak»: Entrenamenduko AA-sistemaren ebaluazioa egiteko eta entrenagarriak ez diren parametroak eta ikaskuntza-prozesua egokitze erabiltzen diren datuak, besteak beste azpidoikuntzarik eta gaingoikuntzarik ez gertatzeko.

31) «Balioztatze-datuaren multzoa»: Datu multzo independente bat, edo entrenamendu-datuaren multzoaren atal bat, zatiketa finko edo aldakor baten bidez lortua.

32) «Proba-datuak»: AA-sistemaren ebaluazio independentea egiteko erabilitako datuak. Ebaluazioaren helburua da ziurtatzea sistema hori aurreikusi bezala dabilela merkatuan jarri edo zerbitzuan ipini aurretik.

33) «Sarrera-datuak»: AA-sistema bati emandako edo sistemak berak zuzenean lortutako datuak, zeinak irteera-emaiza sortzeko baliatzen baititu.

34) «Datu biometrikoak»: Tratamendu tekniko espezifiko baten bitartez lortutako datu pertsonalak, pertsona fisiko baten ezaugarri fisiko, fisiologiko edo portaerazkoei buruzkoak, hala nola aurpegiaren irudiak edo datu daktiloskopikoak.

35) «Identifikazio biometrikoa»: Giza ezaugarri fisiko, fisiologiko, portaerazko edo psikologikoen ezaugarri automatizatua. Helburua da pertsona fisiko baten identitatea zehaztea, datu-base batean gordetako pertsonen datu biometrikoekin alderatuta haren datu biometrikoak.



36) «verificación biométrica»: la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente;

37) «categorías especiales de datos personales»: las categorías de datos personales a que se refieren el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725;

38) «datos operativos sensibles»: los datos operativos relacionados con actividades de prevención, detección, investigación o enjuiciamiento de delitos cuya divulgación podría poner en peligro la integridad de las causas penales;

39) «sistema de reconocimiento de emociones»: un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos;

40) «sistema de categorización biométrica»: un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas;

41) «sistema de identificación biométrica remota»: un sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia;

42) «sistema de identificación biométrica remota en tiempo real»: un sistema de identificación biométrica remota, en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa; engloba no solo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas;

43) «sistema de identificación biométrica remota en diferido»: cualquier sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real;

44) «espacio de acceso público»: cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad;

36) «Egiaztapen biometrikoa»: Pertsona fisikoen identitatearen egiaztapen automatizatua eta bana-banakoa —autentifikazioa barne—, haien datu biometrikoak aurrez emandako datu biometrikoekin alderatuta lortua.

37) «Datu pertsonalen kategoria bereziak»: (EB) 2016/679 Erregelamenduaren 9.1 artikuluan, (EB) 2016/680 Zuzentarauaren 10. artikuluan eta (EB) 2018/1725 Erregelamenduaren 10.1 artikuluan aipatzen diren datu pertsonalen kategoriak.

38) «Bereziki babestutako datu operatiboak»: Delituak prebenitzeko, detektatzeko, ikertzeko edo epaitzeko jardueri lotutako datu operatiboak, zeinen hedapenak arriskuan jar baitezake auzi penalen osotasuna.

39) «Emozioak ezagutzeko sistema»: AA-sistema bat, pertsonen emozioak edo asmoak bereizten edo ondorioztatzen dituen haien datu biometrikoetatik abiatuta.

40) «Kategorizazio biometrikoko sistema»: AA-sistema bat, pertsona fisikoak kategoria espezifikoetan sailkatzen dituen haien datu biometrikoetan oinarrituta. Kanpoan geratzen dira beste zerbitzu komertzial baten osagarri diren eta arrazoi tekniko objektiboengatik ezinbestekoak diren gisa horretako sistemak.

41) «Urruneko identifikazio biometrikoko sistema»: AA-sistema bat, pertsona fisikoak identifikatzekoa, haien parte-hartze aktiborik gabe eta eskuarki urrunetik, pertsonen datu biometrikoak erreferentziako datu-basean agertzen direnekin alderatuta.

42) «Denbora errealean egiten den urruneko identifikazio biometrikoko sistema»: Urruneko identifikazio biometrikoko sistema bat, zeinetan datu biometrikoak jasotzeko, alderatzeko eta identifikatzeko prozesua atzerapen handirik gabe egiten baita; eremu honen barnean sartzen dira bai berehalako identifikazioa, baita atzerapen minimo mugatuak ere, saihesterik egon ez dadin.

43) «Gerora egiten den urruneko identifikazio biometrikoko sistema»: Urruneko identifikazio biometrikoko edozein sistema, denbora errealean egiten den urruneko identifikazio biometrikoko sistema ez dena.

44) «Sarbide publikoko eremua»: Edozein leku fisiko, jabetza publiko edo pribatukoa, zeinetara pertsona fisikoen kopuru zehaztugabe bat sar baitaiteke; bete beharreko sarrera-baldintza zehatzak izan ditzake edo ez, eta edukiera-mugak izan ditzake edo ez.



45) «autoridad garante del cumplimiento del Derecho»:

a) toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, o

b) cualquier otro organismo o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

46) «garantía del cumplimiento del Derecho»: las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

47) «Oficina de IA»: la función de la Comisión consistente en contribuir a la implantación, el seguimiento y la supervisión de los sistemas de IA y modelos de IA de uso general, y a la gobernanza de la IA prevista por la Decisión de la Comisión de 24 de enero de 2024; las referencias hechas en el presente Reglamento a la Oficina de IA se entenderán hechas a la Comisión;

48) «autoridad nacional competente»: una autoridad notificante o una autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a autoridades de vigilancia del mercado se interpretarán como referencias al Supervisor Europeo de Protección de Datos;

49) «incidente grave»: un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias:

a) el fallecimiento de una persona o un perjuicio grave para su salud;

b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas;

45) «Zuzenbidea betearazteko agintaritza»:

a) Agintaritza publiko oro, delituak prebenitzeko, ikertzeko, detektatzeko edo epaitzeko edo zehapen penalak betearazteko eskumena duena, barnean direla segurtasun publikoaren aurkako mehatxuetatik babestea eta mehatxuok prebenitzea; edo

b) beste edozein organismo eta entitate, estatu kideko zuzenbidearen eskutik agintaritza publikoan jarduteko eskumen publikoak baliatzeko ardura jaso duena, delituak prebenitzeko, ikertzeko, detektatzeko edo epaitzeko edo zehapen penalak betearazteko, barnean direla segurtasun publikoaren aurkako mehatxuetatik babestea eta mehatxuok prebenitzea.

46) «Zuzenbidea betearaztea»: Zuzenbidea betearazteko agintaritzek —edo haien izenean dihardutenek— egindako jarduerak, delituak prebenitzeko, ikertzeko, detektatzeko edo epaitzeko edo zehapen penalak betearazteko, barnean direla segurtasun publikoaren aurkako mehatxuetatik babestea eta mehatxuok prebenitzea.

47) «AA-bulegoa»: Batzordearen eginkizuna, helburutzat duena AA-sistemak eta erabilera orokorreko AA-ereduak ezartzen, ikuskatzen eta haien segimendua egiten laguntzea, baita AA gobernatzen laguntzea ere, Batzordearen 2024ko urtarrilaren 24ko Erabakian aurreikusitako moduan. Erregelamendu honetan AA-bulegoari egiten zaizkion erreferentziak Batzordeari egindakotzat ulertuko dira.

48) «Agintaritza nazional eskuduna»: Agintaritza jakinarazle bat edo merkatua zaintzeko agintaritza bat. Batasuneko instituzio, organo eta organismoek erabilitako edo zerbitzuan ipinitako AA-sistemei dagokienez, erregelamendu honetan agintaritza nazional eskudunei edo merkatua zaintzeko agintaritzei egindako erreferentziak Datuak Babesteko Europako Ikuskatzaileari egindakotzat ulertuko dira.

49) «Gorabehera larria»: AA-sistema baten funtzionamenduan jazotako gorabehera edo akatsa, zuzenean edo zeharka honako hauetakoren bat dakarrena:

a) pertsona bat hiltzea edo haren osasunari kalte larria eragitea;

b) azpiegitura kritikoen kudeaketa edo funtzionamendua larriki eta atzera bueltarik gabe nahastea;



c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales;

d) daños graves a la propiedad o al medio ambiente;

50) «datos personales»: los datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

51) «datos no personales»: los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

52) «elaboración de perfiles»: la elaboración de perfiles tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679;

53) «plan de la prueba en condiciones reales»: un documento que describe los objetivos, la metodología, el ámbito geográfico, poblacional y temporal, el seguimiento, la organización y la realización de la prueba en condiciones reales;

54) «plan del espacio controlado de pruebas»: un documento acordado entre el proveedor participante y la autoridad competente en el que se describen los objetivos, las condiciones, el calendario, la metodología y los requisitos para las actividades realizadas en el espacio controlado de pruebas;

55) «espacio controlado de pruebas para la IA»: un marco controlado establecido por una autoridad competente que ofrece a los proveedores y proveedores potenciales de sistemas de IA la posibilidad de desarrollar, entrenar, validar y probar, en condiciones reales cuando proceda, un sistema de IA innovador, con arreglo a un plan del espacio controlado de pruebas y durante un tiempo limitado, bajo supervisión regulatoria;

56) «alfabetización en materia de IA»: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar;

57) «prueba en condiciones reales»: la prueba temporal de un sistema de IA para su finalidad prevista en condiciones reales, fuera de un laboratorio u otro entorno de simulación, con el fin de recabar datos sólidos y fiables y evaluar y comprobar la conformidad del sistema de IA con los requisitos del presente

c) ez betetzea oinarritzko eskubideak babesteko Batasuneko zuzenbideak ezarritako betebeharrak;

d) kalte larriak eragitea jabetzari edo ingurumenari.

50) «Datu pertsonalak»: Datu pertsonalak, (EB) 2016/679 Erregelamenduaren 4.1 artikuluan definitzen diren moduan.

51) «Datu ez-pertsonalak»: Pertsonalak ez diren datuak, (EB) 2016/679 Erregelamenduaren 4.1 artikuluan definitzen diren moduan.

52) «Profilaketa»: Profilak lantzea, (EB) 2016/679 Erregelamenduaren 4.4 artikuluan definitzen den moduan.

53) «Baldintza errealeko probaren plana»: Dokumentu bat, zeinetan baldintza errealeko probaren hainbat xehetasun zehazten baitira, hala nola helburuak, metodologia, eremu geografikoa eta biztanleria- eta denbora-eremuak, segimendua, antolamendua eta gauzatze-prozesua.

54) «Proba-ingurunearen plana»: Dokumentu bat, hornitzaile parte-hartzailearen eta agintaritza eskudunaren artean adostua, zeinetan proba-ingurunean egindako jardueren helburuak, baldintzak, egutegia, metodologia eta betekizunak azaltzen baitira.

55) «AArako proba-ingurune arautua»: Agintaritza eskudun batek ezarritako esparru kontrolatua, AA-sistemen hornitzaileei eta hornitzaile potentzialei aukera ematen diena AA-sistema berritzaile bat garatzeko, entrenatzeko, balioztatze eta probatzeko, egoera errealetan —hala badagokio—, proba-ingurunearen plan baten arabera, denbora mugatu batez eta arau-ikuskapenaren pean.

56) «AAren arloko alfabetatzea»: AAren arloko gaitasunak, ezagutzak eta ulermena, zeinen bidez hornitzaileek, hedapenaren arduradunek eta ukitutako gainerako pertsonak aukera baitute —erregelamendu honi jarraikiz haietako bakoitzari dagozkion eskubide eta betebeharren arabera— AA-sistemen hedapen informatua egiteko eta AAk dakartzan aukerez eta arriskuez jabetzeko, baita eragin ditzakeen kalteez ohartzeko ere.

57) «Baldintza errealeko proba»: AA-sistema bat denbora-tarte batean probatzea, sistemak, laborategitik edo bestelako simulazio-inguruneetatik kanpo, baldintza errealetan izango duen helburu aurreikusia betetzen duen aztertze, hartara datu sendo eta fidagarriak jasotzeko eta AA-sistemak erregelamendu honen



Reglamento; si se cumplen todas las condiciones establecidas en el artículo 57 o 60, no se considerará una introducción en el mercado o una puesta en servicio del sistema de IA en el sentido de lo dispuesto en el presente Reglamento;

58) «sujeto»: a los efectos de la prueba en condiciones reales, una persona física que participa en la prueba en condiciones reales;

59) «consentimiento informado»: la expresión libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en una determinada prueba en condiciones reales tras haber sido informado de todos los aspectos de la prueba que sean pertinentes para su decisión de participar;

60) «ultrasuplantación»: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos;

61) «infracción generalizada»: todo acto u omisión contrario al Derecho de la Unión por el que se protegen los intereses de las personas y que:

a) haya perjudicado o pueda perjudicar los intereses colectivos de personas que residen en al menos dos Estados miembros distintos de aquel en el que:

i) se originó o tuvo lugar el acto u omisión,

ii) esté ubicado o establecido el proveedor de que se trate o, en su caso, su representante autorizado, o

iii) esté establecido el responsable del despliegue en el momento de cometer la infracción;

b) haya perjudicado, perjudique o pueda perjudicar los intereses colectivos de las personas y tenga características comunes —incluidas la misma práctica ilícita o la vulneración del mismo interés— y sea cometido simultáneamente por el mismo operador en al menos tres Estados miembros;

62) «infraestructura crítica»: una infraestructura crítica tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2022/2557;

63) «modelo de IA de uso general»: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de

betekizunak betetzen ote dituen ebaluatze eta egiaztatze. Erregelamenduaren 57. edo 60. artikuluetan ezarritako baldintza guztiak betetzen badira, ez da ulertuko AA-sistema merkatuan jartzea edo zerbitzuan ipintzea denik erregelamendu honetan ezarritakoarekin bat etorrita.

58) «Parte-hartzailea»: Baldintza errealeko proben ondorioetarako, proba horietan parte hartzen duen pertsona fisikoa.

59) «Adostasun informatua»: Parte-hartzaileak askatasunez, espezifikoki, ezbairik gabe eta bere borondatez egindako adierazpena, ziurtatzen duena baldintza errealeko proba jakin batean parte hartu nahi duela, parte hartzeko erabakia hartzeko beharrezkoak diren alderdi guztiei buruzko informazioa jaso ostean.

60) «Faltsutze sakona»: AA batek sortutako edo manipulaturako irudi-, audio- edo bideo-eduki bat, benetako pertsona, objektu, toki, entitate edo gertaera baten antzekoa dena eta oker sinetsaraz dezakeena edukia benetakoa edo egiazkoa dela.

61) «Hedadura handiko arau-haustea»: Pertsonen interesak babesteko ezarritako Batasuneko zuzenbidearen aurkako egite edo ez-egite oro, baldintza hauek betetzen direnean:

a) gutxienez bi estatu kidetan bizi diren pertsonen interes kolektiboek kalte egin izana edo kalte egin ahal izatea, baldin eta estatu kide horiek ez badira:

i) egitea edo ez-egitea gertatu zeneko estatua,

ii) hornitzailea edo, bestela, hornitzailearen ordezkari baimendua kokatuta edo ezarrita dagoen estatua, edo

iii) arau-haustea gertatzen den unean hedapenaren arduraduna kokatuta dagoen estatua;

b) pertsonen interes kolektiboek kalte egin izana, kalte egitea edo kalte egin ahal izatea, eta ezaugarri komunak izatea —zilegia ez den jardunbide bera edo interes beraren urraketa barne— eta kalte hori operadore berberak egitea aldi berean gutxienez hiru estatu kidetan.

62) «Azpiegitura kritikoa»: Azpiegitura kritikoa, (EB) 2022/2557 Erregelamenduaren 4.2 artikuluan definitzen den moduan.

63) «Erabilera orokorreko AA-eredua»: AA-eredu bat —barnean hartuta eskala handiko autoikuskapena erabiliz datu-bolumen handi batekin entrenaturako eredua—, orokortasun-maila nabarmena duena eta gai dena



realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado;

64) «capacidades de gran impacto»: capacidades que igualan o superan las capacidades mostradas por los modelos de IA de uso general más avanzados;

65) «riesgo sistémico»: un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor;

66) «sistema de IA de uso general»: un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA;

67) «operación de coma flotante»: cualquier operación o tarea matemática que implique números de coma flotante, que son un subconjunto de los números reales normalmente representados en los ordenadores mediante un número entero de precisión fija elevado por el exponente entero de una base fija;

68) «proveedor posterior»: un proveedor de un sistema de IA, también de un sistema de IA de uso general, que integra un modelo de IA, con independencia de que el modelo de IA lo proporcione él mismo y esté integrado verticalmente o lo proporcione otra entidad en virtud de relaciones contractuales.

Artículo 4.– Alfabetización en materia de IA

Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en que se van a utilizar dichos sistemas.

zeregin ugari egiteko oso modu egokian —edozein dela ere eredu merkatuan jartzeko modua—, eta ondoren era askotako sistemetan eta aplikazioetan txerta daitekeena; kanpoan geratzen dira merkatuan jarri aurretik ikertzeko, garatzeko eta prototipoak sortzeko erabiltzen diren AA-ereduak.

64) «Inpaktu handiko gaitasunak»: Erabilera orokorreko AA-eredu aurreratuenek erakutsitako gaitasunen pareko gaitasunak edo hortik gorakoak.

65) «Arrisku sistemikoa»: Erabilera orokorreko AA-ereduen inpaktu handiko gaitasunen arrisku espezifikoak, eredu horiek ondorio nabarmenak dituzten heinean Batasuneko merkatuan —bai irismen handia dutelako, bai ondorio negatiboak dituztelako edo ondorio negatiboak izatea aurreikus dakiekeelako osasun publikoan, segurtasunean, segurtasun publikoan, oinarritzko eskubideetan edo gizartean oro har— eta arrisku hori eskala handian heda daitekeen heinean balio-kate osoan barrena.

66) «Erabilera orokorreko AA-sistema»: AA-sistema bat, erabilera orokorreko AA-eredu batean oinarritua eta askotariko helburuetarako erabil daitekeena, zuzenean zein beste AA-sistema batzuetan txertatuta.

67) «Koma mugikorrek eragiketa»: Edozein eragiketa edo ataza matematiko, koma mugikorrek zenbakiak inplikatzeko dituen —hau da, zenbaki errealean azpimultzo bat, zeinak, normalean, oinarri finkoko berretzaile oso batekin berretutako doitasun finkoko zenbaki oso batez irudikatzen baitira ordenagailuetan—.

68) «Ondorengo hornitzailea»: AA-eredu bat integratzen duen AA-sistema baten hornitzailea —erabilera orokorreko AA-sistemak ere barne hartuta—. AA-eredua hornitzaileak berak eman dezake eta bertikalki integratuta egon, edo beste entitate batek eman dezake, kontratu-harremanen bitartez.

4. artikulua.– AAren arloko alfabetatzea

AA-sistemaren hornitzaileek edo hedapenaren arduradunek neurri egokiak haratuko dituzte, bai beren langileek, bai beren izenean AA-sistemen funtzionamenduaz eta erabilera arduratzen diren gainerako pertsonen ahalik eta alfabetatze-maila handiena izan dezaten AAren arloan, kontuan hartuta, batetik, pertsona horiek zer-nolako ezagutza tekniko, esperientzia, hezkuntza eta prestakuntza duten eta, bestetik, zer testuingurutan aurreikusten den AA-sistemak erabiltzea eta zein pertsona edo kolektibotan erabiliko diren.

CAPÍTULO II

II. KAPITULUA



PRÁCTICAS DE IA PROHIBIDAS

AA-JARDUNBIDE DEBEKATUAK

Artículo 5.– Prácticas de IA prohibidas

5. artikulua.– AA-jardunbide debekatuak

1. Quedan prohibidas las siguientes prácticas de IA:

1. Debekatuta geratzen dira AA-jardunbide hauek:

a) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

a) AA-sistema bat merkatuan jartzea, zerbitzuan ipintzea edo erabiltzea, baldin eta sistema horrek pertsonen kontzientzia gainditzen duten teknika subliminalak edo engainuzkoak baliatzen baditu pertsonen edo pertsona-kolektiboen portaera funtsetik aldatzeko helburuarekin edo eraginarekin nabarmenki murriztuz pertsonak erabaki informatua hartzeko duten gaitasuna eta pertsona horiei bestela hartuko ez zuketenerabakia harraraziz, eta, ondorioz, pertsona horiei, beste pertsona batzuei edo pertsona-kolektiboei kalte nabarmenak eragiten badizkie edo halako kalteak eragiteko probabilitate nahikoa sortzen badu.

b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;

b) AA-sistema bat merkatuan jartzea, zerbitzuan ipintzea edo erabiltzea, baldin eta pertsona fisiko baten edo pertsona-kolektibo jakin baten adinean edo desgaitasunean oinarritutako kalteberatasunen batez baliatzen bada, edo egoera sozial edo ekonomiko jakin bat erabiltzen badu, pertsona horren edo kolektibo horretako pertsona baten portaera funtsetik aldatzeko helburuarekin edo eraginarekin, eta, ondorioz, pertsona horri edo besteren bati kalte nabarmenak eragiten badizkie edo halako kalteak eragiteko probabilitate nahikoa sortzen badu.

c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

c) AA-sistema bat merkatuan jartzea, zerbitzuan ipintzea edo erabiltzea, pertsona fisikoak edo pertsona-kolektiboak ebaluatzeko edo sailkatzeko denboraldi jakin batez, oinarritzat hartuta pertsona horien portaera sozialaren edo ezaugarri pertsonalen edo izaerazko ezaugarrien gainean hauteman, ondorioztatu edo aurreikusitakoa, halako moduan non hortik ateratako puntuatze sozialak egoera hauetakoren bat edo batzuk eragiten baititu:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente,

i) trataera kaltegarria edo okerra ematea pertsona fisiko edo pertsonen kolektibo jakin batzuei, pertsona horiek loturarik izan gabe datuak jatorriz sortu edo jaso zireneko testuinguruarekin,

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

ii) trataera kaltegarria edo okerra ematea pertsona fisiko edo pertsonen kolektibo jakin batzuei, justifikaziorik gabe edo neurritz gain haien portaera sozialarekin edo portaera horren larritasunarekin alderatuta.

d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose

d) AA-sistema bat pertsona fisikoen arriskuen ebaluazioa egiteko jartzea merkatuan, ipintzea zerbitzuan edo erabiltzea, arrisku-ebaluazioak egin eta horien bidez pertsona fisiko batek delitu bat egiteko zer arrisku duen balioesteko edo aurreikusteko, oinarri



únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad;

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;

h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,

iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a

bakartzat erabiltza pertsona fisikoaren profila edo haren nortasunaren bereizgarri edo ezaugarriak. Halako AA-sistemei ez zaie debeku hori ezarriko, baldin eta pertsona batek delitu-jarduera batean zer inplikazio duen jakiteko giza balioespenean laguntzeko erabiltzen badira baina balioespene delitu-jarduera batekin zuzenean lotutako gertaera objektibo eta egiaztagarrietan oinarrituta badago jada.

e) AA-sistemak merkatuan jartzea, zerbitzuan ipintzea edo erabiltzea, baldin eta sistema horien helburu zehatza bada Internetetik edo telebista-zirkuitu itxietatik aurpegiko irudiak hautaketarik gabe erauztea aurpegia ezagutzeko datu-baseak sortzeko edo zabaltzeko.

f) AA-sistemak pertsona fisiko bati lanleketan edo hezkuntza-zentroetan emozioak eragiteko jartzea merkatuan, horretarako ipintzea zerbitzuan edo erabiltzea. Salbuespena izango da AA-sistema osasuneko edo segurtasuneko arrazoiengatik instalatzekoa edo merkatuan jartzekoa denean.

g) Kategorizazio biometrikoko sistemak merkatuan jartzea, zerbitzuan ipintzea edo erabiltzea, baldin eta sistema horiek pertsona fisikoak banaka sailkatzen badituzte pertsona horien datu biometrikoetan oinarrituta, horren arabera deduzitzeko edo ondorioztatzeko zein den haien arraza, iritzi politikoa, afiliazio sindikala, sinesmen erlijioso edo filosofikoa, bizitza sexuala edo orientazio sexuala. Debeku honetatik kanpo geratzen dira legez lortutako datu biometrikoen multzoak —hala nola irudiak— etiketatzea edo filtratzea, baita datu biometrikoak zuzenbidea betearazteko kategorizatzea ere.

h) Zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak erabiltzea. Salbuespen modura, erabilera hori debeku honetatik kanpo geratuko da guztiz beharrezkoa bada xede hauetako bat edo batzuk lortzeko:

i) Bahiketen eta gizakien salerosketako edo esplotazio sexualeko kasuetan, biktima zehatzak bilatzeko modu selektiboan, baita desagertutako pertsonak bilatzeko ere.

ii) Pertsona fisikoen bizitza edo segurtasun fisiko arriskuan jartzen duen mehatxu zehatz, garrantzitsu eta berehalako bati aurre hartzeko edo atentatu terrorista bat gertatzeko mehatxu erreala bati aurre hartzeko —mehatxua une horretan bertan izan zein aurreikusgarria izan—.

iii) Delitu baten susmagarri den pertsona bat aurkitzeko eta identifikatzeko, ondoren ikerketa edo



cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.

2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos:

a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

b) las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), del presente artículo deberá cumplir garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con el Derecho nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.

3. A los efectos del apartado 1, párrafo primero, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en

epaitze penala egin edo zehapen penal bat betearazi ahal izateko II. eranskinean aipatutako delituetak baten batengatik, betiere dena delako estatu kidean delitu horri askatasunaz gabetzeko zehapen bat edo segurtasun-neurri bat badagokio zeinak gehienez lau urteko iraupena izango baitu gutxienez.

Lehenengo paragrafoko h) letrak ez du eragotziko (EB) 2016/679 Erregelamenduaren 9. artikuluan datu biometrikokoak zuzenbidea betearazteaz bestelako helburu batzuekin tratatzeari buruz xedatutakoa.

2. Zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak 1. apartatuko lehenengo paragrafoko h) letran zehaztutako helburuetako edozeinetarako erabiltzean, bakar-bakarrik xede zehatza den pertsonaren identifikazioa berresteko erabili behar da, letra horretan zehaztutako helburuei lotuta, eta alderdi hauek izango ditu kontuan:

a) Sistema erabiltzeko bide eman dezakeen egoera nolakoa den eta, zehazki, sistema erabiliko ez balitz sortuko litzatekeen egoerak nolako larritasuna, zer probabilitate eta zer-nolako munta izango lukeen.

b) Sistema erabiltzeak zer ondorio eta nolako larritasuna, zer probabilitate eta zer munta izango lukeen ukitutako pertsonen eskubideetan eta askatasunean.

Gainenera, zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak artikuluko honetako 1. apartatuko lehenengo paragrafoko h) letran zehaztutako helburuetako edozeinetarako erabiltzean, beharrezkoak diren eta neurrizkoak diren berme eta baldintza guztiak bete beharko dira, bat etorrita erabilera hori baimentzen duen zuzenbide nazionalarekin, zehazki muga tenporal, geografiko eta pertsonalei dagokienez. Sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak erabiltzeko baimena emateko, ezinbestekoa izango da zuzenbidea betearazteko agintaritzak aurrez ebaluatzea zer inpaktu izango duen baliabide horrek oinarritzko eskubideetan, 27. artikuluan xedatutakoaren arabera, eta sistema EBren datu-basean erregistratuta edukitzea, 49. artikulukoaren arabera. Dena dela, behar bezala justifikatutako urgentziatzeko kasuetan, sistema horiek EBren datu-basean erregistratu gabe erabiltzen hasi ahal izango da, betiere gerora bidegabeko atzerapenik gabe erregistratzen badira.

3. Kontuan hartzeko 1. apartatuko lehenengo paragrafoko h) letran eta 2. apartatuan zehaztutakoa, zuzenbidea betearazteko helburuz sarbide publikoko



espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le aporten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos especificados en el apartado 1, párrafo primero, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el apartado 2. Dicha autoridad no podrá adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota «en tiempo real».

4. Sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

5. Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho dentro de los límites y en las condiciones que se indican en el apartado 1, párrafo primero, letra h), y los apartados 2 y 3. Los Estados miembros de que se trate deberán establecer en sus respectivos Derechos nacionales las

eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistema bat erabiltzen den aldi oro, agintaritza judizial batek edo erabaki loteslea duen agintaritza administratibo independente batek baimena eman beharko du aurrez, eta agintaritza horren erabakia loteslea izango da sistema hori erabiliko duen estatu kidearentzat. Baimena emateko, aurrez eskaera motibatua egin beharko da, ados etorrita 5. apartatuan zehaztutako zuzenbide nazionalako arauekin. Dena den, behar bezala justifikatutako urgentziatzko egoeretan, baimen hori gabe erabiltzen hasi ahal izango da sistema; alabaina, bidegabeko atzerapenik gabe eskatu beharko da baimena, gehienez ere hogeita lau orduko epean. Baimena ukatuz gero, berehala utziko zaio sistema erabiltzeari, eta berehala bota eta ezabatuko dira datu guztiak, baita sistemaren bidez lortutako emaitzak eta irteera-informazioa ere.

Eskumeneko agintaritza judizialak edo erabaki loteslea duen agintaritza administratibo independente batek baimena eman dezan, seguru jakin beharko du, ematen zaizkion froga objektibo edo zantzu argietan oinarrituta, «denbora errealean egiten den» urruneko identifikazio biometrikoko sistema beharrezkoa eta neurrikoa dela 1. apartatuko lehenengo paragrafoko h) letran zehaztutako helburuetakoren bat lortzeko —eskaeran adieraziko da zein den helburua—, eta zehatz begiratuko du sistemak behar-beharrezko denbora, eremu geografiko eta eremu pertsonala baino hartzen ez duela. Erabakia emateko orduan, 2. atalean adierazitako alderdiak hartuko ditu kontuan agintaritzak. Agintaritza horrek ezin izango du sekula hartu erabakirik, pertsona bati ondorio juridiko kaltegarriren bat eragingo dionik, erabaki horren oinarri bakarra «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemaren irteera-emaitzak izanda.

4. Kalte egin gabe 3. apartatuan xedatutakoari, zuzenbidea betearazteko helburuz «denbora errealean egiten den» urruneko identifikazio biometrikoko sistema erabiltzen denean sarbide publikoko eremuetan, horren berri emango zaie bai merkatua zaintzeko dagokion agintaritzari, bai datuak babesteko agintaritza nazionalari, 5. apartatuan jasotako arau nazionalekin bat etorrita. Jakinarazpenak 6. paragrafoan zehaztutako informazioa jasoko du gutxienez, eta ez du jasoko bereziki babestutako datu operatiborik.

5. Estatu kideek erabakimena izango dute baimena emateko —osorik edo zati batean— zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistema erabil dadin, betiere 1. apartatuko lehenengo paragrafoko h) letran eta 2. eta 3. apartatuetan zehaztutako mugen eta baldintzen barruan. Estatu kideek behar diren arau zehaztuak ezarri beharko dituzte, nork bere zuzenbide nazionalen, aplikatu ahal



normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión y la presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho. Los Estados miembros notificarán dichas normas a la Comisión a más tardar treinta días después de su adopción. Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

6. Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho con arreglo al apartado 4 presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o una autoridad administrativa independiente cuya decisión sea vinculante en relación con las solicitudes de autorización de conformidad con el apartado 3, así como su resultado.

7. La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho elaborados basados en datos agregados relativos a los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de garantía del cumplimiento del Derecho conexas.

8. El presente artículo no afectará a las prohibiciones aplicables cuando una práctica de IA infrinja otras disposiciones de Derecho de la Unión.

izan daitezen 3. apartatuan adierazitako eskaera egiteko, baimena emateko eta baimena baliatzeko prozeduretan, baita prozedura horiekin lotutako ikuskarpenean eta txostenen aurkezpenean ere. Arau horietan zehaztuko da, halaber, 1. apartatuko lehenengo paragrafoko h) letran zerrendatutako zer helburutarako —eta, hala badagokio, h) letrak o iii) tartekian adierazitako zer delituri lotuta— baimendu ahal izango zaien eskumeneko agintaritzei sistema horiek zuzenbidea betearazteko erabiltzea. Estatu kideek arau horien berri emango diote Batzordeari, beranduenez arauak onartu eta hogeita hamar egunera. Estatu kideek, Batasuneko zuzenbidearekin bat etorritik, lege murriztaileagoak onartu ahal izango dituzte urruneko identifikazio biometrikoko sistemen erabilerrari buruz.

6. Estatu kideetako datuak babesteko agintaritzak nazionalak eta merkatua zaintzeko agintaritzak nazionalak, zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistema bat erabiliko dela jakinarazten zaienean, 4. apartatuarekin bat etorritik, erabilera horren gaineko txostena aurkeztuko diote urtero Batzordeari. Horretarako, Batzordeak eredu bat jarriko du estatu kideen eta merkatua zaintzeko eta datuak babesteko agintaritzak nazionalen eskura, eta eredu horretan jasoko da zenbat erabaki hartu dituzten eskumeneko agintaritzak judizialek edo erabaki loteslea duten agintaritzak administratibo independenteek 3. apartatuaren arabera baimen-eskaeren gainean, eta zein izan den erabaki horien emaitza.

7. Batzordeak txostenak argitaratuko ditu urtero zuzenbidea betearazteko helburuz sarbide publikoko eremuetan «denbora errealean egiten den» urruneko identifikazio biometrikoko sistemak erabiltzei buruz, eta, txosten horiek egiteko, 6. apartatuan aipatutako urteko txostenetan oinarrituta estatu kideei buruz jasotako datuak hartuko dira. Urteko txosten horietan ez dira sartuko zuzenbidea betearazteko arlo horri uztartutako jardueren dagokien bereziki babestutako datu operatiboak.

8. Artikulu honek ez die eragingo AA-jardunbide batek Batasuneko zuzenbideko beste xedapen batzuk urratzen dituztenean aplikatzekoak diren debekuei.

CAPÍTULO III

SISTEMAS DE IA DE ALTO RIESGO

SECCIÓN 1

III. KAPITULUA

ARRISKU HANDIKO AA-SISTEMAK

1. ATALA



Clasificación de los sistemas de IA como sistemas de alto riesgo

AA-sistemak arrisku handiko AA-sistematzat sailkatzea

Artículo 6.— Reglas de clasificación de los sistemas de IA de alto riesgo

6. artikulua.— Arrisku handiko AA-sistemak sailkatzeko erregelak

1. Con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación:

a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y

b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I.

2. Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III.

3. No obstante lo dispuesto en el apartado 2, un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones.

El párrafo primero se aplicará cuando se cumpla cualquiera de las condiciones siguientes:

a) que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada;

b) que el sistema de IA esté destinado a mejorar el resultado de una actividad humana previamente realizada;

c) que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o

1. AA-sistema bat a) eta b) letretan aipatutako produktuetan txertatuta egon gabe merkatuan jarri edo zerbitzuan ipini zein ez, arrisku handikotzat joko da honako bi baldintza hauek betetzen baditu:

a) AA-sistema produktu baten segurtasun-osagai gisa erabiltzera bideratuta badago —produktu hori I. eranskinean zerrendatutako Batasunaren harmonizazioko lege-egintzen aplikazio-eremuaren barruan dagoen heinean— edo AA-sistema bera produktu horietako bat bada, eta

b) arestiko a) letraren arabera AA-sistema segurtasun-osagaitzat duen produktuari edo AA-sistema bera den produktuari hirugarrenen adostasunaren ebaluazioa egin behar bazaio, merkatuan jartzeko edo zerbitzuan ipintzeko I. eranskinean zerrendatutako Batasunaren harmonizazioko lege-egintzei jarraikiz.

2. Aurreko 1. apartatuan aipatutako arrisku handiko AA-sistemez gain, III. eranskinean jasotakoak ere arrisku handiko AA-sistematzat joko dira.

3. Aurreko 2. apartatuan xedatutakoa gorabehera, III. eranskinean jasotako AA-sistemak ez dira arrisku handikotzat joko ez badakarte arrisku handirik kaltea eragiteko pertsona fisikoen osasunean, segurtasunean edo oinarritzko eskubideetan, edo ez badute errotik eragiten erabakiak hartzeko emaitzetan.

Lehenengo paragrafoa honako baldintza hauetako edozein betetzen denean aplikatuko da:

a) AA-sistema prozedura-zeregin mugatu bat egitera bideratuta egotea;

b) AA-sistema aurrez egindako giza jarduera bat hobetzera bideratuta egotea;

c) AA-sistema erabakiak hartzeko patroiak hautematera bideratuta egotea edo aurrez eratutako erabakiak hartzeko patroiekiko desbideraketak hautematera, eta sistemaren helburua ez izatea aurrez gizakiak egindako balioespena ordeztzea behar den giza ikuskapenik gabe, ezta balioespen horretan eragitea ere, edota



d) que el sistema de IA esté destinado a realizar una tarea preparatoria para una evaluación que sea pertinente a efectos de los casos de uso enumerados en el anexo III.

No obstante lo dispuesto en el párrafo primero, los sistemas de IA a que se refiere el anexo III siempre se considerarán de alto riesgo cuando el sistema de IA efectúe la elaboración de perfiles de personas físicas.

4. El proveedor que considere que un sistema de IA contemplado en el anexo III no es de alto riesgo documentará su evaluación antes de que dicho sistema sea introducido en el mercado o puesto en servicio. Dicho proveedor estará sujeto a la obligación de registro establecida en el artículo 49, apartado 2. A petición de las autoridades nacionales competentes, el proveedor facilitará la documentación de la evaluación.

5. La Comisión, previa consulta al Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»), y a más tardar el 2 de febrero de 2026, proporcionará directrices que especifiquen la aplicación práctica del presente artículo en consonancia con el artículo 96, junto con una lista exhaustiva de ejemplos prácticos de casos de uso de sistemas de IA que sean de alto riesgo y que no sean de alto riesgo.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, añadiendo nuevas condiciones a las establecidas en dicho apartado, o modificando estas, cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del anexo III, pero que no planteen un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas.

7. La Comisión adoptará actos delegados con arreglo al artículo 97 al objeto de modificar el apartado 3, párrafo segundo, del presente artículo, suprimiendo cualquiera de las condiciones establecidas en él, cuando existan pruebas concretas y fiables de que es necesario para mantener el nivel de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento.

8. Ninguna modificación de las condiciones establecidas en el apartado 3, párrafo segundo, adoptada de conformidad con los apartados 6 y 7 del presente artículo, reducirá el nivel global de protección de la salud, la seguridad y los derechos fundamentales previsto en el presente Reglamento, y cualquier modificación garantizará la coherencia con los actos delegados adoptados con arreglo al artículo 7, apartado

d) AA-sistema ebaluazio bat egiteko prestalanetara bideratuta egotea, III. eranskinean zerrendatutako erabilera-kasuei begira.

Lehenengo paragrafoan xedatutakoa gorabehera, III. eranskinean aipatutako AA-sistemak arrisku handikotzat joko dira sistema horiek pertsona fisikoen profilaketak egiten dituztenean.

4. Hornitzaile batek jotzen badu III. eranskinean jasotako AA-sistema bat ez dela arrisku handikoa, sistemaren ebaluazioa dokumentatuko du sistema merkatuan jarri edo zerbitzuan ipini aurretik. Hornitzaile hori 49.2 artikuluan ezarritako erregistratze-betebeharrari lotuta egongo da. Agintaritza nazional eskudunek eskatuta, hornitzaileak ebaluazioaren gaineko dokumentazioa emango du.

5. Batzordeak, Adimen Artifizialaren Europako Kontseiluari (aurrerantzean «AA-kontseilua») galde egin ostean eta beranduenez 2026ko otsailaren 2an, zenbait gidallerro emango ditu, artikulua hau 96. artikuluekin bat etorrita nola aplikatu zehazteko, eta, horrekin batera, zerrenda bat ere emango du xehe-xehe azalduta arrisku handiko AA-sistemen eta arrisku handikoak ez direnen erabileren adibide praktikoak.

6. Batzordeak ahalmena izango du 97. artikulua araberako egintza eskuordetuak bere egiteko, artikulua honen 3. apartatuko bigarren paragrafoa moldatu eta baldintza berriak apartatu horretan ezarritakoetara gehitzeko edo aurrez zeuden baldintza horiek aldatzeko, froga zehatz eta fidagarriak egonez gero baiesteko III. eranskinaren aplikazio-eremuari dagozkion AA-sistemak daudela baina ez dakartela aparteko arriskurik pertsona fisikoen osasunean, segurtasunean edo oinarritzko eskubideetan kaltea eragiteko.

7. Batzordeak 97. artikulua araberako egintza eskuordetuak hartuko ditu, artikulua honen 3. apartatuaren bigarren paragrafoa moldatze aldera, hartan ezarritako baldintzetako edozein ezabatze, froga zehatz eta fidagarriak egonez gero baiesteko beharrezkoa dela erregelamendu honetan osasunerako, segurtasunerako eta oinarritzko eskubideetarako aurreikusitako babes-mailari eusteko.

8. Hala, 3. apartatuaren bigarren paragrafoan ezarritako baldintzetan artikulua honen 6. eta 7. apartatuen arabera egindako aldaketek ez dute sekula murriztuko erregelamendu honetan osasunerako, segurtasunerako eta oinarritzko eskubideetarako aurreikusitako babes-maila orokorra, eta egiten den aldaketa oro bat etorriko da 7. artikuluko 1. apartatuaren



1, y tendrá en cuenta la evolución tecnológica y del mercado.

Artículo 7.– Modificaciones del anexo III

1. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo III mediante la adición o modificación de casos de uso de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) que los sistemas de IA estén destinados a ser utilizados en cualquiera de los ámbitos que figuran en el anexo III, y

b) que los sistemas de IA planteen un riesgo de perjudicar la salud y la seguridad o de tener repercusiones negativas en los derechos fundamentales, y que dicho riesgo sea equivalente a, o mayor que, el riesgo de perjuicio o de repercusiones negativas que plantean los sistemas de IA de alto riesgo que ya se mencionan en el anexo III.

2. Cuando evalúe la condición prevista en el apartado 1, letra b), la Comisión tendrá en cuenta los criterios siguientes:

a) la finalidad prevista del sistema de IA;

b) la medida en que se haya utilizado o sea probable que se utilice un sistema de IA;

c) la naturaleza y la cantidad de los datos tratados y utilizados por el sistema de IA, en particular si se tratan categorías especiales de datos personales;

d) el grado de autonomía con el que actúa el sistema de IA y la posibilidad de que un ser humano anule una decisión o recomendaciones que puedan dar lugar a un perjuicio;

e) la medida en que la utilización de un sistema de IA ya haya causado un perjuicio a la salud y la seguridad, haya tenido repercusiones negativas en los derechos fundamentales o haya dado lugar a problemas importantes en relación con la probabilidad de dicho perjuicio o dichas repercusiones negativas, según demuestren, por ejemplo, los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes o cualquier otro informe, según proceda;

f) el posible alcance de dicho perjuicio o dichas repercusiones negativas, en particular en lo que respecta a su intensidad y su capacidad para afectar a varias personas o afectar de manera desproporcionada a un determinado colectivo de personas;

arabera hartutako egintza eskuordetuekin, eta aintzat hartuko du teknologiaren eta merkatuaren eboluzioa.

7. artikulua.– III. eranskinaren aldaketak

1. Batzordeak ahalmena izango du 97. artikuluaaren arabera egintza eskuordetuak bere egiteko, III. eranskina moldatu eta arrisku handiko AA-sistemen erabilera-kasuak gehitze edo aldatze aldera, bi baldintza hauek betetzen direnean:

a) AA-sistemak III. eranskinean jasotako eremuetako edozeinetan erabiltzera bideratuta egotea, eta

b) AA-sistemek osasunari edo segurtasunari kalte egiteko edo oinarritzko eskubideetan ondorio kaltegarriak eragiteko arriskua ekartzea eta arrisku hori III. eranskinean jada aipatutako arrisku handiko AA-sistemen kalte-arriskuen edo ondorio kaltegarrien parekoa edo handiagoa izatea.

2. Batzordeak, 1. apartatuaren b) letran aurreikusitako baldintza ebaluatzen duenean, irizpide hauek hartuko ditu kontuan:

a) AA-sistemak zer helburu aurreikusi duen.

b) AA-sistema zer neurritan erabili den edo seguruenik zer neurritan erabiliko den.

c) AA-sistemak zer datu mota eta zenbat datu tratatzen eta erabiltzen dituen, batez ere datu pertsonalen kategoría bereziak direnean.

d) AA-sistemak zer autonomia-mailarekin diharduen, eta aukerarik ote dagoen, erabaki batek edo gomendio batzuek kalte eragin badezakete, gizakiek bertan behera uzteko erabaki edo gomendio horiek.

e) AA-sistemaren erabilerak zer neurritan eragin duen jada kaltea osasunean eta segurtasunean, edo zer neurritan izan dituen ondorio kaltegarriak oinarritzko eskubideetan edo zer neurritan eragin dituen arazo garrantzitsuak, kalte edo ondorio kaltegarri horiek jazotzeko probabilitatearekin alderatuta; hala frogatzen denean, adibidez, agintaritzaz nazional eskudunek aurkeztutako txosten edo alegazio dokumentatuen bidez edo beste edozein txostenen bidez, egoki den moduan.

f) Zer irismen izan dezaketen kalte edo ondorio kaltegarri horiek, batez ere intentsitateari begira eta pertsona bati baino gehiagori eragiteko gaitasunari begira, baita pertsonen kolektibo jakin bati neurrigabe eragiteko gaitasunari begira ere.



g) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan del resultado generado por un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicho resultado;

h) la medida en que exista un desequilibrio de poder o las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del responsable del despliegue de un sistema de IA, en particular debido a su situación, autoridad, conocimientos, circunstancias económicas o sociales, o edad;

i) la medida en que sea fácil corregir o revertir el resultado generado utilizando un sistema de IA, teniendo en cuenta las soluciones técnicas disponibles para corregirlo o revertirlo y sin que deba considerarse que los resultados que afectan negativamente a la salud, la seguridad o los derechos fundamentales son fáciles de corregir o revertir;

j) la probabilidad de que el despliegue del sistema de IA resulte beneficioso para las personas, los colectivos o la sociedad en general, y la magnitud de este beneficio, incluidas posibles mejoras en la seguridad de los productos;

k) la medida en que el Derecho de la Unión vigente establezca:

i) vías de recurso efectivas en relación con los riesgos que plantea un sistema de IA, con exclusión de las acciones por daños y perjuicios,

ii) medidas efectivas para prevenir o reducir notablemente esos riesgos.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar la lista del anexo III mediante la supresión de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:

a) que los sistemas de IA de alto riesgo de que se trate ya no planteen riesgos considerables para los derechos fundamentales, la salud o la seguridad, teniendo en cuenta los criterios enumerados en el apartado 2;

b) que la supresión no reduzca el nivel general de protección de la salud, la seguridad y los derechos fundamentales con arreglo al Derecho de la Unión.

g) Kalte edo ondorio kaltegarri horiek jasan dezaketen pertsonak zer neurritan dauden AA-sistema batek sortutako emaitzen mende, batez ere arrazoi praktiko edo juridikoen ondorioz ez denean arrazoizkoa emaitza horri uko egitea.

h) Zer neurritan egon daitekeen botere-desoreka bat, edo kalte edo ondorio kaltegarri horiek jasan ditzaketen pertsonak zer neurritan dauden AA-sistemaren hedapenaren arduradunarekiko kalteberatasunean, bereziki aintzat hartuta haien egoera, agintea, ezagutza, nondiko norako ekonomiko edo sozialak eta adina.

i) Zer neurritan den erraza AA-sistema bat erabiliz sortutako emaitza zuzentzea edo leheneratzea, kontuan hartuta emaitza zuzentzeko edo leheneratzeko dauden soluzio teknikoak. Ez dira erraz zuzentzeko edo leheneratzeko modukotzat joko osasunean, segurtasunean edo oinarritzko eskubideetan eragin kaltegarria duten emaitzak.

j) Zer probabilitate dagoen AA-sistemaren hedapena onuragarria izan dadin pertsonentzat, kolektiboentzat edo gizartearentzat oro har, eta zenbatekoa den onura hori, barruan hartuta produktuen segurtasunean egin daitezkeen hobekuntzak.

k) Zer neurritan ezartzen dituen Batasuneko zuzenbideak:

i) AA-sistemak dakartzan arriskuei aurre egiteko errekurtso-bide efektiboak, kanpoan utzita kalte-galerekiko ekintzak,

ii) arrisku horiek nabarmen prebenitzeko edo murrizteko neurri efektiboak.

3. Batzordeak ahalmena izango du 97. artikulua eraberrak egintza eskuordetuak bere egiteko, III. eranskineko zerrenda moldatze aldera arrisku handiko AA-sistemak ezabatuta bi baldintza hauek betetzen direnean:

a) arrisku handiko AA-sistemek jada ez ekartzea arrisku nabarmenik oinarritzko eskubideetarako, osasunerako edo segurtasunerako, 2. apartatuan zerrendatutako irizpideak kontuan hartuta;

b) AA-sistemak zerrendatik ezabatzeak ez murriztea Batasuneko zuzenbideak osasunaren, segurtasunaren eta oinarritzko eskubideen arloei emandako babes-maila orokorra.

SECCIÓN 2

2. ATALA



Requisitos de los sistemas de IA de alto riesgo

Arrisku handiko AA-sistemen betekizunak

Artículo 8.– Cumplimiento de los requisitos

1. Los sistemas de IA de alto riesgo cumplirán los requisitos establecidos en la presente sección, teniendo en cuenta sus finalidades previstas, así como el estado actual de la técnica generalmente reconocido en materia de IA y tecnologías relacionadas con la IA. A la hora de garantizar el cumplimiento de dichos requisitos se tendrá en cuenta el sistema de gestión de riesgos a que se refiere el artículo 9.

2. Cuando un producto contenga un sistema de IA al que se apliquen los requisitos del presente Reglamento, así como los requisitos de los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, los proveedores serán responsables de garantizar que su producto cumpla plenamente todos los requisitos aplicables en virtud de los actos legislativos de armonización de la Unión que sean aplicables. Para garantizar el cumplimiento de los sistemas de IA de alto riesgo a que se refiere el apartado 1 de los requisitos establecidos en la presente sección, y con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los procesos de prueba y presentación de información necesarios, y la información y la documentación que faciliten con respecto a su producto en documentación y procedimientos que ya existan y exijan los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A.

Artículo 9.– Sistema de gestión de riesgos

1. Se establecerá, implantará, documentará y mantendrá un sistema de gestión de riesgos en relación con los sistemas de IA de alto riesgo.

2. El sistema de gestión de riesgos se entenderá como un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, que requerirá revisiones y actualizaciones sistemáticas periódicas. Constará de las siguientes etapas:

a) la determinación y el análisis de los riesgos conocidos y previsibles que el sistema de IA de alto riesgo pueda plantear para la salud, la seguridad o los derechos fundamentales cuando el sistema de IA de alto riesgo se utilice de conformidad con su finalidad prevista;

b) la estimación y la evaluación de los riesgos que podrían surgir cuando el sistema de IA de alto riesgo se

8. artikulua.– Betekizunak betetzea

1. Arrisku handiko AA-sistemek atal honetan ezarritako betekizunak betetzeko, kontuan hartuko da zer helburu aurreikusi duten eta zein den teknikaren unean uneko egoera orokorra AAren arloan eta AAri lotutako teknologien arloan. Betekizun horiek betetzen direla bermatzeko, 9. artikuluan jasotako arriskuak kudeatzeko sistema hartuko da aintzat.

2. Produktu batek AA-sistema bat duenean eta sistema horri erregelamendu honen betekizunak aplikatzen bazaizkio, bai eta I. eranskineko A atalean jasotako Batasunaren harmonizazioko lege-egintzetako betekizunak ere, hornitzaileak arduratuko dira bermatzeaz produktu horrek erabat betetzen dituela Batasunaren harmonizazioko legeriatik dagozkion egintzen arabera aplikatzekoak zaizkion betekizun guztiak. 1. apartatuan zehaztutako arrisku handiko AA-sistematik atal honetan ezarritako betekizunak betetzen dituztela bermatzeko, eta, horrekin batera, koherentzia ziurtatzeko, bikoiztasunak saihesteko eta karga gehigarriak gutxienekora murrizteko, hornitzaileek aukera izango dute, egoki bada, beharrezkoak diren proba-prozesuak eta informazioa aurkezteko prozesuak txertatzeko beren produktuaren gainean aurrez prestatutako informazioari eta dokumentazioari, zeina beharrezkoa baita I. eranskineko A atalean zerrendatutako Batasunaren harmonizazioko lege-egintzen arabera.

9. artikulua.– Arriskuak kudeatzeko sistema

1. Arrisku handiko AA-sistemen arriskuak kudeatzeko sistema bat ezarri, txertatu, dokumentatu eta mantenduko da.

2. Arriskuak kudeatzeko sistema iterazio-prozesu jarraitutzat ulertu behar da; hala, arrisku handiko AA-sistemaren bizi-ziklo osoan planifikatu eta gauzatuko da, eta aldian-aldian modu sistematikoan ikuskatzea eta eguneratzea eskatuko du. Etapa hauek izango ditu:

a) Zehaztea eta aztertzea zer arrisku ezagun eta aurreikusgarri dakartzan arrisku handiko AA-sistematik osasunerako, segurtasunerako edo oinarritzko eskubideetarako, bere helburu aurreikusien arabera erabiltzen denean.

b) Balioestea eta ebaluatzea zer arrisku sor daitezkeen arrisku handiko AA-sistema bere helburu aurreikusien arabera erabiltzen denean eta arrazoiz



utilice de conformidad con su finalidad prevista y cuando se le dé un uso indebido razonablemente previsible;

c) la evaluación de otros riesgos que podrían surgir, a partir del análisis de los datos recogidos con el sistema de vigilancia poscomercialización a que se refiere el artículo 72;

d) la adopción de medidas adecuadas y específicas de gestión de riesgos diseñadas para hacer frente a los riesgos detectados con arreglo a la letra a).

3. Los riesgos a que se refiere el presente artículo son únicamente aquellos que pueden mitigarse o eliminarse razonablemente mediante el desarrollo o el diseño del sistema de IA de alto riesgo o el suministro de información técnica adecuada.

4. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), tendrán debidamente en cuenta los efectos y la posible interacción derivados de la aplicación combinada de los requisitos establecidos en la presente sección, con vistas a reducir al mínimo los riesgos de manera más eficaz al tiempo que se logra un equilibrio adecuado en la aplicación de las medidas para cumplir dichos requisitos.

5. Las medidas de gestión de riesgos mencionadas en el apartado 2, letra d), considerarán aceptables los riesgos residuales pertinentes asociados a cada peligro, así como el riesgo residual general de los sistemas de IA de alto riesgo.

A la hora de determinar las medidas de gestión de riesgos más adecuadas, se procurará:

a) eliminar o reducir los riesgos detectados y evaluados de conformidad con el apartado 2 en la medida en que sea técnicamente viable mediante un diseño y un desarrollo adecuados del sistema de IA de alto riesgo;

b) implantar, cuando proceda, unas medidas de mitigación y control apropiadas que hagan frente a los riesgos que no puedan eliminarse;

c) proporcionar la información requerida conforme al artículo 13 y, cuando proceda, impartir formación a los responsables del despliegue.

Con vistas a eliminar o reducir los riesgos asociados a la utilización del sistema de IA de alto riesgo, se tendrán debidamente en cuenta los conocimientos técnicos, la experiencia, la educación y la formación que se espera que posea el responsable del despliegue, así como el contexto en el que está previsto que se utilice el sistema.

aurreikus daitekeen erabilera desagoki bat ematen zaionean.

c) Ebaluatzea zer beste arrisku sor daitezkeen, 72. artikuluan azaldutako merkaturatu osteko zaintza-sistemaren bidez jasotako datuen azterketan oinarrituta.

d) Arriskuak kudeatzeko neurri egoki eta zehatzak hartzea, a) letraren arabera hautemandako arriskuei aurre egiteko.

3. Artikulu honetan aipatzen diren arriskuak zorrotz mugatuta daude arrisku handiko AA-sistemaren garapen edo diseinuaren bidez edo informazio tekniko egokiaren bidez arrazoizko moduan leundu edo ezabatu daitezkeen arriskueta.

4. Bestalde, 2. apartatuko d) letran aipatutako arriskuak kudeatzeko neurriek egokiro hartuko dituzte aintzat atal honetan ezarritako betekizunen aplikazio konbinatuaren ondorioz sor daitezkeen eraginak eta interakzioa, ahalik eta gehien eta ahalik eta modu eraginkorrean murrizteko arriskuak, hartara oreka egokia lortzeko betekizun horiek betetzeko neurrien aplikazioan.

5. Horrez gain, 2. apartatuko d) letran aipatutako arriskuak kudeatzeko neurriek onargarritzat joko dituzte arrisku bakoitzak dituen hondar-arriskuak, baita arrisku handiko AA-sistemen hondar-arrisku orokorra ere.

Arriskuak kudeatzeko neurri egokienak zehazteko orduan, jarduketa hauek egiten saiatuko da:

a) 2. apartatuaren arabera hautemandako eta ebaluatutako arriskuak ezabatzen edo murrizten, teknikoki bideragarri den heinean, arrisku handiko AA-sistema egokiro diseinatuta eta garatuta.

b) Arriskuak ezin badira ezabatu, arriskuak leuntzeko eta kontrolatzeko neurriak ezartzen.

c) 13. artikuluaaren arabera informazioa ematen, eta, egoki denean, hedapenaren arduradunei prestakuntza ematen.

Arrisku handiko AA-sistemen erabilerari lotutako arriskuak ezabatzeko edo leuntzeko, behar bezala hartuko da kontuan hedapenaren arduradunak zer esperientzia, heziketa eta prestakuntza edukitzea espero izatekoa den, bai, halaber, zer testuingurutan aurreikusten den sistema erabiltzea.



6. Los sistemas de IA de alto riesgo serán sometidos a pruebas destinadas a determinar cuáles son las medidas de gestión de riesgos más adecuadas y específicas. Dichas pruebas comprobarán que los sistemas de IA de alto riesgo funcionan de manera coherente con su finalidad prevista y cumplen los requisitos establecidos en la presente sección.

7. Los procedimientos de prueba podrán incluir pruebas en condiciones reales de conformidad con el artículo 60.

8. Las pruebas de los sistemas de IA de alto riesgo se realizarán, según proceda, en cualquier momento del proceso de desarrollo y, en todo caso, antes de su introducción en el mercado o puesta en servicio. Las pruebas se realizarán utilizando parámetros y umbrales de probabilidades previamente definidos que sean adecuados para la finalidad prevista del sistema de IA de alto riesgo.

9. Cuando se implante el sistema de gestión de riesgos previsto en los apartados 1 a 7, los proveedores prestarán atención a si, en vista de su finalidad prevista, es probable que el sistema de IA de alto riesgo afecte negativamente a las personas menores de dieciocho años y, en su caso, a otros colectivos vulnerables.

10. En el caso de los proveedores de sistemas de IA de alto riesgo que estén sujetos a requisitos relativos a procesos internos de gestión de riesgos con arreglo a otras disposiciones pertinentes del Derecho de la Unión, los aspectos previstos en los apartados 1 a 9 podrán formar parte de los procedimientos de gestión de riesgos establecidos con arreglo a dicho Derecho, o combinarse con ellos.

Artículo 10.– Datos y gobernanza de datos

1. Los sistemas de IA de alto riesgo que utilizan técnicas que implican el entrenamiento de modelos de IA con datos se desarrollarán a partir de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad a que se refieren los apartados 2 a 5 siempre que se utilicen dichos conjuntos de datos.

2. Los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo. Dichas prácticas se centrarán, en particular, en lo siguiente:

a) las decisiones pertinentes relativas al diseño;

6. Arrisku handiko AA-sistemei proba jakin batzuk ezarriko zaizkie zehazteko zein diren arriskuak kudeatzeko neurri egokienak eta doienak. Proba horien bidez egiaztatuko da arrisku handiko AA-sistemek modu koherentean funtzionatzen dutela beren helburu aurreikusiari begira eta atal honetan ezarritako betekizunak betetzen dituztela.

7. Proba-prozeduren barruan, baldintza errealeko probak ere sartu ahal izango dira, 60. artikularekin bat etorrita.

8. Arrisku handiko AA-sistemetako probak garapen-prozesuaren edozein momentutan egingo dira, betiere merkatuan jarri edo zerbitzuan ipini aurretik. Probak egiteko, arrisku handiko AA-sistemen helburu aurreikusirako aproposak diren parametroak eta probabilitate-atalaseak erabiliko dira, aurrez parametro eta atalase horiek egokiro zehaztuta.

9. Arriskuak kudeatzeko sistema ezartzen denean (1. apartatutik 7.era azalduta), hornitzaileek arreta berezia jarriko dute zehazteko ea sistemen helburu aurreikusiaren arabera probabilitaterik dagoen arrisku handiko AA-sistemak eragin kaltegarria izateko hemezortzi urtetik beherako pertsonetan edo beste kolektibo kaltebera batzuetan.

10. Arrisku handiko AA-sistemetako hornitzaileak Batasuneko zuzenbidearen beste xedapen batzuei dagozkien arrisku-kudeaketako barne-prozesuen betekizunei lotuta badaude, 1. apartatutik 9.era aurreikusitako alderdiak zuzenbide horren arabera ezarritako arrisku-kudeaketako prozeduretan txertatu ahal izango dira, edo prozedura horiekin konbinatu.

10. artikulua.– Datuak eta datuen gobernantza

1. AA-ereduak datuekin entrenatzeko teknikak erabiltzen dituzten arrisku handiko AA-sistemak entrenamendu-, balioztatze- eta proba-datuen multzoen bidez garatuko dira, betiere datu multzoek 2. apartatutik 5.era azaldutako kalitate-irizpideak betetzen dituztela bermatuta datu multzo horiek erabiltzen diren guztietan.

2. Entrenamendu-, balioztatze- eta proba-datuen multzoei arrisku handiko AA-sistemaren helburu aurreikusirako egokiak diren datu-gobernantza eta -kudeaketako jarduketak ezarriko zaizkie. Jarduketa horiek alderdi hauek hartuko dituzte ardatz:

a) Diseinuari buruzko erabakiak hartzea.



b) los procesos de recogida de datos y el origen de los datos y, en el caso de los datos personales, la finalidad original de la recogida de datos;

c) las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, la actualización, el enriquecimiento y la agregación;

d) la formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos;

e) una evaluación de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios;

f) el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones;

g) medidas adecuadas para detectar, prevenir y mitigar posibles sesgos detectados con arreglo a la letra f);

h) la detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del presente Reglamento, y la forma de subsanarlas.

3. Los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la mayor medida posible, carecerán de errores y estarán completos en vista de su finalidad prevista. Asimismo, tendrán las propiedades estadísticas adecuadas, por ejemplo, cuando proceda, en lo que respecta a las personas o los colectivos de personas en relación con los cuales está previsto que se utilice el sistema de IA de alto riesgo. Los conjuntos de datos podrán reunir esas características para cada conjunto de datos individualmente o para una combinación de estos.

4. Los conjuntos de datos tendrán en cuenta, en la medida necesaria para la finalidad prevista, las características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice el sistema de IA de alto riesgo.

5. En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo de conformidad con lo dispuesto en el apartado 2, letras f) y g), del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías

b) Datuak jasotzeko prozesuak eta datuen jatorria zehaztea eta, datu pertsonalen kasuan, datuak jasotzeko jatorrizko helburua ere bai.

c) Datuak prestatzeko egoki diren tratamendu-eragiketak egitea, hala nola oharak hartzea, etiketatzea, araztea, eguneratzea, aberastea eta eranstea.

d) Suposizioak formulatzea, bereziki datuek neurtzen edo adierazten ei duten informazioari dagokionez.

e) Beharrezkoak diren datu multzoak eskuragarri dauden, zenbat diren eta egokiak diren ebaluatzea.

f) Aztertzea ea alborapenen bat dagoen pertsonen osasunari eta segurtasunari eragin diezaikeena, oinarritzko eskubideei kalte egin diezaikeena edo Batasuneko zuzenbideak debekatutako diskriminazioen bat sor dezakeena, bereziki datu-irteerek eragina dutenean etorkizuneko eragiketetako sarrera-informazioetan.

g) Neurri egokiak ezartzea f) letraren arabera egon litezkeen alborapenak hautemateko, prebenitzeko eta leuntzeko.

h) Datuetan erregelamendu hau betetzeko oztopo diren hutsuneak eta urritasunak hautematea, eta huts horiek konpontzeko bidea aurkitzea.

3. Entrenamendu-, balioztatze- eta proba-datuen multzoak egokiak eta behar bezain esanguratsuak izango dira, eta errorerik gabeak eta ahalik eta osoenak ere izango dira, helburu aurreikusia kontuan hartuta. Bestalde, behar diren propietate estatistikoak izango dituzte; adibidez, pertsona edo pertsona-kolektibo jakinen gainean, pertsona horiekin arrisku handiko AA-sistema erabiltzea aurreikusten denean. Datu multzoek ezaugarri horiek eduki ahal izango dituzte, bai datu multzo bakoitzerako, bai datu multzoen konbinazio baterako.

4. Datu multzoek, helburu aurreikusirako behar den neurrian, kontuan hartuko dituzte arrisku handiko AA-sistema erabiltzea aurreikusten den ingurune geografiko, kontestual, konduktual eta funtzionalaren ezaugarri edo osagai bereziak.

5. Arrisku handiko AA-sistemei lotutako alborapenak artikuluko 2. apartatuko f) eta g) letretan zehaztutakoaren arabera hautematen eta zuzentzen direla bermatzeko guztiz beharrezkoa denean, sistema horien hornitzaileek aukera izango dute salbuespenez datu pertsonalen kategoria bereziak tratatzeko, betiere



especiales de datos personales siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas. Además de las disposiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, para que se produzca dicho tratamiento deben cumplirse todas las condiciones siguientes:

a) que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos;

b) que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización;

c) que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas;

d) que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos;

e) que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior;

f) que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.

6. Para el desarrollo de sistemas de IA de alto riesgo que no empleen técnicas que impliquen el entrenamiento de modelos de IA, los apartados 2 a 5 se aplicarán únicamente a los conjuntos de datos de prueba.

Artículo 11.– Documentación técnica

behar diren bermeak ematen badira pertsona fisikoen oinarritzeko eskubideak eta askatasunak babesteko. Tratamendu hori egiteko, (EB) 2016/679 eta (EB) 2018/1725 erregelamenduetan eta (EB) 2016/680 Zuzentarauan ezarritako xedapenez gain, baldintza hauek guztiak bete behar dira:

a) Beste datu batzuk tratatzean, hala nola datu sintetikoak edo anonimizatuak, ez egotea aukerarik alborapenak eraginkortasunez hautemateko eta zuzentzeko.

b) Datu pertsonalen kategoría bereziak lotuta egotea datu pertsonalak berrerabiltzeko muga teknikoetara eta segurtasunaren eta intimitatearen babesaren arloko punta-puntako neurrietara, pseudonimizazioa barne.

c) Datu pertsonalen kategoría bereziak tratatzeko neurri zehatzak ezartzea datu pertsonalak modu seguruan, egokiro babestuta eta behar diren bermeei lotuta tratatzen direla ziurtatzeko, besteak beste kontrol zorrotzak ezarrita eta sarbide-dokumentazioa eskatuta, erabilera desegokirik egin ez dadin eta berma dadin pertsona baimenduek bakarrik dutela irispidea datu pertsonaletara, betiere behar diren konfidentzialtasun-betebeharrak beteta.

d) Datu pertsonalen kategoría bereziak ez bidaltzea eta ez transferitzea hirugarren batzuei, eta hirugarren horiek ez edukitzea modurik datu horiek eskuratzeko.

e) Datu pertsonalen kategoría bereziak ezabatzea, behin alborapena zuzenduta dagoela edo datu pertsonalak gordetzeko aldia amaituta dagoela —data hori lehenago iristen bada—.

f) (EB) 2016/679 eta (EB) 2018/1725 erregelamenduen eta (EB) 2016/680 Zuzentarauaren arabera egindako tratamendu-jardueren erregistroetan jasotzea zergatik zen guztiz beharrezkoa datu pertsonalen kategoría bereziak tratatzea alborapenak hauteman eta zuzentzeko eta zergatik ezin zen lortu helburu hori bera beste datu batzuk tratatuta.

6. Arrisku handiko AA-sistemak garatzeko erabiltzen diren teknikak ez dutenean AA-ereduen entrenamendurik behar, proba-datuen multzoei bakarrik aplikatuko zaizkie 2. apartatutik 5.era bitartekoak.

11. artikulua.– Dokumentazio teknikoak



1. La documentación técnica de un sistema de IA de alto riesgo se elaborará antes de su introducción en el mercado o puesta en servicio, y se mantendrá actualizada.

La documentación técnica se redactará de modo que demuestre que el sistema de IA de alto riesgo cumple los requisitos establecidos en la presente sección y que proporcione de manera clara y completa a las autoridades nacionales competentes y a los organismos notificados la información necesaria para evaluar la conformidad del sistema de IA con dichos requisitos. Contendrá, como mínimo, los elementos contemplados en el anexo IV. Las pymes, incluidas las empresas emergentes, podrán facilitar los elementos de la documentación técnica especificada en el anexo IV de manera simplificada. A tal fin, la Comisión establecerá un formulario simplificado de documentación técnica orientado a las necesidades de las pequeñas empresas y las microempresas. Cuando una pyme, incluidas las empresas emergentes, opte por facilitar la información exigida en el anexo IV de manera simplificada, utilizará el formulario a que se refiere el presente apartado. Los organismos notificados aceptarán dicho formulario a efectos de la evaluación de la conformidad.

2. Cuando se introduzca en el mercado o se ponga en servicio un sistema de IA de alto riesgo asociado a un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión mencionados en el anexo I, sección A, se elaborará un único conjunto de documentos técnicos que contenga toda la información mencionada en el apartado 1, así como la información que exijan dichos actos legislativos.

3. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo IV, cuando sea necesario, para garantizar que, en vista de los avances técnicos, la documentación técnica proporcione toda la información necesaria para evaluar si el sistema cumple los requisitos establecidos en la presente sección.

Artículo 12.– Conservación de registros

1. Los sistemas de IA de alto riesgo permitirán técnicamente el registro automático de acontecimientos (en lo sucesivo, «archivos de registro») a lo largo de todo el ciclo de vida del sistema.

2. Para garantizar un nivel de trazabilidad del funcionamiento del sistema de IA de alto riesgo que resulte adecuado para la finalidad prevista del sistema, las capacidades de registro permitirán que se registren acontecimientos pertinentes para:

a) la detección de situaciones que puedan dar lugar a que el sistema de IA de alto riesgo presente un

1. Arrisku handiko AA-sistema baten dokumentazio teknikoa merkatuan jarri edo zerbitzuan ipini aurretik landuko da, eta eguneratuta edukiko da.

Dokumentazio teknikoan, garbiro frogatu beharko da arrisku handiko AA-sistema horrek atal honetan ezarritako betekizunak betetzen dituela, eta argi eta osoki eman beharko zaie agintaritzaz nazional eskudunei eta organismo jakinaraziei AA-sistema betekizun horiekin ados datorrela ebaluatu ahal izateko behar den informazio guztia. Gutxienez, IV. eranskinean aurreikusitako elementuak izango ditu. ETEek — enpresa emergenteak barne— modu sinplifikatuan aurkeztu ahal izango dituzte IV. eranskinean zehaztutako dokumentazio teknikoaren elementuak. Horretarako, Batzordeak, dokumentazio teknikoaren formulario sinplifikatu bat ezarriko du, enpresa txikien eta mikroenpresen beharretara egokitua. ETE batek — enpresa emergenteak barne— IV. eranskinean zehaztutako informazioa modu sinplifikatuan aurkeztea aukeratzen badu, apartatu honetan zehaztutako formularioa erabiliko du. Organismo jakinaraziek formulario hori onartuko dute adostasuna ebaluatzeko jarduketetarako.

2. I. eranskineko A atalean aipatutako Batasunaren harmonizazioko lege-egintzen aplikazio-eremuan sartzen den produktu bati lotutako arrisku handiko AA-sistema bat merkatuan jartzen edo zerbitzuan ipintzen denean, dokumentu teknikoaren multzo bakarra eratu da, eta dokumentu multzo horretan jasoko da 1. apartatuan aipatutako informazio guztia, baita lege-egintza horiek eskatzen duten informazio guztia ere.

3. Batzordeak ahalmena izango du 97. artikulua eraberrak egintza eskuordetuak bere egiteko, IV. eranskina moldatze aldera, beharrezkoa denean, hartara bermatuta geratzeko aurrerapen teknikoak gertatu ahala dokumentazio teknikoak behar den informazio guztia emango duela sistemak atal honetan ezartzen diren betekizunak betetzen dituen ebaluatzeko.

12. artikulua.– Erregistroak gordetzea

1. Arrisku handiko AA-sistemek teknikoki aukera emango dute gertaeren erregistro automatikoa egiteko (aurrerantzean «erregistro-artxiboak») sistemaren balio-bizitza osoan.

2. Arrisku handiko AA-sistemaren funtzionamenduaren trazabilitate-maila sistemaren helburu aurreikusirako egokia dela bermatzeko, erregistro-gaitasunek modua emango dute helburu hauetarako gertaerak erregistratzeko:

a) Hautemateko zer egoeratan gerta daitekeen arrisku handiko AA-sistemak 79.1 artikulua



riesgo en el sentido del artículo 79, apartado 1, o a una modificación sustancial;

b) la facilitación de la vigilancia poscomercialización a que se refiere el artículo 72, y

c) la vigilancia del funcionamiento de los sistemas de IA de alto riesgo a que se refiere el artículo 26, apartado 5.

3. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las capacidades de registro incluirán, como mínimo:

a) un registro del período de cada uso del sistema (la fecha y la hora de inicio y la fecha y la hora de finalización de cada uso);

b) la base de datos de referencia con la que el sistema ha cotejado los datos de entrada;

c) los datos de entrada con los que la búsqueda ha arrojado una correspondencia;

d) la identificación de las personas físicas implicadas en la verificación de los resultados que se mencionan en el artículo 14, apartado 5.

Artículo 13.– Transparencia y comunicación de información a los responsables del despliegue

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones pertinentes previstas en la sección 3.

2. Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue.

3. Las instrucciones de uso contendrán al menos la siguiente información:

a) la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado;

b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, con inclusión de:

araberako arriskua ekartzea edo funtsezko aldaketa bat eragitea.

b) 72. artikuluan aipatutako merkaturatu osteko zaintza egiteko.

c) Arrisku handiko AA-sistemen funtzionamendua zaintzeko (26.5 artikuluan aipatua).

3. III. eranskinen 1. puntuko a) letran aipatutako arrisku handiko AA-sistemen kasuan, erregistro-gaitasunen barruan, hauek sartutako dira gutxienez:

a) Sistemaren erabilera bakoitza noiz egin den (erregistro batean jasoko da erabilera bakoitza zein data eta ordutan hasi den eta zein ordutan amaitu).

b) Sistemak sarrera-datuak eratzeko erreferentziako zer datu-base erabili duen.

c) Bilaketak zer sarrera-daturekin lortu duen korrespondentzia.

d) Zein pertsona fisikok parte hartu duten emaitzen egiaztapenean (14.5 artikuluan aipatuak).

13. artikulua.– Gardentasunez jardutea eta hedapenaren arduradunei informazioa komunikatzea

1. Arrisku handiko AA-sistemak diseinatzeko eta garatzeko orduan, bermatuko da sistemek behar den gardentasun-mailaz dihardutela, hartara hedapenaren arduradunek egokiro interpreta eta erabil ditzaten sistemaren iteera-emaitzak. Gardentasun mota eta maila egokia bermatuko da hornitzaileak eta hedapenaren arduradunak 3. atalean aurreikusitako betekizunak bete ditzaten.

2. Arrisku handiko AA-sistemek erabilera-jarraibideak izango dituzte formatu digitalean edo egoki den besteren batean, eta, jarraibide horietan, hedapenaren arduradunentzako informazio zehatz, oso, zuzen eta argia jasoko da haienezako modu irisgarri eta ulergarrian.

3. Erabilera-jarraibideetan, informazio hau jasoko da gutxienez:

a) Tratamenduaren arduradunaren identitatea eta harremanetarako datuak eta, halakorik badago, haren ordezkari baimenduarenak.

b) Arrisku handiko AA-sistemaren funtzionamendu ezaugarriak, gaitasunak eta mugak, barruan direla:



i) su finalidad prevista,

ii) el nivel de precisión (incluidos los parámetros para medirla), solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse, así como cualquier circunstancia conocida y previsible que pueda afectar al nivel de precisión, solidez y ciberseguridad esperado,

iii) cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales a que se refiere el artículo 9, apartado 2,

iv) en su caso, las capacidades y características técnicas del sistema de IA de alto riesgo para proporcionar información pertinente para explicar sus resultados de salida,

v) cuando proceda, su funcionamiento con respecto a determinadas personas o determinados colectivos de personas en relación con los que esté previsto utilizar el sistema,

vi) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA de alto riesgo,

vii) en su caso, información que permita a los responsables del despliegue interpretar los resultados de salida del sistema de IA de alto riesgo y utilizarla adecuadamente;

los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso;

las medidas de supervisión humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA de alto riesgo por parte de los responsables del despliegue;

los recursos informáticos y de hardware necesarios, la vida útil prevista del sistema de IA de alto riesgo y las medidas de mantenimiento y cuidado necesarias (incluida su frecuencia) para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a las actualizaciones del software;

i) sistemaren helburu aurreikusia;

ii) 15. artikuluan aipatutako zehaztasunaren (neurketa-parametroak barne), sendotasunaren eta zibersegurtasunaren maila, arrisku handiko AA-sistema probatzeko eta balioztatze erabili dena eta espero izatekoa dena; bai, halaber, zehaztasun-, sendotasun- eta zibersegurtasun-maila horri eragin diezaiokeen edozelako gorabehera ezagun edo aurreikusgarri;

iii) arrisku handiko AA-sistemaren gaineko gorabehera ezagun edo aurreikusgarri guztiak, aintzat hartuta hala helburu aurreikusiaaren araberako erabilerak nola arrazoiz aurreikus daitezkeen erabilera desegokiak, erabilera horiek arriskua eragin diezaieketen heinean bai osasunari eta segurtasunari, bai oinarritzko eskubideei, 9.2 artikuluan aipatutakoari jarraikiz;

iv) hala badagokio, arrisku handiko AA-sistemek beren irteera-emaitzak azaltzeko informazioa emateko dituzten gaitasun eta ezaugarri teknikoak;

v) hala badagokio, sistemen jardunbidea, pertsona edo pertsona-kolektibo jakin batzuei dagokienez, sistema pertsona horiekin erabiltzekoa den heinean;

vi) hala badagokio, sarrera-datuak buruzko zehaztapenak edo erabilitako entrenamendu-, balioztatze- eta proba-datuak multzoei buruz beharrezkoa den beste edozein informazio, arrisku handiko AA-sistemaren helburu aurreikusia aintzat hartuta;

vii) hala badagokio, hedapenaren arduradunei arrisku handiko AA-sistemaren irteera-emaitzak interpretatzen eta egokiro erabiltzen laguntzen dien informazioa.

Arrisku handiko AA-sisteman eta haren jardunbidean gertatutako aldaketak, hasierako adostasunaren ebaluazioa egiterakoan hornitzaileak aurrez zehaztuak, hala badagokio.

14. artikuluan aipatutako giza ikuskapeneko neurriak, barnean direla hedapenaren arduradunek arrisku handiko AA-sistemen irteera-emaitzak interpretatu ahal izateko ezarritako neurri teknologikak.

Beharrezkoak diren baliabide informatiko eta hardware-baliabideak, arrisku handiko AA-sistemen balio-bizitza aurreikusia eta sistemak egokiro diharduela ziurtatzeko behar diren mantentze- eta zaintza-neurri guztiak (haien maiztasuna ere kontuan hartuta), softwarearen eguneratzeari dagokionez ere bai.



f) cuando proceda, una descripción de los mecanismos incluidos en el sistema de IA de alto riesgo que permita a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro de conformidad con el artículo 12.

Artículo 14.– Supervisión humana

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas.

2. El objetivo de la supervisión humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan a pesar de la aplicación de otros requisitos establecidos en la presente sección.

3. Las medidas de supervisión serán proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA de alto riesgo, y se garantizarán bien mediante uno de los siguientes tipos de medidas, bien mediante ambos:

a) las medidas que el proveedor defina y que integre, cuando sea técnicamente viable, en el sistema de IA de alto riesgo antes de su introducción en el mercado o su puesta en servicio;

las medidas que el proveedor defina antes de la introducción del sistema de IA de alto riesgo en el mercado o de su puesta en servicio y que sean adecuadas para que las ponga en práctica el responsable del despliegue.

4. A efectos de la puesta en práctica de lo dispuesto en los apartados 1, 2 y 3, el sistema de IA de alto riesgo se ofrecerá al responsable del despliegue de tal modo que las personas físicas a quienes se encomiende la supervisión humana puedan, según proceda y de manera proporcionada a:

a) entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados;

ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo

f) Egoki denean, arrisku handiko AA-sisteman barne hartutako mekanismoen deskribapena, haren bidez hedapenaren arduradunek egokiro lortu, biltegiratu eta interpretatu ahal izan ditzaten 12. artikuluaaren arabera erregistro-artxiboak.

14. artikulua.– Giza ikuskapena

1. Erabiltzen ari diren bitartean pertsona fisikoek modu eraginkorrean zaindu ahal izateko moduan diseinatu eta garatuko dira arrisku handiko AA-sistemak, eta, horretarako, gizakia-makina interfazeko tresna egokiak eman beharko zaizkie.

2. Giza ikuskapenaren helburua izango da prebenitzea edo ahalik eta gehien murriztea, arrisku handiko AA-sistema bat helburu aurrekusiaren arabera erabiltzen denean edo arrazoiz aurreikus daitekeen erabilera desegoki bat ematen zaionean, osasunerako, segurtasunerako edo oinarritzko eskubideetarako sor litezkeen arriskuak, bereziki arrisku horiek desagertzen ez badira atal honetan ezarritako beste betekizun batzuk aplikatu arren.

3. Gainbegiratze-neurriak proportzionalak izango dira arrisku handiko AA-sistemaren arriskuak, autonomia-maila eta erabilera-testuingurua kontuan hartuta, eta jarraian azaldu diren neurri mota hauetako bat edo biak ezarritik bermatuko dira. Hona hemen:

a) arrisku handiko AA-sistema merkatuan jarri edo zerbitzuan ipini aurretik, eta teknikoki bideragarria denean, hornitzaileak zehazten eta integratzen dituen neurriak;

arrisku handiko AA-sistema merkatuan jarri edo zerbitzuan ipini aurretik hornitzaileak zehazten dituen neurriak, egokiak badira hedapenaren arduradunak praktikan jartzeko.

4. Artikulu honetako 1., 2. eta 3. apartatuetan xedatutakoa praktikan jartzeko, arrisku handiko AA-sistema modu jakinean eskainiko zaio hedapenaren arduradunari, giza ikuskapenaren ardura duten pertsona fisikoek, dagokionaren arabera eta modu proportzionatuan, hauek egin ahal izan ditzaten:

a) behar bezala ulertu arrisku handiko AA-sistemaren gaitasunak eta mugak, eta behar bezala zaindu haren funtzionamendua, anomaliak adibidez, funtzionamendu-arazoak eta ustekabeko portaerak detektatzeko eta konpontzeko;

jakitun izan joera egon litekeela automatikoki edo gehiegi fidatzeko arrisku handiko AA-sistema batek sortutako irteera-emaitezkin («automatizazio-



(«sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión;

interpretar correctamente los resultados de salida del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles;

decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que este genere;

intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura.

5. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 1, letra a), las medidas a que se refiere el apartado 3 del presente artículo garantizarán, además, que el responsable del despliegue no actúe ni tome ninguna decisión basándose en la identificación generada por el sistema, salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación.

El requisito de la verificación por parte de al menos dos personas físicas por separado no se aplicará a los sistemas de IA de alto riesgo utilizados con fines de garantía del cumplimiento del Derecho, de migración, de control fronterizo o de asilo cuando el Derecho nacional o de la Unión considere que la aplicación de este requisito es desproporcionada.

Artículo 15.– Precisión, solidez y ciberseguridad

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida.

2. Para abordar los aspectos técnicos sobre la forma de medir los niveles adecuados de precisión y solidez establecidos en el apartado 1 y cualquier otro parámetro de rendimiento pertinente, la Comisión, en cooperación con las partes interesadas y organizaciones pertinentes, como las autoridades de metrología y de evaluación comparativa, fomentará, según proceda, el desarrollo de parámetros de referencia y metodologías de medición.

alborapena»), bereziki pertsona fisikoek erabakiren bat hartzeko helburua duten informazioa edo gomendioak emateko erabiltzen diren sistemekin;

behar bezala interpretatu arrisku handiko AA-sistemaren irteera-emaizak, kontuan izanda, esaterako, eskura dauden interpretazio-metodo eta -tresnak;

erabaki, edozein egoera zehatzetan, ez dela erabiliko arrisku handiko AA-sistema, edo sistema horrek sortzen dituen irteera-emaizak baztertu, baliogabetu edo lehengoratu direla;

arrisku handiko AA-sistemaren funtzionamenduan esku hartu, edo sistema eten, bai gelditzeko botoia sakatuz, bai sistema modu seguruan geldiarazteko antzeko prozedura baten bidez.

5. Erregelamendu honen III. eranskineko 1. puntuko a) letran aipatzen diren arrisku handiko AA-sistemen kasuan, artikuluko honen 3. apartatuan aipatzen diren neurriek berrmatuko dute, gainera, hedapenaren arduradunak ez duela jardungo eta ez duela inolako erabakirik hartuko sistemak sortutako identifikazioan oinarrituta, salbu eta behar diren konpetentzia, prestakuntza eta aginpidea dituzten gutxienez bi pertsona fisikok nor bere aldetik egiaztatu eta berretsi badute identifikazio hori.

Gutxienez bi pertsona fisikok nor bere aldetik egiaztatze betekizuna ez zaie aplikatuko zuzenbidea betearazteko, migrazioko, muga-kontrolako edo asiloko helburuekin erabilitako arrisku handiko AA-sistemei, baldin eta zuzenbide nazionalak edo Batasuneko zuzenbideak irizten badio neurritz kanpokoa dela betekizun hori aplikatzeko beharra.

15. artikulua.– Zehaztasuna, sendotasuna eta zibersegurtasuna

1. Zehaztasun-, sendotasun- eta zibersegurtasun-maila egokiak lortzeko eta beren bizi-ziklo osoan ezaugarri horiek modu uniforme mantentzeko moduan diseinatu eta garatuko dira arrisku handiko AA-sistemak.

2. Artikulu honetako 1. apartatuan ezarritako zehaztasun- eta sendotasun-maila aproposak eta beste edozein errendimendu-parametro egoki neurtzeko moduari buruzko alderdi teknikoak jorratzeko, dagokionaren arabera, erreferentzia-parametroak eta neurketa-metodologiak garatzea sustatuko du Batzordeak, alderdi interesdunekin eta dagozkion antolakundeekin lankidetzan —hala nola metrologiako eta konparaziozko ebaluazioko agintaritzekin—.



3. En las instrucciones de uso que acompañen a los sistemas de IA de alto riesgo se indicarán los niveles de precisión de dichos sistemas, así como los parámetros pertinentes para medirla.

4. Los sistemas de IA de alto riesgo serán lo más resistentes posible en lo que respecta a los errores, fallos o incoherencias que pueden surgir en los propios sistemas o en el entorno en el que funcionan, en particular a causa de su interacción con personas físicas u otros sistemas. Se adoptarán medidas técnicas y organizativas a este respecto.

La solidez de los sistemas de IA de alto riesgo puede lograrse mediante soluciones de redundancia técnica, tales como copias de seguridad o planes de prevención contra fallos.

Los sistemas de IA de alto riesgo que continúan aprendiendo tras su introducción en el mercado o puesta en servicio se desarrollarán de tal modo que se elimine o reduzca lo máximo posible el riesgo de que los resultados de salida que pueden estar sesgados influyan en la información de entrada de futuras operaciones (bucles de retroalimentación) y se garantice que dichos bucles se subsanen debidamente con las medidas de reducción de riesgos adecuadas.

5. Los sistemas de IA de alto riesgo serán resistentes a los intentos de terceros no autorizados de alterar su uso, sus resultados de salida o su funcionamiento aprovechando las vulnerabilidades del sistema.

Las soluciones técnicas encaminadas a garantizar la ciberseguridad de los sistemas de IA de alto riesgo serán adecuadas a las circunstancias y los riesgos pertinentes.

Entre las soluciones técnicas destinadas a subsanar vulnerabilidades específicas de la IA figurarán, según corresponda, medidas para prevenir, detectar, combatir, resolver y controlar los ataques que traten de manipular el conjunto de datos de entrenamiento («envenenamiento de datos»), o los componentes entrenados previamente utilizados en el entrenamiento («envenenamiento de modelos»), la información de entrada diseñada para hacer que el modelo de IA cometa un error («ejemplos adversarios» o «evasión de modelos»), los ataques a la confidencialidad o los defectos en el modelo.

SECCIÓN 3

Obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y de otras partes

3. Arrisku handiko AA-sistemekin batera ematen diren erabilera-jarraibideetan, sistema horien zehaztasun-mailak adieraziko dira, bai eta horiek neurtzeko erabil daitezkeen parametroak ere.

4. Arrisku handiko AA-sistemek ahalik eta ondoen egin beharko diete aurre sistemetan edo funtzionatzen duten ingurunean sor daitezkeen errore, hutsegite edo inkoherentziei, bereziki pertsona fisikoekin edo beste sistema batzuekin elkarreragitearen ondorioz sortzen badira. Horretarako, neurri teknikoak eta antolakuntzakoak hartuko dira.

Arrisku handiko AA-sistemak sendoak izatea lortzeko, erredundantzia teknikoko soluzioak erabil daitezke, hala nola segurtasun-kopiak edo hutsegiteen aurkako prebentzio-planak.

Merkatuan jarri edo zerbitzuan ipini ostean ikasten jarraitzen duten arrisku handiko AA-sistemak garatzean, helburua izango da ezabatzea edo ahalik eta gehien murriztea alboratuta egon daitezkeen irteera-emaitez etorkizuneko eragiketen sarrera-informazioan eragina izateko arriskua (atzeraelikatze-begiztak), eta bermatu egingo da begizta horiek behar bezala zuzentzen direla arriskuak murrizteko neurri egokien bitartez.

5. Arrisku handiko AA-sistemek aurre egingo diete baimendu gabeko hirugarrenek, sistemaren kalteberatasuna aprobetxatuz, sistemaren erabilera, irteera-emaitez edo funtzionamendua aldatzeko egiten dituzten saiakerei.

Arrisku handiko AA-sistemen zibersegurtasuna bermatzera bideratutako soluzio teknikoak egokiak izango dira sor litezkeen inguruabar eta arriskueterako.

AAren berariazko kalteberatasunak konpontzera bideratutako soluzio teknikoaren artean, dagokionaren arabera, halakoak prebenitu, detektatu, eragotzi, konpondu eta kontrolatzeko neurriak daude: entrenamendu-datuaren multzoa manipulatzeko saiatzen diren erasoak («datuak pozoitzea»), entrenamenduan alde aurretik erabilitako osagai entrenatuak manipulatzeko saiatzen direnak («ereduak pozoitzea»), AA-ereduak errore bat egiteko diseinatzen den sarrera-informazioa («adibide aurkariak» edo «ereduen ihesa»), konfidentzialtasunaren aurkako erasoak edo ereduaren akatsak.

3. ATALA

Arrisku handiko AA-sistemen hornitzaileen, hedapenaren arduradunen eta beste alderdi batzuen betebeharrak



Artículo 16.— Obligaciones de los proveedores de sistemas de IA de alto riesgo

Los proveedores de sistemas de IA de alto riesgo:

a) velarán por que sus sistemas de IA de alto riesgo cumplan los requisitos definidos en la sección 2;

indicarán en el sistema de IA de alto riesgo o, cuando no sea posible, en el embalaje del sistema o en la documentación que lo acompañe, según proceda, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto;

contarán con un sistema de gestión de la calidad que cumpla lo dispuesto en el artículo 17;

conservarán la documentación a que se refiere el artículo 18;

cuando estén bajo su control, conservarán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 19;

f) se asegurarán de que los sistemas de IA de alto riesgo sean sometidos al procedimiento pertinente de evaluación de la conformidad a que se refiere el artículo 43 antes de su introducción en el mercado o puesta en servicio;

g) elaborarán una declaración UE de conformidad en virtud de lo dispuesto en el artículo 47;

h) colocará el marcado CE en el sistema de IA de alto riesgo o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, para indicar la conformidad con el presente Reglamento, de acuerdo con lo dispuesto en el artículo 48;

cumplirán las obligaciones de registro a que se refiere el artículo 49, apartado 1;

j) adoptarán las medidas correctoras necesarias y facilitarán la información exigida en el artículo 20;

k) demostrarán, previa solicitud motivada de la autoridad nacional competente, la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2;

l) velarán por que el sistema de IA de alto riesgo cumpla requisitos de accesibilidad de conformidad con las Directivas (UE) 2016/2102 y (UE) 2019/882.

Artículo 17.— Sistema de gestión de la calidad

16. artikulua.— Arrisku handiko AA-sistemen hornitzaileen betebeharrak

Arrisku handiko AA-sistemen hornitzaileek lan hauek egingo dituzte:

a) Zaindu egingo dute arrisku handiko AA-sistemek bete egiten dituztela 2. atalean ezarritako betekizunak.

Beren izena, izen komertzial erregistratua edo marka erregistratua eta harremanetarako helbidea adieraziko dituzte arrisku handiko AA-sisteman edo, hor ezin denean, sistemaren enbalajea edo harekin batera doan dokumentazioan, dagokionaren arabera.

Kalitatea kudeatzeko sistema bat izango dute —17. artikuluan ezarritakoa beteko du—.

Gorde egingo dute 18. artikuluan aipatzen den dokumentazioa.

Beren kontrolpean daudenean, gorde egingo dituzte arrisku handiko beren AA-sistemek automatikoki sortutako erregistro-artxiboak —19. artikuluan aipatzen dira—.

f) Ziurtatu egingo dute arrisku handiko AA-sistemei adostasuna ebaluatzeko prozedura egokia aplikatzen zaiela —43. artikuluan aipatzen da— merkatuan jarri edo zerbitzuan ipini aurretik.

g) EB adostasun-adierazpena egingo dute, 47. artikuluan xedatutakoari jarraikiz.

h) CE marka jarriko dute arrisku handiko AA-sisteman edo, hor ezin denean, sistemaren enbalajea edo harekin batera doan dokumentazioan, erregelamendu honekin bat datorrela adierazteko, 48. artikuluan xedatutakoaren arabera.

Bete egingo dituzte 49.1 artikuluan aipatzen diren erregistro-betebeharrak.

j) Behar diren neurri zuzentzaileak hartuko dituzte eta 20. artikuluan eskatutako informazioa emango dute.

k) Frogatu egingo dute, agintaritza nazional eskudunak arrazoituta eskatuz gero, arrisku handiko AA-sistema bat datorrela 2. atalean ezarritako betekizunekin.

l) Zaindu egingo dute arrisku handiko AA-sistemak irisgarritasun-betekizunak betetzen dituela (EB) 2016/2102 eta (EB) 2019/882 zuzentarauen arabera.

17. artikulua.— Kalitatea kudeatzeko sistema



1. Los proveedores de sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema deberá consignarse de manera sistemática y ordenada en documentación en la que se recojan las políticas, los procedimientos y las instrucciones e incluirá, al menos, los siguientes aspectos:

a) una estrategia para el cumplimiento de la normativa, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y de los procedimientos de gestión de las modificaciones de los sistemas de IA de alto riesgo;

las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño del sistema de IA de alto riesgo;

las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el desarrollo del sistema de IA de alto riesgo y en el control y el aseguramiento de la calidad de este;

los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que se ejecutarán;

las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad o no cubran todos los requisitos pertinentes establecidos en la sección 2, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla dichos requisitos;

f) los sistemas y procedimientos de gestión de datos, lo que incluye su adquisición, recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con esa finalidad;

g) el sistema de gestión de riesgos que se menciona en el artículo 9;

h) el establecimiento, aplicación y mantenimiento de un sistema de vigilancia poscomercialización de conformidad con el artículo 72;

i) los procedimientos asociados a la notificación de un incidente grave con arreglo al artículo 73;

1. Arrisku handiko AA-sistemen hornitzaileek kalitatea kudeatzeko sistema bat ezarriko dute erregelamendu hau betetzen dela bermatzeko. Sistema hori modu sistematiko eta ordenatuan jaso beharko da politikak, prozedurak eta jarraibideak jasotzen dituen dokumentazioan. Alderdi hauek izango ditu gutxienez:

a) Araudia betetzeko estrategia, barne hartuta adostasuna ebaluatzeko prozedurak eta arrisku handiko AA-sistemen aldaketak kudeatzeko prozedurak betetzea.

Arrisku handiko AA-sistemaren diseinuan eta diseinuaren kontrol eta egiaztapenean erabiliko diren teknika, prozedura eta jarduketa sistematikoak.

Arrisku handiko AA-sistema garatzeko eta haren kalitatea kontrolatu eta ziurtatzeko erabiliko diren teknika, prozedura eta jarduketa sistematikoak.

Arrisku handiko AA-sistema garatu aurretik, bitartean eta ondoren egingo diren azterketa-, proba- eta balioztatze-prozedurak, eta horiek gauzatzeko maiztasuna.

Aplikatuko diren zehaztapen teknikoak, arauak barne, eta, dagozkion arau harmonizatuak osorik aplikatzen ez direnean edo 2. atalean ezarritako betekizun guztiak betetzen ez dituztenean, arrisku handiko AA-sistemak betekizun horiek betetzen dituela zaintzeko erabiliko diren bitartekoak.

f) Datuak kudeatzeko sistema eta prozedurak, hau da, datuak eskuratu, bildu, aztertu, etiketatu, biltegiratu, iragazi, prospekzioa eta agregazioa egin eta gordetzeko sistema eta prozedurak, eta datuekin lotutako beste edozein eragiketa, baldin eta arrisku handiko AA-sistemak merkatuan jarri edo zerbitzuan ipini aurretik egiten bada helburu horrekin.

g) Arriskuak kudeatzeko sistema —9. artikuluan aipatzen da—.

h) Merkaturatu osteko zaintza-sistema bat ezarri, aplikatu eta mantentzea, 72. artikuluaaren arabera.

i) Gorabehera larri baten jakinarazpenari lotutako prozedurak, 73. artikuluaaren arabera.



j) la gestión de la comunicación con las autoridades nacionales competentes, otras autoridades pertinentes, incluidas las que permiten acceder a datos o facilitan el acceso a ellos, los organismos notificados, otros operadores, los clientes u otras partes interesadas;

k) los sistemas y procedimientos para llevar un registro de toda la documentación e información pertinente;

l) la gestión de los recursos, incluidas medidas relacionadas con la seguridad del suministro;

m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado.

2. La aplicación de los aspectos mencionados en el apartado 1 será proporcional al tamaño de la organización del proveedor. Los proveedores respetarán, en todo caso, el grado de rigor y el nivel de protección requerido para garantizar la conformidad de sus sistemas de IA de alto riesgo con el presente Reglamento.

3. Los proveedores de sistemas de IA de alto riesgo que estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad o una función equivalente con arreglo al Derecho sectorial pertinente de la Unión podrán incluir los aspectos enumerados en el apartado 1 como parte de los sistemas de gestión de la calidad con arreglo a dicho Derecho.

4. En el caso de los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de establecer un sistema de gestión de la calidad, salvo en relación con lo dispuesto en el apartado 1, letras g), h) e i), del presente artículo cuando se respeten las normas sobre los sistemas o procesos de gobernanza interna de acuerdo con el Derecho pertinente de la Unión en materia de servicios financieros. A tal fin, se tendrán en cuenta todas las normas armonizadas que se mencionan en el artículo 40.

Artículo 18.— Conservación de la documentación

1. Durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, el proveedor mantendrá a disposición de las autoridades nacionales competentes:

j) Agintaritza nazional eskudunekin, beste agintaritza egoki batzuekin —datuetarako sarbidea ematen edo errazten dutenak barne—, organismo jakinaraziekin, beste operadore batzuekin, bezeroekin edo beste alderdi interesdun batzuekin izango den komunikazioaren kudeaketa.

k) Beharrezko diren dokumentazioa eta informazioa erregistratzeko sistema eta prozedurak.

l) Baliabideen kudeaketa, horniduraren segurtasunarekin zerikusia duten neurriak barne.

m) Kontuak emateko esparru bat, zuzendaritzako langileen erantzukizunak eta bestelakoak definituko dituen, apartatu honetan zerrendatutako alderdi guztiei dagokienez.

2. Artikulu honen 1. apartatuan aipatutako alderdien aplikazioa hornitzailearen antolakundearen tamainaren arabera izango da. Hornitzaileek, nolana ere, arrisku handiko AA-sistemak erregelamendu honekin bat datozela bermatzeko eskatutako zorrotasun- eta babes-mailak errespetatuko dituzte.

3. Kalitatea kudeatzeko sistemei buruzko betebeharrak dituzten arrisku handiko AA-sistemen hornitzaileek edo Batasuneko zuzenbide sektorialaren arabera baliokidea den eginkizun bat bete behar dutenek 1. apartatuan zerrendatutako alderdiak sartu ahal izango dituzte kalitatea kudeatzeko sistemen zati gisa, zuzenbide horren arabera.

4. Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera ezarritako barne-gobernantza, -sistema edo -prozesuei buruzko betekizunak bete behar dituzten finantza-entitateak direnean hornitzaileak, ulertuko da kalitatea kudeatzeko sistema bat ezartzeko betebeharra bete dela, artikulu honen 1. apartatuko g), h) eta i) letretan xedatutakoari dagokionez izan ezik, barne-gobernantzako sistemei edo prozesuei buruzko arauak errespetatzen direnean, finantza-zerbitzuen arloan Batasunean dagokion zuzenbidearekin bat etorritik. Horretarako, 40. artikuluan aipatzen diren arau harmonizatu guztiak hartuko dira kontuan.

18. artikulua.— Dokumentazioa gordetzea

1. Arrisku handiko AA-sistema merkatuan jarri edo zerbitzuan ipini eta hamar urteko epean, hornitzaileak dokumentu hauek edukiko ditu agintaritza nazional eskudunen eskura:



a) la documentación técnica a que se refiere el artículo 11;

la documentación relativa al sistema de gestión de la calidad a que se refiere el artículo 17;

la documentación relativa a los cambios aprobados por los organismos notificados, si procede;

las decisiones y otros documentos expedidos por los organismos notificados, si procede;

la declaración UE de conformidad contemplada en el artículo 47.

2. Cada Estado miembro determinará las condiciones en las que la documentación a que se refiere el apartado 1 permanecerá a disposición de las autoridades nacionales competentes durante el período indicado en dicho apartado en los casos en que un proveedor o su representante autorizado establecido en su territorio quiebre o cese en su actividad antes del final de dicho período.

3. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán la documentación técnica como parte de la documentación conservada en virtud del Derecho pertinente de la Unión en materia de servicios financieros.

Artículo 19.— Archivos de registro generados automáticamente

1. Los proveedores de sistemas de IA de alto riesgo conservarán los archivos de registro a que se refiere el artículo 12, apartado 1, que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control. Sin perjuicio del Derecho aplicable de la Unión o nacional, los archivos de registro se conservarán durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que el Derecho de la Unión o nacional aplicable, en particular el Derecho de la Unión en materia de protección de datos personales, disponga otra cosa.

2. Los proveedores que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo como parte de la documentación conservada en virtud

a) dokumentazio teknikoa —11. artikuluan aipatzen da—;

kalitatea kudeatzeko sistemaren dokumentazioa —17. artikuluan dago zehaztuta—;

organismo jakinaraziek onartutako aldaketei buruzko dokumentazioa, hala badagokio;

organismo jakinaraziek emandako erabakiak eta bestelako dokumentuak, hala badagokio;

EB adostasun-adierazpena —47. artikuluan dago zehaztuta—.

2. Estatu kide bakoitzak zehaztuko du zer baldintzatan egongo den 1. apartatuan aipatzen den dokumentazioa agintaritza nazional eskudunen eskura, apartatu horretan adierazitako aldian, baldin eta bere lurraldean ezarritako hornitzaile batek edo haren ordezkari baimenduak porrot egin edo jarduera eteten badu aldi hori amaitu baino lehen.

3. Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera ezarritako barne-gobernantza, -sistema edo -prozesuei buruzko betekizunak bete behar dituzten finantza-entitateak direnean hornitzaileak, gordetako dokumentazioaren zati gisa mantenduko dute dokumentazio teknikoa, finantza-zerbitzuen arloan Batasunean dagokion zuzenbidearekin bat etorritz.

19. artikulua.— Automatikoki sortutako erregistro-artxiboak

1. Arrisku handiko AA-sistemen hornitzaileek gorde egingo dituzte arrisku handiko AA-sistemek automatikoki sortutako erregistro-artxiboak —12.1 artikuluan daude aipatuta—, artxibo horiek beren kontrolpean dauden neurrian. Aplikatzekoa den Batasuneko zuzenbidea edo zuzenbide nazionala alde batera utzi gabe, erregistro-artxiboak arrisku handiko AA-sistemaren helburu aurreikusirako egokia den denbora-tartean gordeko dira, gutxienez sei hilabetez, salbu eta besterik xedatzen badu aplikatzekoa den Batasuneko zuzenbideak edo zuzenbide nazionalak, bereziki datu pertsonalen babesaren arloko Batasuneko zuzenbideak.

2. Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera ezarritako barne-gobernantza, -sistema edo -prozesuei buruzko betekizunak bete behar dituzten finantza-entitateak direnean hornitzaileak, gordetako dokumentazioaren zati gisa mantenduko dituzte arrisku handiko beren AA-sistemek automatikoki sortzen dituzten erregistro-artxiboak, finantza-zerbitzuen arloan dagokion zuzenbidearekin bat etorritz.



del Derecho pertinente en materia de servicios financieros.

Artículo 20.— Medidas correctoras y obligación de información

1. Los proveedores de sistemas de IA de alto riesgo que consideren o tengan motivos para considerar que un sistema de IA de alto riesgo que han introducido en el mercado o puesto en servicio no es conforme con el presente Reglamento adoptarán inmediatamente las medidas correctoras necesarias para que sea conforme, para retirarlo del mercado, desactivarlo o recuperarlo, según proceda. Informarán de ello a los distribuidores del sistema de IA de alto riesgo de que se trate y, en su caso, a los responsables del despliegue, al representante autorizado y a los importadores.

2. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, y el proveedor tenga conocimiento de dicho riesgo, este investigará inmediatamente las causas, en colaboración con el responsable del despliegue que lo haya notificado, en su caso, e informará a las autoridades de vigilancia del mercado competentes respecto al sistema de IA de alto riesgo de que se trate y, cuando proceda, al organismo notificado que haya expedido un certificado para dicho sistema de conformidad con lo dispuesto en el artículo 44, en particular sobre la naturaleza del incumplimiento y sobre cualquier medida correctora adoptada.

Artículo 21.— Cooperación con las autoridades competentes

1. Los proveedores de sistemas de IA de alto riesgo, previa solicitud motivada de una autoridad competente, proporcionarán a dicha autoridad toda la información y la documentación necesarias para demostrar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, en una lengua que la autoridad pueda entender fácilmente y que sea una de las lenguas oficiales de las instituciones de la Unión, indicada por el Estado miembro de que se trate.

2. Previa solicitud motivada de una autoridad competente, los proveedores darán también a dicha autoridad, cuando proceda, acceso a los archivos de registro generados automáticamente del sistema de IA de alto riesgo a que se refiere el artículo 12, apartado 1, en la medida en que dichos archivos estén bajo su control.

3. Toda información obtenida por una autoridad competente con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

20. artikulua.— Neurri zuzentzaileak eta informatzeko betebeharra

1. Arrisku handiko AA-sistemen hornitzaileek, merkatuan jarri edo zerbitzuan ipini duten arrisku handiko AA-sistema bat erregelamendu honekin ados ez datorrela uste badute edo hori pentsatzeko arrazoiak badituzte, behar diren neurri zuzentzaileak hartuko dituzte, berehala, sistema hori merkatutik erretiratzeko, desaktibatzeko edo berreskuratzeko, dagokionaren arabera. Horren berri emango diete arrisku handiko AA-sistemaren banatzaileei eta, hala badagokio, hedapenaren arduradunei, ordezkari baimenduari eta inportatzaileei.

2. Arrisku handiko AA-sistema batek arriskuren bat dakarrenean 79.1 artikulua zentzuan eta hornitzaileak arrisku horren berri duenean, berehala ikertuko ditu kausak, arriskua jakinarazi duen hedapenaren arduradunarekin lankidetzan, hala badagokio, eta merkatua zaintzeko agintaritza eskudunei jakinaraziko die, kasuan kasuko arrisku handiko AA-sistemari dagokionez, eta, hala dagokionean, sistema horretarako ziurtagiri bat eman duen organismo jakinaraziari —44. artikuluan xedatutakoaren arabera —, bereziki ez-betetzearen izaerari eta hartutako edozein neurri zuzentzailei dagokienez.

21. artikulua.— Lankidetzak agintaritzak eskudunekin

1. Arrisku handiko AA-sistemen hornitzaileek, agintaritzak eskudun batek arrazoituta eskatuz gero, behar den informazio eta dokumentazio guztia emango diote agintaritzak horri arrisku handiko AA-sistemak 2. atalean ezarritako betekizunak betetzen dituela frogatzeko, agintaritzak erraz ulertzeko moduko hizkuntza batean, Batasuneko instituzioetako hizkuntza ofiziala izango dena, dagokion estatu kideak adierazia.

2. Agintaritzak eskudun batek arrazoituta eskatuz gero, hornitzaileek sarbidea emango diote agintaritzak horri arrisku handiko AA-sistemak automatikoki sortutako erregistro-artxiboak eskuratzeko —12.1 artikuluan daude aipatuta—, artxibo horiek beren kontrolpean dauden neurrian.

3. Agintaritzak eskudun batek artikulua honen arabera lortutako informazio guztia 78. artikuluan ezarritako konfidentzialtasun-betebeharren arabera tratatuko da.



Artículo 22.— Representantes autorizados de los proveedores de sistemas de IA de alto riesgo

1. Antes de comercializar sus sistemas de IA de alto riesgo en el mercado de la Unión, los proveedores establecidos en terceros países tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.
2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.
3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a las autoridades de vigilancia del mercado, cuando lo soliciten, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión según lo indicado por la autoridad de competente. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:

a) verificar que se han elaborado la declaración UE de conformidad a que se refiere el artículo 47 y la documentación técnica a que se refiere el artículo 11 y que el proveedor ha llevado a cabo un procedimiento de evaluación de la conformidad adecuado;

conservar a disposición de las autoridades competentes y de las autoridades u organismos nacionales a que se refiere el artículo 74, apartado 10, durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, los datos de contacto del proveedor que haya nombrado al representante autorizado, una copia de la declaración UE de conformidad a que se refiere el artículo 47, la documentación técnica y, en su caso, el certificado expedido por el organismo notificado;

proporcionar a una autoridad competente, previa solicitud motivada, toda la información y la documentación, incluida la mencionada en el presente párrafo, letra b), que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2, incluido el acceso a los archivos de registro a que se refiere el artículo 12, apartado 1, generados automáticamente por ese sistema, en la medida en que dichos archivos estén bajo el control del proveedor;

cooperar con las autoridades competentes, previa solicitud motivada, en todas las acciones que estas emprendan en relación con el sistema de IA de alto riesgo, en particular para reducir y mitigar los riesgos que este presente;

22. artikulua.— Arrisku handiko AA-sistemen hornitzaileen ordezkari baimenduak

1. Hirugarren herrialdeetan kokatutako hornitzaileek, arrisku handiko haien AA-sistemak Batasuneko merkatuan merkaturatu aurretik, Batasunean kokatuta dagoen ordezkari baimendu bat izendatu beharko dute idatzizko mandatu baten bidez.
2. Hornitzailearengandik jasotako mandatuan zehaztutako lanak egiteko aukera emango diete hornitzaileek ordezkari baimenduei.
3. Hornitzailearengandik jasotako mandatuan zehaztutako lanak egingo dituzte ordezkari baimenduek. Merkatua zaintzeko agintaritzek hala eskatuz gero, mandatuaren kopia bat emango diete, Batasuneko instituzioetako hizkuntza ofizialetako batean, agintaritza eskudunak adierazitakoaren arabera. Erregelamendu honen ondorioetarako, lan hauek egiteko baimena emango dio mandatuak ordezkari baimenduari:

a) Egiaztatzea ea egin diren EB adostasun-adierazpena —47. artikuluan aipatzen da— eta dokumentazio teknikoa —11. artikuluan aipatzen da—, eta egiaztatzea hornitzaileak adostasuna ebaluatzeko prozedura egokia gauzatu duela.

Erregelamendu honen 74.10 artikuluan aipatzen diren agintaritza eskudunen eta agintaritza edo organismo nazionalen eskura gordetzea, arrisku handiko AA-sistema merkatuan jarri edo zerbitzuan ipini eta hamar urteko epean, ordezkari baimendua izendatu duen hornitzailearekin harremanetan jartzeko datuak, EB adostasun-adierazpenaren kopia bat —47. artikuluan dago zehaztuta—, dokumentazio teknikoa eta, hala badagokio, organismo jakinaraziak emandako ziurtagiria.

Agintaritza eskudun bati ematea, arrazoituta eskatuz gero, arrisku handiko AA-sistemak 2. atalean ezarritako betekizunak betetzen dituela frogatzeko behar den informazio eta dokumentazio guztia, paragrafo honen b) letran aipatutakoa barne, baita sistema horrek automatikoki sortutako erregistro-artxiboetarako sarbidea ere —12.1 artikuluan daude aipatuta—, artxibo horiek hornitzailearen kontrolpean dauden neurrian.

Agintaritza eskudunekin lankidetzan aritzea, arrazoituta eskatuz gero, agintaritza horiek arrisku handiko AA-sistemarekin lotuta abiarazten dituzten ekintza guztietan, bereziki sistema horrek dakartzan arriskuak murrizteko eta arintzeko badira.



cuando proceda, cumplir las obligaciones de registro a que se refiere el artículo 49, apartado 1, o si el registro lo lleva a cabo el propio proveedor, garantizar que la información a que se refiere el anexo VIII, sección A, punto 3, es correcta.

El mandato habilitará al representante autorizado para que las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.

4. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene las obligaciones que le atañen con arreglo al presente Reglamento. En tal caso, además, informará de inmediato de la terminación del mandato y de los motivos de esta medida a la autoridad de vigilancia del mercado pertinente, así como, cuando proceda, al organismo notificado pertinente.

Artículo 23.— Obligaciones de los importadores

1. Antes de introducir un sistema de IA de alto riesgo en el mercado, los importadores se asegurarán de que el sistema sea conforme con el presente Reglamento verificando que:

a) el proveedor del sistema de IA de alto riesgo haya llevado a cabo el procedimiento de evaluación de la conformidad pertinente a que se refiere el artículo 43;

el proveedor haya elaborado la documentación técnica de conformidad con el artículo 11 y el anexo IV;

el sistema lleve el marcado CE exigido y vaya acompañado de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso;

el proveedor haya designado a un representante autorizado de conformidad con el artículo 22, apartado 1.

2. Si el importador tiene motivos suficientes para considerar que un sistema de IA de alto riesgo no es conforme con el presente Reglamento, ha sido falsificado o va acompañado de documentación falsificada, no lo introducirá en el mercado hasta que se haya conseguido la conformidad de dicho sistema. Si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 79, apartado 1, el importador informará de ello al proveedor del sistema, a los representantes autorizados y a las autoridades de vigilancia del mercado.

Hala dagokionean, 49.1 artikuluan aipatzen diren erregistro-betebeharrak betetzea, edo, erregistroa hornitzaileak berak egiten badu, VIII. eranskinetako A ataleko 3. puntuan aipatzen den informazioa zuzena dela bermatzea.

Mandatuak ordezkari baimendua gaituko du agintaritza eskudunak harekin jar daitezen harremanetan — hornitzailearekin jarri beharrean harremanetan edo hornitzailearekin jartzeaz gain— erregelamendu hau betetzearekin zerikusia duten gai guztiei dagokienez.

4. Ordezkarri baimenduak mandatua amaituko du baldin eta uste badu hornitzaileak urratu egiten dituela erregelamendu honen arabera dituen betebeharrak, edo hori pentsatzeko arrazoiak baditu. Kasu horretan, gainera, berehala jakinaraziko dio merkatua zaintzeko agintaritzari mandatua amaitu duela, eta horretarako arrazoiak berri ere emango dio; halaber, hala dagokionean, organismo jakinarazari ere emango dio horren guztiaren berri.

23. artikulua.— Inportatzaileen betebeharrak

1. Arrisku handiko AA-sistema bat merkatuan jarri aurretik, sistema erregelamendu honekin ados datorrela ziurtatuko dute inportatzaileek, eta alderdi hauek egiaztatuko dituzte horretarako:

a) ea arrisku handiko AA-sistemaren hornitzaileak adostasuna ebaluatzeko prozedura gauzatu duen —43. artikuluan dago aipatuta—;

ea hornitzaileak dokumentazio teknikoak prestatu duen —11. artikuluan eta IV. eranskinean dago aipatuta—;

ea sistemak CE marka duen, eta ea EB adostasun-adierazpena —47. artikuluan aipatutakoa— eta erabilera-jarraibideak ere badituen;

ea hornitzaileak ordezkari baimendu bat izendatu duen —22.1 artikuluan arabera—.

2. Inportatzaileak nahikoa arrazoi duenean pentsatzeko arrisku handiko AA-sistemaren bat ez datorrela ados erregelamendu honekin, faltsifikatu egin dela edo dokumentazio faltsutua duela, ez du merkatuan jarriko, harik eta sistema horren gaineko adostasuna lortu arte. Arrisku handiko AA-sistemak arriskuren bat dakarrenean 79.1 artikuluan zentzuan, inportatzaileak horren berri emango die sistemaren hornitzaileari, ordezkari baimenduei eta merkatua zaintzeko agintaritzari.



3. Los importadores indicarán, en el embalaje del sistema de IA de alto riesgo o en la documentación que lo acompañe, cuando proceda, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto.

4. Mientras sean responsables de un sistema de IA de alto riesgo, los importadores se asegurarán de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometan el cumplimiento de los requisitos establecidos en la sección 2 por parte de dicho sistema.

5. Los importadores conservarán, durante un período de diez años a contar desde la introducción en el mercado o la puesta en servicio del sistema de IA de alto riesgo, una copia del certificado expedido por el organismo notificado, en su caso, de las instrucciones de uso y de la declaración UE de conformidad a que se refiere el artículo 47.

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

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

Artículo 24.– Obligaciones de los distribuidores

1. Antes de comercializar un sistema de IA de alto riesgo, los distribuidores verificarán que este lleve el marcado CE exigido, que vaya acompañado de una copia de la declaración UE de conformidad a que se refiere el artículo 47 y de las instrucciones de uso, y que el proveedor y el importador de dicho sistema, según corresponda, hayan cumplido sus obligaciones establecidas en el artículo 16, letras b) y c), y el artículo 23, apartado 3, respectivamente.

2. Si un distribuidor considera o tiene motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo no es conforme con los requisitos establecidos en la sección 2, no lo comercializará hasta que se haya conseguido esa conformidad. Además, si el sistema de IA de alto riesgo presenta un riesgo en el sentido del artículo 79,

3. Inportatzaileek beren izena, izen komertzial erregistratua edo marka erregistratua eta harremanetarako helbidea adieraziko dituzte arrisku handiko AA-sistemaren enbalajea edo harekin batera doan dokumentazioan, hala dagokionean.

4. Arrisku handiko AA-sistema baten arduradunak diren bitartean, inportatzaileek ziurtatuko dute biltegiatze- edo garraio-baldintzek, hala dagokionean, ez dutela arriskuan jartzen sistema horrek 2. atalean ezarritako betekizunak betetzea.

5. Arrisku handiko AA-sistema merkatuan jarri edo zerbitzuan ipini eta hamar urtez gordeko dute inportatzaileek organismo jakinaraziak emandako ziurtagiriaren kopia bat eta, hala badagokio, EB adostasun-adierazpenaren —47. artikuluan dago zehaztuta— eta erabilera-jarraibideen kopia bana.

6. Inportatzaileek beharrezko den informazio eta dokumentazio guztia —5. apartatuan aipatutakoak barne— emango diete agintaritza eskudunei, arrazoituta eskatuz gero, arrisku handiko AA-sistema batek 2. atalean ezarritako betekizunak betetzen dituela frogatzeko, agintaritzek erraz ulertzeko moduko hizkuntza batean. Horretarako, halaber, zaindu egingo dute dokumentazio teknikoa agintaritza horien esku jartzen dela.

7. Agintaritza eskudunek neurriren bat hartzen badute inportatzaileek merkatuan jarri duten arrisku handiko AA-sistema baten inguruan, inportatzaileak lankidetzan arituko dira agintaritza eskudun horiekin, bereziki sistema horrek dakartzan arriskuak murrizteko eta arintzeko bada.

24. artikulua.– Banatzaileen betebeharrak

1. Arrisku handiko AA-sistema bat merkaturatu aurretik, banatzaileek egiaztatu egingo dute eskatzen den CE marka daramala eta EB adostasun-adierazpenaren —47. artikuluan aipatzen da— eta erabilera-jarraibideen kopia bana dituela, eta sistema horren hornitzaileak eta inportatzaileak, dagokionaren arabera, 16.b), 16.c) eta 23.3 artikuluetan ezarritako betebeharrak bete dituztela, hurrenez hurren.

2. Banatzaile batek, eskura duen informazioan oinarrituta, uste badu arrisku handiko AA-sistemaren bat ez datorrela ados 2. atalean ezarritako betekizunekin, edo hori pentsatzeko arrazoiak baditu, ez du merkaturatuko harik eta betekizunekin ados etortzea lortu arte. Gainera, arrisku handiko AA-sistemak arriskuren bat dakarrenean 79.1 artikuluen zentzuan,



apartado 1, el distribuidor informará de ello al proveedor o importador del sistema, según corresponda.

3. Mientras sean responsables de un sistema de IA de alto riesgo, los distribuidores se asegurarán de que las condiciones de almacenamiento o transporte, cuando proceda, no comprometen el cumplimiento por parte del sistema de los requisitos establecidos en la sección 2.

4. Los distribuidores que consideren o tengan motivos para considerar, con arreglo a la información en su poder, que un sistema de IA de alto riesgo que han comercializado no es conforme con los requisitos establecidos en la sección 2 adoptarán las medidas correctoras necesarias para que sea conforme, para retirarlo del mercado o recuperarlo, o velarán por que el proveedor, el importador u otro operador pertinente, según proceda, adopte dichas medidas correctoras. Cuando un sistema de IA de alto riesgo presente un riesgo en el sentido del artículo 79, apartado 1, su distribuidor informará inmediatamente de ello al proveedor o al importador del sistema y a las autoridades competentes respecto al sistema de IA de alto riesgo de que se trate y dará detalles, en particular, sobre la no conformidad y las medidas correctoras adoptadas.

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

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

Artículo 25.— Responsabilidades a lo largo de la cadena de valor de la IA

1. Cualquier distribuidor, importador, responsable del despliegue o tercero será considerado proveedor de un sistema de IA de alto riesgo a los efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor previstas en el artículo 16 en cualquiera de las siguientes circunstancias:

a) cuando ponga su nombre o marca en un sistema de IA de alto riesgo previamente introducido en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignan de otro modo;

banatzaileak horren berri emango dio sistemaren hornitzaileari edo inportatzaileari, dagokionaren arabera.

3. Arrisku handiko AA-sistema baten arduradunak diren bitartean, banatzaileek ziurtatuko dute biltegiatze- edo garraio-baldintzek, hala dagokionean, ez dutela arriskuan jartzen sistema horrek 2. atalean ezarritako betekizunak betetzea.

4. Baldin eta banatzailearen batek, eskura duen informazioan oinarrituta, uste badu merkaturatu duen arrisku handiko AA-sistemaren bat ez datorrela ados 2. atalean ezarritako betekizunekin, edo hori pentsatzeko arrazoiak baditu, behar diren neurriak hartuko ditu betekizunekin ados etor dadin, edo merkatutik erretiratzeko edo berreskuratzeko, edo zaindu egingo du hornitzaileak, inportatzaileak edo dagokion beste operadore batek, dagokionaren arabera, neurri zuzentzaile horiek hartuko dituela. Arrisku handiko AA-sistemak arriskuren bat dakarrenean 79.1 artikulua zentzuan, haren banatzaileak berehala emango die horren berri sistemaren hornitzaileari edo inportatzaileari eta dagokion arrisku handiko AA-sistemari dagozkion agintaritza eskudunei, eta, bereziki, desadostasunari buruzko xehetasunak eta hartu diren neurri zuzentzaileak azalduko ditu.

5. Arrisku handiko AA-sistema baten banatzaileek beharrezko den informazio eta dokumentazio guztia emango diete agintaritza eskudunei, arrazoituta eskatuz gero, sistemak 2. atalean ezarritako betekizunak betetzen dituela frogatzeko hartu behar izan diren jarduketari buruz —1.tik 4.era bitarteko apartatueta ezarritakoa betez—.

6. Agintaritza eskudunek neurritan bat hartzen badute banatzaileek merkaturatu duten arrisku handiko AA-sistema baten inguruan, banatzaileak lankidetzan arituko dira agintaritza eskudun horiekin, bereziki sistema horrek dakartzan arriskuak murrizteko edo arintzeko bada.

25. artikulua.— AAren balio-kateko erantzukizunak

1. Erregelamendu honen ondorioetarako, banatzaile, inportatzaile, hedapenaren arduradun edo hirugarren oro arrisku handiko AA-sistema baten hornitzaileat hartuko da, eta 16. artikuluan aurreikusita dauden hornitzailearen betebeharrak bete beharko ditu, egoera hauetako edozein gertatzen denean:

a) Bere izena edo marka jartzen dioenean ordurako merkatuan jarrita edo zerbitzuan ipinita dagoen arrisku handiko AA-sistema bati, betebeharrak beste modu batean esleitzen direla ezartzen duten kontratu-akordioak gorabehera.



cuando modifique sustancialmente un sistema de IA de alto riesgo que ya haya sido introducido en el mercado o puesto en servicio de tal manera que siga siendo un sistema de IA de alto riesgo con arreglo al artículo 6;

cuando modifique la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido considerado de alto riesgo y ya haya sido introducido en el mercado o puesto en servicio, de tal manera que el sistema de IA de que se trate se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6.

2. Cuando se den las circunstancias mencionadas en el apartado 1, el proveedor que inicialmente haya introducido en el mercado el sistema de IA o lo haya puesto en servicio dejará de ser considerado proveedor de ese sistema de IA específico a efectos del presente Reglamento. Ese proveedor inicial cooperará estrechamente con los nuevos proveedores y facilitará la información necesaria, el acceso técnico u otra asistencia razonablemente previstos que sean necesarios para el cumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en lo que respecta al cumplimiento de la evaluación de la conformidad de los sistemas de IA de alto riesgo. El presente apartado no se aplicará en los casos en que el proveedor inicial haya indicado claramente que su sistema de IA no debe ser transformado en un sistema de IA de alto riesgo y, por lo tanto, no está sujeto a la obligación de facilitar la documentación.

3. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de productos contemplados en los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el fabricante del producto será considerado proveedor del sistema de IA de alto riesgo y estará sujeto a las obligaciones previstas en el artículo 16 en alguna de las siguientes circunstancias:

a) que el sistema de IA de alto riesgo se introduzca en el mercado junto con el producto bajo el nombre o la marca del fabricante del producto;

que el sistema de IA de alto riesgo se ponga en servicio bajo el nombre o la marca del fabricante del producto después de que el producto haya sido introducido en el mercado.

4. El proveedor de un sistema de IA de alto riesgo y el tercero que suministre un sistema de IA de alto riesgo, herramientas, servicios, componentes o procesos que se utilicen o integren en un sistema de IA de alto riesgo especificarán, mediante acuerdo escrito, la información, las capacidades, el acceso técnico y otra asistencia que sean necesarios, sobre la base del estado de la técnica generalmente reconocido, para que el proveedor del

Nabarmen aldatzen duenean merkatuan jarrita edo zerbitzuan ipinita dagoen arrisku handiko AA-sistema bat, baina arrisku handiko AA-sistema bat izaten jarraitzen duenean 6. artikuluan ezarritakoaren arabera.

Merkatuan jarrita edo zerbitzuan ipinita dagoen eta arrisku handikotzat jo ez den AA-sistema baten helburu aurreikusia aldatzen duenean, erabilera orokorreko AA-sistema batena barne, baldin eta AA-sistema hori arrisku handiko AA-sistema bihurtzen bada 6. artikuluan ezarritakoaren arabera.

2. Artikulu honen 1. apartatuan aipatutako inguruabarrak gertatzen direnean, AA-sistema hasiera batean merkatuan jarri edo zerbitzuan ipini zuen hornitzaileak utzi egingo dio AA-sistema espezifiko horren hornitzaile izateari erregelamendu honen ondorioetarako. Hasierako hornitzaile horrek lankidetza estuan jardungo du hornitzaile berriekin, eta beharrezkoak diren informazioa, sarbide teknikoa edo zentzuz aurreikusitako beste laguntza batzuk emango ditu erregelamendu honetan ezarritako betebeharrak betetzeko, eta bereziki arrisku handiko AA-sistemen adostasuna ebaluatzeko betebeharra betetzeko. Apartatu hau ez da aplikatuko baldin eta hasierako hornitzaileak argi adierazi badu bere AA-sistema ez dela eraldatu behar arrisku handiko AA-sistema izateko, eta, beraz, ez duela dokumentazioa emateko betebeharrak.

3. Batasunaren harmonizazioko lege-egintzek —I. eranskineko A atalean daude zerrendatuta— araututako produktuen segurtasun-osagaiak diren arrisku handiko AA-sistemen kasuan, produktuaren fabrikatzailea hartuko da arrisku handiko AA-sistemaren hornitzailetzat, eta 16. artikuluan aurreikusita dauden betebeharrak bete beharko ditu, egoera hauetako edozein gertatzen denean:

a) Arrisku handiko AA-sistema produktuaren fabrikatzailearen izenarekin edo markarekin jartzen denean merkatuan produktuarekin batera.

Produktua merkatuan jarri ondoren ipintzen denean arrisku handiko AA-sistema zerbitzuan produktuaren fabrikatzailearen izenarekin edo markarekin.

4. Arrisku handiko AA-sistema baten hornitzaileak eta arrisku handiko AA-sistema bat edo arrisku handiko AA-sistemetan erabiltzen edo integratzen diren tresnak, zerbitzuak, osagaiak edo prozesuak hornitzen dituen hirugarrenak idatzizko akordio bidez zehaztuko dituzte beharrezkoak diren informazioa, gaitasunak, sarbide teknikoa eta beste laguntza batzuk, oro har aitoritutako teknikaren egoeran oinarrituta, arrisku handiko AA-



sistema de IA de alto riesgo pueda cumplir plenamente las obligaciones establecidas en el presente Reglamento. El presente apartado no se aplicará a terceros que pongan a disposición del público herramientas, servicios, procesos o componentes distintos de modelos de IA de uso general, en el marco de una licencia libre y de código abierto.

La Oficina de IA podrá elaborar y recomendar cláusulas contractuales tipo, de carácter voluntario, entre los proveedores de sistemas de IA de alto riesgo y terceros que suministren herramientas, servicios, componentes o procesos que se utilicen o integren en los sistemas de IA de alto riesgo. Cuando elabore esas cláusulas contractuales tipo de carácter voluntario, la Oficina de IA tendrá en cuenta los posibles requisitos contractuales aplicables en determinados sectores o modelos de negocio. Las cláusulas contractuales tipo de carácter voluntario se publicarán y estarán disponibles gratuitamente en un formato electrónico fácilmente utilizable.

5. Los apartados 2 y 3 se entenderán sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial, la información empresarial confidencial y los secretos comerciales, de conformidad con el Derecho de la Unión y nacional.

Artículo 26.– Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo

1. Los responsables del despliegue de sistemas de IA de alto riesgo adoptarán medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen, de acuerdo con los apartados 3 y 6.

2. Los responsables del despliegue encomendarán la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

3. Las obligaciones previstas en los apartados 1 y 2 no afectan a otras obligaciones que el Derecho nacional o de la Unión imponga a los responsables del despliegue ni a su libertad para organizar sus propios recursos y actividades con el fin de poner en práctica las medidas de supervisión humana que indique el proveedor.

4. Sin perjuicio de lo dispuesto en los apartados 1 y 2, el responsable del despliegue se asegurará de que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos.

sistemaren hornitzaileak erabat bete ahal izan ditzan erregelamendu honetan ezarritako betebeharrak. Apartatu hau ez zaie aplikatuko erabilera orokorreko AA-ereduez bestelako tresnak, zerbitzuak, prozesuak edo osagaiak herritarren eskura jartzen dituzten hirugarrenei, lizentzia libre eta kode ireki baten esparruan egiten badute.

AA-bulegoak kontratueterako klausula-ereduak prestatu eta gomenda ditzake, borondatezkoak, arrisku handiko AA-sistemen hornitzaileentzat eta arrisku handiko AA-sistemetan erabiltzen edo integratzen diren tresnak, zerbitzuak, osagaiak edo prozesuak hornitzen dituzten hirugarrenentzat. Kontratueterako borondatezko klausula-eredu horiek egiten dituenean, AA-bulegoak kontuan hartuko ditu sektore edo negozio-eredu jakin batzuetan aplikatzekoak izan daitezkeen kontratu-betekizunak. Kontratueterako borondatezko klausulak argitaratu egingo dira, eta doan egongo dira eskuragarri erraz erabiltzeko moduko formatu elektroniko batean.

5. Jabetza intelektual eta industrialeko eskubideak eta enpresa-informazio konfidentziala edo merkataritza-sekretuak zaindu eta babesteko beharra alde batera utzi gabe ulertuko dira 2. eta 3. apartatuak, Batasuneko zuzenbidearekin eta zuzenbide nazionalarekin bat etorritik.

26. artikulua.– Arrisku handiko AA-sistemen hedapenaren arduradunen betebeharrak

1. Arrisku handiko AA-sistemen hedapenaren arduradunek neurri teknikoak eta antolakuntzakoak hartuko dituzte sistema horiek erabilera-jarraibideen arabera erabiltzen dituztela bermatzeko, 3. eta 6. apartatuen arabera.

2. Behar diren konpetentzia, prestakuntza eta aginpidea dituzten pertsona fisikoen esku utziko dute hedapenaren arduradunek giza ikuskapena.

3. Artikulu honen 1. eta 2. apartatuetan aurreikusitako betebeharrak ez diete eragiten Batasuneko zuzenbideak edo zuzenbide nazionalak hedapenaren arduradunei ezartzen dizkien beste betebeharrak batzuei, ez eta hornitzaileak adierazitako giza ikuskapeneko neurriak praktikan jartzeko baliabide eta jarduera propioak antolatzeko askatasunari ere.

4. Artikulu honen 1. eta 2. apartatuetan xedatutakoa gorabehera, hedapenaren arduradunak ziurtatu egingo du sarrera-datuak egokiak eta behar bezain adierazgarriak direla, arrisku handiko AA-sistemaren helburu aurreikusia kontuan hartuta, datu horien gaineko kontrola egiten duen neurrian.



5. Los responsables del despliegue vigilarán el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso y, cuando proceda, informarán a los proveedores con arreglo al artículo 72. Cuando los responsables del despliegue tengan motivos para considerar que utilizar el sistema de IA de alto riesgo conforme a sus instrucciones puede dar lugar a que ese sistema de IA presente un riesgo en el sentido del artículo 79, apartado 1, informarán, sin demora indebida, al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente y suspenderán el uso de ese sistema. Cuando los responsables del despliegue detecten un incidente grave, informarán asimismo inmediatamente de dicho incidente, en primer lugar, al proveedor y, a continuación, al importador o distribuidor y a la autoridad de vigilancia del mercado pertinente. En el caso de que el responsable del despliegue no consiga contactar con el proveedor, el artículo 73 se aplicará *mutatis mutandis*. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue de sistemas de IA que sean autoridades garantes del cumplimiento del Derecho.

En el caso de los responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros, se considerará que se ha cumplido la obligación de vigilancia prevista en el párrafo primero cuando se respeten las normas sobre sistemas, procesos y mecanismos de gobernanza interna de acuerdo con el Derecho pertinente en materia de servicios financieros.

6. Los responsables del despliegue de sistemas de IA de alto riesgo conservarán los archivos de registro que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que se disponga otra cosa en el Derecho de la Unión o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales.

Los responsables del despliegue que sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros mantendrán los archivos de registro como parte de la documentación conservada en virtud del Derecho de la Unión en materia de servicios financieros.

7. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empleadores informarán a los

5. Hedapenaren arduradunek arrisku handiko AA-sistemaren funtzionamendua zaindiko dute erabilera-jarraibideetan oinarrituta, eta, hala dagokionean, informazioa emango diete hornitzaileei, 72. artikulua arabera. Hedapenaren arduradunek arrazoiak badituzte pentsatzeko arrisku handiko AA-sistema bere jarraibideen arabera erabiltzearen ondorioz gerta daitekeela AA-sistema horrek arriskuren bat ekartzea 79.1 artikulua zentzuan, bidegabeko atzerapenik gabe jakinaraziko diete hornitzaileari edo banatzaileari eta merkatua zaintzeko dagokion agintaritzari, eta eten egingo dute sistema horren erabilera. Hedapenaren arduradunek gorabehera larri bat detektatzen dutenean, berehala jakinaraziko diete, lehenik eta behin, hornitzaileari, eta, ondoren, inportatzaileari edo banatzaileari eta merkatua zaintzeko dagokion agintaritzari. Hedapenaren arduradunak hornitzailearekin harremanetan jartzea lortzen ez badu, *mutatis mutandis* aplikatuko da 73. artikulua. Betebehar horretan ez dira sartuko zuzenbidea betearazteko agintaritzaren AA-sistemen hedapenaren arduradunen bereziki babestutako datu operatiboak.

Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera ezarritako barne-gobernanta, -sistema edo -prozesuei buruzko betekizunak bete behar dituzten finantza-entitateak direnean hedapenaren arduradunak, lehenengo paragrafoan aurreikusitako zaintza-betebeharra bete dela ulertuko da barne-gobernantzako sistema, prozesu eta mekanismoei buruzko arauak errespetatzen direnean, finantza-zerbitzuen arloan Batasunean dagokion zuzenbidearekin bat etorritik.

6. Arrisku handiko AA-sistemen hedapenaren arduradunek gorde egingo dituzte arrisku handiko AA-sistemen automatikoki sortutako erregistro-artxiboak, artxibo horiek beren kontrolpean dauden neurrian. Arrisku handiko AA-sistemaren helburu aurreikusirako egokia den denbora-tartean gordeko dituzte, gutxienez sei hilabetez, salbu eta besterik xedatzen badu aplikatzekoa den Batasuneko zuzenbideak edo zuzenbide nazionalak, bereziki datu pertsonalen babesaren arloko Batasunean zuzenbidearekin bat etorritik.

Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera ezarritako barne-gobernanta, -sistema edo -prozesuei buruzko betekizunak bete behar dituzten finantza-entitateak direnean hedapenaren arduradunak, gordetako dokumentazioaren zati gisa mantenduko dituzte erregistro-artxiboak, finantza-zerbitzuen arloan Batasunean dagokion zuzenbidearekin bat etorritik.

7. Arrisku handiko AA-sistema bat lantokian zerbitzuan ipini edo erabili aurretik, arrisku handiko AA-sistemaren erabilaren eraginpean egongo direla



representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo. Esta información se facilitará, cuando proceda, con arreglo a las normas y procedimientos establecidos en el Derecho de la Unión y nacional y conforme a las prácticas en materia de información a los trabajadores y sus representantes.

8. Los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas o instituciones, órganos y organismos de la Unión cumplirán las obligaciones de registro a que se refiere el artículo 49. Cuando dichos responsables del despliegue constaten que el sistema de IA de alto riesgo que tienen previsto utilizar no ha sido registrado en la base de datos de la UE a que se refiere el artículo 71, no utilizarán dicho sistema e informarán al proveedor o al distribuidor.

9. Cuando proceda, los responsables del despliegue de sistemas de IA de alto riesgo utilizarán la información facilitada conforme al artículo 13 del presente Reglamento para cumplir la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos que les imponen el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680.

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

En caso de que se deniegue la autorización contemplada en el párrafo primero, dejará de utilizarse el sistema de identificación biométrica remota en diferido objeto de la solicitud de autorización con efecto inmediato y se eliminarán los datos personales asociados al uso del sistema de IA de alto riesgo para el que se solicitó la autorización.

Dicho sistema de IA de alto riesgo de identificación biométrica remota en diferido no se utilizará en ningún caso a los efectos de la garantía del cumplimiento del Derecho de forma indiscriminada, sin que exista relación

jakinaraziko diete enplegatzaile diren hedapenaren arduradunek langileen ordezkarietara eta ukitutako langileei. Informazio hori, hala dagokionean, Batasuneko zuzenbidean edo zuzenbide nazionalen ezarritako arau eta prozeduren arabera emango da, eta langileei eta haien ordezkarietara informazioa emateko jardunbideei jarraikiz.

8. Batasuneko instituzio, organo eta organismo edo agintaritzak publikoak diren arrisku handiko AA-sistemen hedapenaren arduradunek 49. artikuluan aipatzen diren erregistro-betebeharrak beteko dituzte. Hedapenaren arduradun horiek egiaztatzen badute erabili nahi duten arrisku handiko AA-sistema ez dela erregistratu 71. artikuluan aipatzen den EBren datu-basean, ez dute sistema hori erabiliko, eta hornitzaileari edo banatzaileari jakinaraziko diote.

9. Hala dagokionean, arrisku handiko AA-sistemen hedapenaren arduradunek erregelamendu honen 13. artikuluan arabera emandako informazioa erabiliko dute (EB) 2016/679 Erregelamenduari 35. artikulua edo (EB) 2016/680 Zuzentarauaren 27. artikulua datuen babesaren gaineko inpaktuen ebaluazioa egiteko ezartzen dieten betebeharrak betetzeko.

10. (EB) 2016/680 Zuzentarauan xedatutakoa gorabehera, ikerketa bat egiten ari bada eta ikerketa horren helburua bada delitu baten susmagarria edo egile zigortua aurkitzeko bilaketa selektiboa egitea, gerora egiten den urruneko identifikazio biometrikoko arrisku handiko AA-sistema baten hedapenaren arduradunak sistema hori erabiltzeko baimena eskatuko dio, *ex ante* edo bidegabeko atzerapenik gabe, eta gehienez berrogeita zortzi orduko epean, agintaritzak judizial edo administratibo bati, baldin eta agintaritzak horren erabakiak lotesleak badira eta berrikuspen judizialaren mende badaude, salbu eta susmagarri posible bat hasieran identifikatzeko erabiltzen bada, delituari zuzenean lotutako egitate objektibo eta egiaztagarrietan oinarrituta. Delitu jakin bat ikertzeko behar-beharrezkoa dena mugatu beharko da erabilera bakoitza.

Baldin eta lehenengo paragrafoan jasotako baimena ukatzen bada, ordutik aurrera ez da gehiago erabiliko gerora egiten den urruneko identifikazio biometrikoko sistema hori —eskaeraren xede dena—, berehalako ondorioekin, eta ezabatu egingo dira baimena eskatu zen arrisku handiko AA-sistemaren erabilerrari lotutako datu pertsonalak.

Gerora egiten den urruneko identifikazio biometrikoko arrisku handiko AA-sistema hori ez da inola ere erabiliko bereizkuntzarik gabe zuzenbidea betearazteko, ez baldin badago inolako loturarik delitu batekin, prozesu



alguna con un delito, un proceso penal, una amenaza real y actual o real y previsible de delito, o con la búsqueda de una persona desaparecida concreta. Se velará por que las autoridades garantes del cumplimiento del Derecho no puedan adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida de dichos sistemas de identificación biométrica remota en diferido.

El presente apartado se entiende sin perjuicio del artículo 9 del Reglamento (UE) 2016/679 y del artículo 10 de la Directiva (UE) 2016/680 para el tratamiento de los datos biométricos.

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

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

Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota en diferido.

11. Sin perjuicio de lo dispuesto en el artículo 50 del presente Reglamento, los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas informarán a las personas físicas de que están expuestas a la utilización de los sistemas de IA de alto riesgo. En el caso de los sistemas de IA de alto riesgo que se utilicen a los efectos de la garantía del cumplimiento del Derecho, se aplicará el artículo 13 de la Directiva (UE) 2016/680.

12. Los responsables del despliegue cooperarán con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con el sistema de

penal batekin, delitua gertatzeko benetako eta uneko mehatxu batekin edo delitua gertatzeko benetako eta aurreikusteko moduko mehatxu batekin, edo desagertuta dagoen pertsona jakin bat bilatzearekin. Zaindu egingo da zuzenbidea betearazteko agintaritzek ezin izango dutela hartu pertsona bati ondorio juridiko kaltegarriak eragingo dizkion erabakirik, baldin eta erabaki horren oinarri bakarra gerora egiten den urruneko identifikazio biometrikoko sistemen irteera-emaizak badira.

Apartatu honek ez die kalterik egingo (EB) 2016/679 Erregelamenduaren 9. artikuluari eta (EB) 2016/680 Zuzentarauaren 10. artikuluari, datu biometrikoen tratamenduaren arloan.

Helburua edo hedapenaren arduraduna gorabehera, arrisku handiko AA-sistema horien erabilera oro dokumentatuko da dagokion polizia-espedituean, eta dagokion merkatua zaintzeko agintaritzaren eta datuak babesteko agintaritza nazionalaren esku jarriko da, aldez aurretik eskatuz gero, kanpoan geratuko dela zuzenbidea betearaztearekin lotutako bereziki babestutako datu operatiboak zabaltzea. Paragrafo honek ez ditu eragotziko (EB) 2016/680 Zuzentarauak kontrol-agintaritzei emandako ahalak.

Hedapenaren arduradunek urtero aurkeztuko dizkiete txostenak merkatua zaintzeko agintaritza egokiari eta datuak babesteko agintaritza nazionalari. Txosten horietan azalduko dute ea zer-nolako erabilera eman dieten gerora egiten den urruneko identifikazio biometrikoko sistemei, kanpoan geratuko dela zuzenbidea betearaztearekin lotutako bereziki babestutako datu operatiboak zabaltzea. Hedapen bat baino gehiago estaltzeko moduan gehitu ahal izango dira txostenak.

Estatu kideek, Batasuneko zuzenbidearekin bat etorritik, lege murriztaileagoak onartu ahal izango dituzte gerora egiten den urruneko identifikazio biometrikoko sistemen erabilerari buruz.

11. Erregelamendu honen 50. artikuluan xedatutakoari kalterik egin gabe, III. eranskinean aipatzen diren arrisku handiko AA-sistemen hedapenaren arduradunek, pertsona fisikoekin lotutako erabakiak hartzen badituzte edo erabakiak hartzen laguntzen badute, arrisku handiko AA-sistemen erabileraren eraginpean daudela jakinaraziko diete pertsona fisikoei. Zuzenbidea betearazteko erabiltzen diren arrisku handiko AA-sistemen kasuan, (EB) 2016/680 Zuzentarauaren 13. artikulua aplikatuko da.

12. Hedapenaren arduradunak lankidetzan arituko dira agintaritza eskudunekin, erregelamendu hau aplikatzeko



IA de alto riesgo con el objetivo de aplicar el presente Reglamento.

Artículo 27.– Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo

1. Antes de desplegar uno de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del despliegue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, y los responsable del despliegue de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, letras b) y c), llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales. A tal fin, los responsables del despliegue llevarán a cabo una evaluación que consistirá en:

a) una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista;

una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo;

las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico;

los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos determinadas con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el proveedor con arreglo al artículo 13;

una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso;

f) las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación.

2. La obligación descrita con arreglo al apartado 1 se aplicará al primer uso del sistema de IA de alto riesgo. En casos similares, el responsable del despliegue podrá basarse en evaluaciones de impacto relativas a los derechos fundamentales realizadas previamente o a evaluaciones de impacto existentes realizadas por los proveedores. Si, durante el uso del sistema de IA de alto

helburuarekin agintaritza horiek arrisku handiko AA-sistemari dagokionez hartzen duten edozein neurritan.

27. artikulua.– Oinarritzko eskubideen gaineko inpaktuaren ebaluazioa arrisku handiko AA-sistemetarako

1. Erregelamendu honen 6.2 artikuluan aipatutako arrisku handiko AA-sistema bat hedatu aurretik, III. eranskinen 2. puntuan zerrendatutako eremuan erabiliko diren arrisku handiko AA-sistemak izan ezik, sistema horiek erabiltzeak oinarritzko eskubideen gainean izan dezakeen inpaktua ebaluatuko dute hedapenaren arduradunek, baldin eta zerbitzu publikoak ematen dituzten entitate pribatuak edo zuzenbide publikoko organismoak badira, edo III. eranskinen 5. puntuko b) eta c) letretan aipatzen diren arrisku handiko AA-sistemen hedapenaren arduradunak badira. Horretarako, ebaluazio bat egingo dute hedapenaren arduradunek, alderdi hauek zehaztuz:

a) deskribapen bat, azalduz arrisku handiko AA-sistema hedapenaren arduradunaren zer prozesutan erabiliko den helburu aurreikusiarekin bat;

deskribapen bat, azalduz zer denbora-tartetan aurreikusi den erabiltzea arrisku handiko AA-sistema bakoitza, eta zein den sistema erabiltzeko aurreikusten den maiztasuna;

testuinguru espezifikoan erabili izanak uki ditzakeen pertsona fisikoen eta kolektiboen kategoriak;

apartatu honetako c) letren arabera, pertsona fisikoen eta kolektiboen kategoriei eragin diezaiaketen kalte-arrisku espezifikoak, kontuan hartuta hornitzaileak 13. artikuluen arabera emandako informazioa;

giza ikuskapeneko neurrien aplikazioaren deskribapen bat, erabilera-jarraibideen arabera;

f) arrisku horiek gauzatuz gero hartu beharko liratekeen neurriak, barne-gobernantzako erabakiak eta erreklamazio-mekanismoak barne.

2. Arrisku handiko AA-sistemaren lehenengo erabilerari aplikatuko zaio 1. apartatuaren arabera deskribatutako betebeharra. Antzeko kasuetan, aldez aurretik egin diren oinarritzko eskubideen gaineko inpaktuaren ebaluazioak edo hornitzaileek egindako inpaktuaren ebaluazioak hartu ahal izango ditu oinarri hedapenaren arduradunak. Arrisku handiko AA-sistema



riesgo, el responsable del despliegue considera que alguno de los elementos enumerados en el apartado 1 ha cambiado o ha dejado de estar actualizado, adoptará las medidas necesarias para actualizar la información.

3. Una vez realizada la evaluación a que se refiere el apartado 1 del presente artículo, el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado, presentando el modelo cumplimentado a que se refiere el apartado 5 del presente artículo. En el caso contemplado en el artículo 46, apartado 1, los responsables del despliegue podrán quedar exentos de esta obligación de notificación.

4. Si ya se cumple cualquiera de las obligaciones establecidas en el presente artículo mediante la evaluación de impacto relativa a la protección de datos realizada con arreglo al artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo complementará dicha evaluación de impacto relativa a la protección de datos.

5. La Oficina de IA elaborará un modelo de cuestionario, también mediante una herramienta automatizada, a fin de facilitar que los responsables del despliegue cumplan sus obligaciones en virtud del presente artículo de manera simplificada.

SECCIÓN 4

Autoridades notificantes y organismos notificados

Artículo 28.— Autoridades notificantes

1. Cada Estado miembro nombrará o constituirá al menos una autoridad notificante que será responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión. Dichos procedimientos se desarrollarán por medio de la cooperación entre las autoridades notificantes de todos los Estados miembros.

2. Los Estados miembros podrán decidir que la evaluación y la supervisión contempladas en el apartado 1 sean realizadas por un organismo nacional de acreditación en el sentido del Reglamento (CE) n.º 765/2008 y con arreglo a este.

3. Las autoridades notificantes se constituirán, se organizarán y funcionarán de forma que no surjan conflictos de intereses con los organismos de

erabiltzen den bitartean, hedapenaren arduradunak uste badu 1. apartatuan zerrendatutako elementuren bat aldatu dela edo eguneratuta egoteari utzi diola, behar diren neurriak hartuko ditu informazioa eguneratzeko.

3. Artikulu honen 1. apartatuan aipatzen den ebaluazioa egin ondoren, hedapenaren arduradunak emaitzen berri emango dio merkatua zaintzeko agintaritzari, beteta aurkeztuz artikulu honen 5. apartatuan aipatzen den eredua. Erregelamendu honen 46.1 artikuluan aurreikusitako kasuan, hedapenaren arduradunak salbuetsita gera daitezke jakinarazteko betebeharrak horretatik.

4. Artikulu honetan ezarritako betebeharrak edozein jada betetzen bada (EB) 2016/679 Erregelamenduari 35. artikuluari edo (EB) 2016/680 Zuzentarauaren 27. artikuluari arabera egindako datuen babesaren gaineko inpaktuaren ebaluazioaren bidez, artikulu honen 1. apartatuan aipatzen den oinarriko eskubideen gaineko inpaktuaren ebaluazioak osatu egingo du datuen babesaren gaineko inpaktuaren ebaluazio hori.

5. AA-bulegoak galdetegi-eredu bat egingo du, tresna automatizatu baten bidez, modu sinplifikatuan errazteko hedapenaren arduradunak artikulu honen arabera dituzten betebeharrak bete ditzatela.

4. ATALA

Agintaritza jakinarazleak eta organismo jakinaraziak

28. artikulua.— Agintaritza jakinarazleak

1. Estatu kide bakoitzak agintaritza jakinarazle bat izendatu edo eratuko du gutxienez, eta adostasuna ebaluatzeako organismoen ebaluazio, izendapen eta jakinarazpenerako behar diren prozedurak ezartzeaz eta gauzatzeaz eta organismoak berak gainbegiratzear arduratuko da agintaritza jakinarazle hori. Estatu kide guztietako agintaritza jakinarazleen arteko lankidetzaren bidez garatuko dira prozedura horiek.

2. Estatu kideek hala erabakitzen badute, (EE) 765/2008 Erregelamenduan ezarritakoari jarraituz egiaztapen-organismo nazional batek egin ahal izango ditu 1. apartatuan aurreikusitako ebaluazioa eta gainbegiratzea, erregelamendu horretan ezarritakoaren arabera.

3. Agintaritza jakinarazleak eratzeko, antolatzeak eta funtzionatzeko moduak ez du inolako interes-gatazkarik eragingo adostasuna ebaluatzeako organismoekin, eta



evaluación de la conformidad y que se garantice la imparcialidad y objetividad de sus actividades.

4. Las autoridades notificantes se organizarán de forma que las decisiones relativas a la notificación de los organismos de evaluación de la conformidad sean adoptadas por personas competentes distintas de las que llevaron a cabo la evaluación de dichos organismos.

5. Las autoridades notificantes no ofrecerán ni ejercerán ninguna actividad que efectúen los organismos de evaluación de la conformidad, ni ningún servicio de consultoría de carácter comercial o competitivo.

6. Las autoridades notificantes preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.

7. Las autoridades notificantes dispondrán de suficiente personal competente para efectuar adecuadamente sus tareas. Cuando proceda, el personal competente tendrá los conocimientos especializados necesarios para ejercer sus funciones, en ámbitos como las tecnologías de la información, la IA y el Derecho, incluida la supervisión de los derechos fundamentales.

Artículo 29.– Solicitud de notificación por parte de un organismo de evaluación de la conformidad

1. Los organismos de evaluación de la conformidad presentarán una solicitud de notificación ante la autoridad notificante del Estado miembro en el que estén establecidos.

2. La solicitud de notificación irá acompañada de una descripción de las actividades de evaluación de la conformidad, del módulo o módulos de evaluación de la conformidad y los tipos de sistemas de IA en relación con los cuales el organismo de evaluación de la conformidad se considere competente, así como de un certificado de acreditación, si lo hay, expedido por un organismo nacional de acreditación, que declare que el organismo de evaluación de la conformidad cumple los requisitos establecidos en el artículo 31.

Se añadirá cualquier documento válido relacionado con las designaciones existentes del organismo notificado solicitante en virtud de cualquier otro acto de la legislación de armonización de la Unión.

3. Si el organismo de evaluación de la conformidad de que se trate no puede facilitar un certificado de acreditación, entregará a la autoridad notificante todas las pruebas documentales necesarias para verificar,

guztiz bermatuko da haien jardueren inpartzialtasuna eta objektibotasuna.

4. Agintaritza jakinarazleak antolatzean, kontuan hartuko da adostasuna ebaluatzeneko organismoen jakinarazpenei buruzko erabakiak organismo horien ebaluazioa egin zutenez bestelako pertsona gaituek hartu behar dituztela.

5. Agintaritza jakinarazleek ez dute eskainiko, ezta gauzatuko ere, adostasuna ebaluatzeneko organismoek egiten duten jarduerarik, eta ez dute inolako aholkularitza-zerbitzu komertzial edo lehiakorrik emango.

6. Lortutako informazioaren konfidentzialtasuna bermatuko dute agintaritza jakinarazleek, 78. artikuluan xedatutakoaren arabera.

7. Agintaritza jakinarazleek beren zereginak behar bezala egiteko behar beste langile gaitu izango dituzte. Hala dagokionean, langile gaituek beren eginkizunak betetzeko behar dituzten ezagutza espezializatuak izango dituzte, hala nola informazioaren teknologien, adimen artifizialaren eta zuzenbidearen alorretan, oinarritzko eskubideak gainbegiratzea barne.

29. artikulua.– Adostasuna ebaluatzeneko organismo baten jakinarazpen-eskaera

1. Adostasuna ebaluatzeneko organismoek jakinarazpen-eskaera bat aurkeztuko diote ezarrita dauden estatu kideko agintaritza jakinarazleari.

2. Jakinarazpen-eskaerarekin batera, deskribapen bat aurkeztuko da, bertan azaltzeko adostasuna ebaluatzeneko jarduerak, adostasuna ebaluatzeneko modulua edo moduluak eta adostasuna ebaluatzeneko organismoak haren eskumenekotzat jotzen dituen AA-sistema motak; horrez gain, egiaztapen-ziurtagiri bat ere aurkeztuko da, halakorik badago, egiaztapen-organismo nazional batek emana, adostasuna ebaluatzeneko organismoak 31. artikuluan ezarritako betekizunak betetzen dituela adierazteko.

Halaber, Batasunaren harmonizazioko legeriako egintzaren bati jarraikiz organismo jakinarazi eskatzaileak dituen izendapenekin zerikusia duen beste edozein baliozko dokumentu gehituko da.

3. Baldin eta adostasuna ebaluatzeneko organismoak ezin badu egiaztapen-ziurtagiririk eman, 31. artikuluan ezarritako betekizunak betetzen dituela egiaztatu, aitortu eta gainbegiratu ahal izateko beharrezkoak diren



reconocer y supervisar periódicamente que cumple los requisitos establecidos en el artículo 31.

4. En lo que respecta a los organismos notificados designados de conformidad con cualquier otro acto legislativo de armonización de la Unión, todos los documentos y certificados vinculados a dichas designaciones podrán utilizarse para apoyar su procedimiento de designación en virtud del presente Reglamento, según proceda. El organismo notificado actualizará la documentación a que se refieren los apartados 2 y 3 del presente artículo cuando se produzcan cambios pertinentes, para que la autoridad responsable de los organismos notificados pueda supervisar y verificar que se siguen cumpliendo todos los requisitos establecidos en el artículo 31.

Artículo 30.— Procedimiento de notificación

1. Las autoridades notificantes solo podrán notificar organismos de evaluación de la conformidad que hayan cumplido los requisitos establecidos en el artículo 31.

2. Las autoridades notificantes notificarán a la Comisión y a los demás Estados miembros, mediante el sistema de notificación electrónica desarrollado y gestionado por la Comisión, cada organismo de evaluación de la conformidad a que se refiere el apartado 1.

3. La notificación a que se refiere el apartado 2 del presente artículo incluirá información detallada de las actividades de evaluación de la conformidad, el módulo o módulos de evaluación de la conformidad y los tipos de sistemas de IA afectados, así como la certificación de competencia pertinente. Si la notificación no está basada en el certificado de acreditación a que se refiere el artículo 29, apartado 2, la autoridad notificante facilitará a la Comisión y a los demás Estados miembros las pruebas documentales que demuestren la competencia del organismo de evaluación de la conformidad y las disposiciones existentes destinadas a garantizar que se supervisará periódicamente al organismo y que este continuará satisfaciendo los requisitos establecidos en el artículo 31.

4. El organismo de evaluación de la conformidad de que se trate únicamente podrá realizar las actividades de un organismo notificado si la Comisión o los demás Estados miembros no formulan ninguna objeción en el plazo de dos semanas tras la notificación de una autoridad notificante cuando esta incluya el certificado de acreditación a que se refiere el artículo 29, apartado 2, o de dos meses tras la notificación de la autoridad notificante cuando esta incluya las pruebas documentales a que se refiere el artículo 29, apartado 3.

dokumentu-froga guztiak emango dizkio agintaritzak jakinarazleari.

4. Batasunaren harmonizazioko lege-egintzaren bati jarraikiz izendatutako organismo jakinaraziei dagokienez, izendapen horiei lotutako dokumentu eta ziurtagiri guztiak erabili ahal izango dira erregelamendu honen arabera dagokien izendapen-prozedurari sostengu emateko, dagokionaren arabera. Aldaketaren bat dagoenean, organismo jakinaraziak artikuluan honen 2. eta 3. apartatuetan aipatzen den dokumentazioa eguneratuko du, 31. artikuluan ezarritako betekizun guztiak betetzen jarraitzen direla gainbegiratu eta egiaztatu ahal izan dezan organismo jakinarazien agintaritzak arduradunak.

30. artikulua.— Jakinarazteko prozedura

1. Erregelamendu honen 31. artikuluan ezarritako betekizunak bete dituzten adostasuna ebaluatzeko organismoak bakarrik jakinarazi ahal izango dituzte agintaritzak jakinarazleek.

2. Batzordeak garatu eta kudeatutako jakinarazpen elektronikoko sistemaren bidez emango die agintaritzak jakinarazleek Batzordeari eta gainerako estatu kideei 1. apartatuan aipatutako adostasuna ebaluatzeko organismoen berri.

3. Artikulu honen 2. apartatuan aipatzen den jakinarazpenak informazio zehatza jasoko du adostasuna ebaluatzeko jardueri buruz, adostasuna ebaluatzeko moduluari edo moduluei buruz eta ukitutako AA-sistema motei buruz; era berean, dagokion gaitasun-ziurtagiria ere jasoko du. Jakinarazpena ez baldin badago oinarrituta 29.2 artikuluan aipatutako egiaztapen-ziurtagirian, adostasuna ebaluatzeko organismoaren eskumena egiaztatzen duten dokumentu-frogak emango dizkie agintaritzak jakinarazleak Batzordeari eta gainerako estatu kideei, bai eta organismoa aldizka gainbegiratu delako eta 31. artikuluan ezarritako betekizunak betetzen jarraitzen duela bermatzeko dauden xedapenak ere.

4. Adostasuna ebaluatzeko dena delako organismoak organismo jakinarazi baten jarduerak egin ahal izateko, ezinbestekoa izango da Batzordeak edo gainerako estatu kideek ez dezatela eragozpenik jarri agintaritzak jakinarazle baten jakinarazpena jaso eta bi asteko epean —baldin eta 29.2 artikuluan aipatzen den egiaztapen-ziurtagiria jasotzen badu—, edo agintaritzak jakinarazlearen jakinarazpena jaso eta bi hilabeteko epean —baldin eta 29.3 artikuluan aipatzen diren dokumentu-frogak jasotzen baditu—.



5. Cuando se formulen objeciones, la Comisión iniciará sin demora consultas con los Estados miembros pertinentes y el organismo de evaluación de la conformidad. En vista de todo ello, la Comisión enviará su decisión al Estado miembro afectado y al organismo de evaluación de la conformidad pertinente.

Artículo 31.— Requisitos relativos a los organismos notificados

1. Los organismos notificados se establecerán de conformidad con el Derecho nacional de los Estados miembros y tendrán personalidad jurídica.
2. Los organismos notificados satisfarán los requisitos organizativos, de gestión de la calidad, recursos y procesos, necesarios para el desempeño de sus funciones, así como los requisitos adecuados en materia de ciberseguridad.
3. La estructura organizativa, la distribución de las responsabilidades, la línea jerárquica y el funcionamiento de los organismos notificados ofrecerán confianza en su desempeño y en los resultados de las actividades de evaluación de la conformidad que realicen los organismos notificados.
4. Los organismos notificados serán independientes del proveedor de un sistema de IA de alto riesgo en relación con el cual lleven a cabo actividades de evaluación de la conformidad. Los organismos notificados serán independientes de cualquier otro operador con un interés económico en los sistemas de IA de alto riesgo que se evalúen, así como de cualquier competidor del proveedor. Ello no será óbice para el uso de sistemas de IA de alto riesgo evaluados que sean necesarios para las actividades del organismo de evaluación de la conformidad o para el uso de tales sistemas de alto riesgo con fines personales.
5. Los organismos de evaluación de la conformidad, sus máximos directivos y el personal responsable de la realización de las tareas de evaluación de la conformidad no intervendrán directamente en el diseño, el desarrollo, la comercialización o el uso de dichos sistemas de IA de alto riesgo, ni tampoco representarán a las partes que llevan a cabo estas actividades. Además, no efectuarán ninguna actividad que pudiera entrar en conflicto con su independencia de criterio o su integridad en relación con las actividades de evaluación de la conformidad para las que han sido notificados. Ello se aplicará especialmente a los servicios de consultoría.
6. Los organismos notificados estarán organizados y gestionados de modo que se garantice la independencia, objetividad e imparcialidad de sus actividades. Los organismos notificados documentarán

5. Eragozpenik jartzen bada, Batzordeak atzerapenik gabe hasiko ditu kontsultak kasuan kasuko estatu kideekin eta adostasuna ebaluatzeako organismoarekin. Hori guztia ikusita, ukitutako estatu kideari eta adostasuna ebaluatzeako dagokion organismoari bidaliko die Batzordeak hartutako erabakia.

31. artikulua.— Organismo jakinaraziei dagozkien betekizunak

1. Organismo jakinaraziak estatu kideetako zuzenbide nazionalaren arabera ezarriko dira, eta nortasun juridikoa izango dute.
2. Organismo jakinaraziek beren eginkizunak betetzeko beharrezkoak diren antolaketa, kalitate-kudeaketako eta baliabide eta prozesuetako betekizunak beteko dituzte, bai eta zibersegurtasunaren arloan egokiak diren betekizunak ere.
3. Organismo jakinarazien antolamendu-egiturak, erantzukizunen banaketak, lerro hierarkikoak eta funtzionamenduak konfiantza emango dute haien jardunean eta organismo jakinaraziek egiten dituzten adostasuna ebaluatzeako jardueren emaitzetan.
4. Organismo jakinaraziak, arrisku handiko AA-sistema baten gaineko adostasuna ebaluatzeako jarduerak egiten diren bitartean, independenteak izango dira sistema horren hornitzailearekiko. Organismo jakinaraziak guztiz independenteak izango dira ebaluatzen diren arrisku handiko AA-sistemetan interes ekonomikoa duen beste edozein operadorearekiko, bai eta hornitzailearen edozein lehiakiderekiko ere. Hori ez da oztopo izango adostasuna ebaluatzeako organismoaren jarduerak egiteko beharrezkoak diren ebaluatutako arrisku handiko AA-sistemak erabiltzeko, edo arrisku handiko sistema horiek helburu pertsonalekin erabiltzeko.
5. Adostasuna ebaluatzeako organismoek, haien zuzendari nagusiek eta adostasuna ebaluatzeako lanak egiteaz arduratzen diren langileek ez dute zuzenean esku hartuko arrisku handiko AA-sistema horiek diseinatu, garatu, merkaturatu edo erabiltzen, eta ez dituzte ordezkatuko jarduera horiek egiten dituzten alderdiak. Gainera, ez dute egingo, jakinarazpenaren ondorioz dituzten adostasuna ebaluatzeako jardueri dagokienez, beren irizpide-independentziarekin edo osotasunarekin gatazkan egon daitekeen jarduerarik. Aholkularitza-zerbitzuei aplikatuko zaie bereziki hori.
6. Organismo jakinaraziak antolatu eta kudeatzean, bermatu egingo dira bere jardueren independentzia, objektibotasuna eta inpartzialtasuna. Organismo jakinaraziek egitura bat eta prozedurak dokumentatu eta



e implantarán una estructura y procedimientos que garanticen la imparcialidad y permitan promover y poner en práctica los principios de imparcialidad aplicables en toda su organización, a todo su personal y en todas sus actividades de evaluación.

7. Los organismos notificados contarán con procedimientos documentados que garanticen que su personal, sus comités, sus filiales, sus subcontratistas y todos sus organismos asociados o personal de organismos externos mantengan, de conformidad con el artículo 78, la confidencialidad de la información que llegue a su poder en el desempeño de las actividades de evaluación de la conformidad, excepto en aquellos casos en que la ley exija su divulgación. El personal de los organismos notificados estará sujeto al secreto profesional en lo que respecta a toda la información obtenida en el ejercicio de las funciones que les hayan sido encomendadas en virtud del presente Reglamento, salvo en relación con las autoridades notificantes del Estado miembro en el que desarrollen sus actividades.

8. Los organismos notificados contarán con procedimientos para desempeñar sus actividades que tengan debidamente en cuenta el tamaño de los proveedores, el sector en que operan, su estructura y el grado de complejidad del sistema de IA de que se trate.

9. Los organismos notificados suscribirán un seguro de responsabilidad adecuado para sus actividades de evaluación de la conformidad, salvo que la responsabilidad la asuma el Estado miembro en que estén establecidos con arreglo al Derecho nacional o que el propio Estado miembro sea directamente responsable de la evaluación de la conformidad.

10. Los organismos notificados serán capaces de llevar a cabo todas sus tareas con arreglo al presente Reglamento con el máximo grado de integridad profesional y la competencia técnica necesaria en el ámbito específico, tanto si dichas tareas las efectúan los propios organismos notificados como si se realizan en su nombre y bajo su responsabilidad.

11. Los organismos notificados contarán con competencias técnicas internas suficientes para poder evaluar de manera eficaz las tareas que lleven a cabo agentes externos en su nombre. El organismo notificado dispondrá permanentemente de suficiente personal administrativo, técnico, jurídico y científico que tenga experiencia y conocimientos relativos a los tipos de sistemas de IA, los datos y la computación de datos pertinentes y a los requisitos establecidos en la sección 2.

12. Los organismos notificados participarán en las actividades de coordinación según lo previsto en el artículo 38. Asimismo, tomarán parte directamente o

ezarriko dituzte, halako moldez non inpartzialtasuna bermatuko duten eta aplikatzekoak diren inpartzialtasun-printzipioak sustatu eta praktikan jartzea ahalbidetuko duten antolakunde osoan, langile guztiei eta ebaluazio-jarduera guztietan.

7. Organismo jakinaraziek prozedura dokumentatuak izango dituzte, beren langileek, komiteek, filialek, azpikontrastek eta haiei atxikitako organismo guztiek edo kanpoko organismoetako langileek, 78. artikuluekin bat etorritik, adostasuna ebaluatzeko jarduerak egitean lortzen duten informazioaren konfidentzialtasuna zaintzen dutela bermatzeko, legeak informazio hori zabaltzea eskatzen duen kasuetan izan ezik. Organismo jakinarazietako langileak sekretu profesionalaren pean egongo dira erregelamendu honen arabera agindu zaizkien eginkizunak betetzean lortutako informazio guztiari dagokionez, jarduerak garatzen dituzten estatu kideko agintaritzak jakinarazleei dagokienez izan ezik.

8. Organismo jakinaraziek prozedurak izango dituzte beren jarduerak egiteko, behar bezala kontuan hartuta hornitzaileen tamaina, jarduten duten sektorea, haien egitura eta dagokion AA-sistemaren konplexutasun-maila.

9. Organismo jakinaraziek behar bezalako erantzukizun-aseguru bat sinatuko dute adostasuna ebaluatzeko beren jardueretarako, salbu eta erantzukizuna bere gain hartzen badu ezarritako dagoen estatu kideak —zuzenbide nazionalaren arabera—, edo estatu kidea bera bada adostasuna ebaluatzeko arduradun zuzena.

10. Organismo jakinaraziak gai izango dira beren zeregin guztiak erregelamendu honen arabera egiteko, ahalik eta osotasun profesional handienarekin eta eremu espezifikoan behar den konpetentzia teknikoarekin, bai zeregin horiek organismo jakinaraziek beraiek egiten dituztenean, bai beste batek egiten dituztenean haien izenean eta haien erantzukizunpean.

11. Organismo jakinaraziek barne-konpetentzia tekniko nahikoak izango dituzte kanpoko eragileek haien izenean egiten dituzten zereginak eraginkortasunez ebaluatu ahal izateko. AA-sistema motei, datuei eta datuen konputazioari eta 2. atalean ezarritako betekizunei buruzko esperientzia eta ezagutza dituzten behar adina administrari, teknikari, langile juridiko eta zientzialari izango ditu, etengabe, organismo jakinaraziak.

12. Organismo jakinaraziek koordinazio-jardueretan parte hartuko dute, 38. artikuluan aurreikusitakoaren arabera. Era berean, zuzenean edo ordezkariaren baten



mediante representación en organizaciones europeas de normalización, o se asegurarán de mantenerse al corriente de la situación actualizada de las normas pertinentes.

Artículo 32.— Presunción de conformidad con los requisitos relativos a los organismos notificados

Cuando un organismo de evaluación de la conformidad demuestre que cumple los criterios establecidos en las normas armonizadas pertinentes, o en partes de estas, cuyas referencias estén publicadas en el Diario Oficial de la Unión Europea, se presumirá que cumple los requisitos establecidos en el artículo 31 en la medida en que las normas armonizadas aplicables contemplen esos mismos requisitos.

Artículo 33.— Filiales de organismos notificados y subcontratación

1. Cuando un organismo notificado subcontrate tareas específicas relacionadas con la evaluación de la conformidad o recurra a una filial, se asegurará de que el subcontratista o la filial cumplan los requisitos establecidos en el artículo 31 e informará a la autoridad notificante en consecuencia.
2. Los organismos notificados asumirán la plena responsabilidad de las tareas realizadas por cualesquiera subcontratistas o filiales.
3. Las actividades solo podrán subcontratarse o delegarse en una filial previo consentimiento del proveedor. Los organismos notificados pondrán a disposición del público una lista de sus filiales.
4. Los documentos pertinentes sobre la evaluación de las cualificaciones del subcontratista o de la filial y el trabajo que estos realicen en virtud del presente Reglamento se mantendrán a disposición de la autoridad notificante durante un período de cinco años a partir de la fecha de finalización de la subcontratación.

Artículo 34.— Obligaciones operativas de los organismos notificados

1. Los organismos notificados verificarán la conformidad de los sistemas de IA de alto riesgo siguiendo los procedimientos de evaluación de la conformidad establecidos en el artículo 43.
2. Los organismos notificados evitarán cargas innecesarias para los proveedores cuando desempeñen sus actividades, y tendrán debidamente en cuenta el tamaño del proveedor, el sector en que opera, su estructura y el grado de complejidad del sistema de IA de alto riesgo de que se trate, en particular con vistas a reducir al mínimo las cargas administrativas y los costes

bidez hartuko dute parte Europako normalizazio-antolakundeetan, edo kasuan kasuko arauen egoeraren berri eguneratua izateaz arduratuko dira.

32. artikulua.— Organismo jakinaraziei dagozkien betekizunekiko adostasun-presuntzioa

Adostasuna ebaluatzeko organismo batek frogatzen badu dagozkion arau harmonizatuetan edo horien zati batzuetan ezarritako irizpideak betetzen dituela —haien erreferentziak Europar Batasunaren Aldizkari Ofizialean argitaratuta daudela—, ondorioztatuko da 31. artikuluan ezarritako betekizunak betetzen dituela, aplikatu beharreko arau harmonizatuak betekizun horiek berak jasotzen dituzten heinean.

33. artikulua.— Organismo jakinarazien filialak eta azpikontratazioa

1. Organismo jakinarazi batek adostasuna ebaluatzearekin lotutako zeregin espezifikoak azpikontratatzeko dituen edo filial batengana jotzen duenean, ziurtatuko du azpikontratatutako edo filialak bete egiten dituela 31. artikuluan ezarritako betekizunak, eta horren berri emango dio agintaritzari jakinarazleari.
2. Organismo jakinaraziek beren gain hartuko dute azpikontratatutako edo filialak egindako lanen erantzukizun osoa.
3. Jarduerak filial bati azpikontratatu edo eskuordetu ahal izateko, hornitzaileak ados dagoela adierazi beharko du aldez aurretik. Organismo jakinaraziek beren filialen zerrenda bat jarriko dute herritarren eskura.
4. Azpikontratatutako edo filialaren kualifikazioen ebaluazioari eta erregelamendu honen arabera egiten duten lanari buruzko dokumentuak agintaritzari jakinarazlearen eskura egongo dira bost urtez, azpikontratazioa amaitzen denetik aurrera.

34. artikulua.— Organismo jakinarazien betebeharrak

1. Organismo jakinaraziek arrisku handiko AA-sistemen adostasuna egiaztatuko dute, 43. artikuluan ezarritako adostasuna ebaluatzeko prozedurei jarraituz.
2. Organismo jakinaraziek saihestu egingo dute hornitzaileentzat beharrezkoak ez diren kargak eragitea beren jarduerak egiten dituzten bitartean, eta behar bezala hartuko dituzte kontuan, dagokion arrisku handiko AA-sistemari dagokionez, hornitzailearen tamaina, zein sektoretan jarduten duen, haren egitura eta konplexutasun-maila, bereziki ahalik eta gehien



del cumplimiento para las microempresas y pequeñas empresas en el sentido de la Recomendación 2003/361/CE. El organismo notificado respetará, sin embargo, el grado de rigor y el nivel de protección requeridos para que el sistema de IA de alto riesgo cumpla los requisitos del presente Reglamento.

3. Los organismos notificados pondrán a disposición de la autoridad notificante mencionada en el artículo 28, y le presentarán cuando se les pida, toda la documentación pertinente, incluida la documentación de los proveedores, a fin de que dicha autoridad pueda llevar a cabo sus actividades de evaluación, designación, notificación y supervisión, y de facilitar la evaluación descrita en la presente sección.

Artículo 35.— Números de identificación y listas de organismos notificados

1. La Comisión asignará un número de identificación único a cada organismo notificado, incluso cuando un organismo sea notificado con arreglo a más de un acto de la Unión.

2. La Comisión hará pública la lista de organismos notificados con arreglo al presente Reglamento, incluidos sus números de identificación y las actividades para las que hayan sido notificados. La Comisión se asegurará de que la lista se mantenga actualizada.

Artículo 36.— Cambios en las notificaciones

1. La autoridad notificante notificará a la Comisión y a los demás Estados miembros cualquier cambio pertinente en la notificación de un organismo notificado a través del sistema de notificación electrónica a que se refiere el artículo 30, apartado 2.

2. Los procedimientos establecidos en los artículos 29 y 30 se aplicarán a las ampliaciones del ámbito de aplicación de la notificación.

Para modificaciones de la notificación distintas de las ampliaciones de su ámbito de aplicación, se aplicarán los procedimientos establecidos en los apartados 3 a 9.

3. Cuando un organismo notificado decida poner fin a sus actividades de evaluación de la conformidad, informará de ello a la autoridad notificante y a los proveedores afectados tan pronto como sea posible y, cuando se trate de un cese planeado, al menos un año antes de poner fin a sus actividades. Los certificados del organismo notificado podrán seguir siendo válidos durante un plazo de nueve meses después del cese de las actividades del organismo notificado, siempre que otro organismo notificado haya confirmado por escrito

murritzeko administrazio-kargak eta betetze-kostuak mikroenpresentzat eta enpresa txikientzat, 2003/361/EE Gomendioaren ildotik. Organismo jakinaraziak, hala ere, errespetatu egingo ditu arrisku handiko AA-sistemak erregelamendu honetako betekizunak betetzeko eskatzen diren zorroztasun- eta babes-mailak.

3. Organismo jakinaraziek dagokion dokumentazio guztia —hornitzaileen dokumentazioa barne— jarriko dute 28. artikuluan aipatutako agintaritza jakinarazlearen esku, eta eskatzen zaienean aurkeztu egingo diote, agintaritza horrek ebaluazio-, izendapen-, jakinarazpen- eta gainbegiratze-jarduerak egin ahal izan ditzan eta atal honetan deskribatutako ebaluazioa erraztu dezan.

35. artikulua.— Organismo jakinarazien identifikazio-zenbakiak eta zerrendak

1. Batzordeak identifikazio-zenbaki bakar bana emango die organismo jakinaraziei, baita organismo bat Batasunaren egintza baten baino gehiagoren arabera jakinarazia denean ere.

2. Batzordeak erregelamendu honen araberako organismo jakinarazien zerrenda bat argitaratuko du, haien identifikazio-zenbakiak zehaztuta eta zer jardueratarako jakinarazi diren adierazita. Halaber, zerrenda eguneratuta mantentzen dela ziurtatuko du Batzordeak.

36. artikulua.— Aldaketak jakinarazpenetan

1. Aldaketarik egin behar bada organismo jakinarazi baten jakinarazpenean, agintaritza jakinarazleak Batzordeari eta gainerako estatu kideei jakinaraziko die, 30.2 artikuluan aipatzen den jakinarazpen elektronikoko sistemaren bidez.

2. Jakinarazpenaren aplikazio-eremua zabaltzen denean, 29. eta 30. artikuluetan ezarritako prozedurak aplikatuko dira.

Jakinarazpenaren aplikazio-eremua zabaltzeaz bestelako aldaketaren bat egiten denean, 3.etik 9.era bitarteko apartatueta ezarritako prozedurak aplikatuko dira.

3. Organismo jakinarazi batek adostasuna ebaluatzeke bere jarduerak amaitzea erabakitzen duenean, horren berri emango die agintaritza jakinarazleari eta ukitutako hornitzaileei, ahal bezain laster; gainera, lehenagotik pentsatu denean jarduera etengo dela, jarduerak amaitu baino urtebete lehenago jakinarazi beharko da, gutxienez. Organismo jakinarazien ziurtagiriek baliozkoak izaten jarraitu ahal izango dute organismo jakinaraziaren jarduerak amaitu eta bederatzi hilabeteko epean, baldin eta beste



que asumirá la responsabilidad de los sistemas de IA de alto riesgo cubiertos por dichos certificados. Este último organismo notificado realizará una evaluación completa de los sistemas de IA de alto riesgo afectados antes del vencimiento de ese plazo de nueve meses y antes de expedir nuevos certificados para esos sistemas. Si el organismo notificado ha puesto fin a sus actividades, la autoridad notificante retirará la designación.

4. Si una autoridad notificante tiene motivo suficiente para considerar que un organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, la autoridad notificante investigará el asunto sin demora y con la máxima diligencia. En ese contexto, informará al organismo notificado de que se trate acerca de las objeciones formuladas y le ofrecerá la posibilidad de exponer sus puntos de vista. Si la autoridad notificante llega a la conclusión de que el organismo notificado ya no cumple los requisitos establecidos en el artículo 31 o no está cumpliendo sus obligaciones, dicha autoridad limitará, suspenderá o retirará la designación, según el caso, dependiendo de la gravedad del incumplimiento de dichos requisitos u obligaciones. Asimismo, informará de ello inmediatamente a la Comisión y a los demás Estados miembros.

5. Cuando su designación haya sido suspendida, limitada o retirada total o parcialmente, el organismo notificado informará a los proveedores afectados a más en un plazo de diez días.

6. En caso de la limitación, suspensión o retirada de una designación, la autoridad notificante adoptará las medidas oportunas para garantizar que los archivos del organismo notificado de que se trate se conserven, y para ponerlos a disposición de las autoridades notificantes de otros Estados miembros y de las autoridades de vigilancia del mercado, a petición de estas.

7. En caso de la limitación, suspensión o retirada de una designación, la autoridad notificante:

a) evaluará las repercusiones en los certificados expedidos por el organismo notificado;

presentará a la Comisión y a los demás Estados miembros un informe con sus conclusiones en un plazo de tres meses a partir de la notificación de los cambios en la designación;

exigirá al organismo notificado que suspenda o retire, en un plazo razonable determinado por la autoridad, todo certificado indebidamente expedido, a fin de garantizar

organismo jakinarazi batek idatziz baieztatu badu bere gain hartuko duela ziurtagiri horiek estaltzen dituzten arrisku handiko AA-sistemen erantzukizuna. Azken organismo jakinarazi horrek, bederatzi hilabeteko epe hori amaitu aurretik eta sistema horietarako ziurtagiri berriak eman baino lehen, ebaluazio oso bat egingo du ukitutako arrisku handiko AA-sistemei buruz. Organismo jakinaraziak bere jarduerak amaitu baditu, agintaritza jakinarazleak izendapena kenduko dio.

4. Agintaritza jakinarazle batek arrazoi nahikoa badu pentsatzeko organismo jakinarazi batek jada ez dituela betetzen 31. artikuluan ezarritako betekizunak edo ez dituela bere betebeharrak betetzen, agintaritza jakinarazleak atzerapenik gabe eta ahalik eta arreta handienaz ikertuko du gaia. Testuingurua hori dela, agertutako eragozpenen berri emango dio ukitutako organismo jakinaraziari, eta haren ikuspuntuak azaltzeko aukera emango dio. Agintaritza jakinarazleak ondorioztatzen badu organismo jakinaraziak jada ez dituela betetzen 31. artikuluan ezarritako betekizunak edo ez dituela bere betebeharrak betetzen, izendapena mugatu, eten edo kendu egingo du agintaritza horrek, dagokionaren arabera, betekizun edo betebeharrak bete ez izanak zenbateko larritasuna duen kontuan hartuta. Era berean, berehala emango die horren berri Batzordeari eta gainerako estatu kideei.

5. Izendapena eten, mugatu edo kendu bada —erabat edo partzialki—, organismo jakinaraziak gehienez hamar eguneko epean jakinaraziko die ukitutako hornitzaileei.

6. Izendapen bat mugatu, eten edo kentzen bada, agintaritza jakinarazleak neurri egokiak hartuko ditu organismo jakinaraziaren artxiboak gordetzen direla bermatzeko, eta beste estatu kide batzuetako agintaritza jakinarazleen eta merkatua zaintzeko agintaritzen eskura jartzeko, hala eskatzen badute.

7. Izendapen bat mugatu, eten edo kentzen bada, zeregin hauek egingo ditu agintaritza jakinarazleak:

a) Organismo jakinaraziek emandako ziurtagirietan izango dituen ondorioak ebaluatu.

Bere ondorioak azaltzen dituen txosten bat aurkeztu Batzordeari eta gainerako estatu kideei, izendapenean egindako aldaketak jakinarazi eta hiru hilabeteko epean.

Behar ez bezala emandako ziurtagiri guztiak agintaritzak zehaztutako arrazoizko epe batean eten edo ken ditzala eskatu organismo jakinaraziari, merkatuan dauden



la conformidad continua de los sistemas de IA de alto riesgo en el mercado;

informará a la Comisión y a los Estados miembros de los certificados cuya suspensión o retirada haya exigido;

facilitará a las autoridades nacionales competentes del Estado miembro en el que el proveedor tenga su domicilio social toda la información pertinente sobre los certificados cuya suspensión o retirada haya exigido; dicha autoridad tomará las medidas oportunas, cuando sea necesario, para evitar un riesgo para la salud, la seguridad o los derechos fundamentales.

8. Salvo en el caso de los certificados expedidos indebidamente, y cuando una designación haya sido suspendida o limitada, los certificados mantendrán su validez en una de las circunstancias siguientes:

a) cuando, en el plazo de un mes a partir de la suspensión o la limitación, la autoridad notificante haya confirmado que no existe riesgo alguno para la salud, la seguridad o los derechos fundamentales en relación con los certificados afectados por la suspensión o la limitación y haya fijado un calendario de acciones para subsanar la suspensión o la limitación, o

cuando la autoridad notificante haya confirmado que no se expedirán, modificarán ni volverán a expedir certificados relacionados con la suspensión mientras dure la suspensión o limitación, y declare si el organismo notificado tiene o no la capacidad, durante el período de la suspensión o limitación, de seguir supervisando los certificados expedidos y siendo responsable de ellos; cuando la autoridad notificante determine que el organismo notificado no tiene la capacidad de respaldar los certificados expedidos, el proveedor del sistema cubierto por el certificado deberá confirmar por escrito a las autoridades nacionales competentes del Estado miembro en que tenga su domicilio social, en un plazo de tres meses a partir de la suspensión o limitación, que otro organismo notificado cualificado va a asumir temporalmente las funciones del organismo notificado para supervisar los certificados y ser responsable de ellos durante el período de la suspensión o limitación.

9. Salvo en el caso de los certificados expedidos indebidamente, y cuando se haya retirado una designación, los certificados mantendrán su validez durante nueve meses en las circunstancias siguientes:

a) la autoridad nacional competente del Estado miembro en el que tiene su domicilio social el proveedor del sistema de IA de alto riesgo cubierto por el certificado ha confirmado que no existe ningún riesgo para la salud, la seguridad o los derechos

arrisku handiko AA-sistemek etengabeko adostasuna dutela bermatzeko.

Zer ziurtagiri eten edo kentzeko eskatu duen jakinarazi Batzordeari eta estatu kideei.

Eteteko edo kentzeko eskatu dituen ziurtagiriei buruz beharrezko den informazio guztia eman hornitzaileak egoitza soziala duen estatu kideko agintaritza nazional eskudunei; agintaritza horrek neurri egokiak hartuko ditu, beharrezkoa denean, osasunerako, segurtasunerako edo oinarritzko eskubideetarako arriskurik egon ez dadin.

8. Behar ez bezala emandako ziurtagirien kasuan izan ezik, eta izendapen bat eten edo mugatu denean, ziurtagiriek baliozkoak izaten jarraituko dute egoera hauetakoren bat betetzen denean:

a) izendapena eten edo mugatu eta hilabeteko epean, agintaritza jakinarazleak berretsi duenean, eteteak edo mugatzeak ukitutako ziurtagiriei dagokienez, ez dagoela inolako arriskurik osasunerako, segurtasunerako edo oinarritzko eskubideetarako, eta ekintzen egutegi bat ezarri duenean etetea edo mugatzea zuzentzeko; edo

agintaritza jakinarazleak berretsi duenean etetearekin edo mugatzearekin zerikusia duten ziurtagiriak ez direla egingo, aldatuko edo berriro egingo etenak edo mugak irauten duen bitartean, eta deklaratzan duenean organismo jakinaraziak ahalmena duen ala ez, etenak edo mugak irauten duen bitartean, emandako ziurtagiriak gainbegiratzan jarraitzeko, eta horien erantzule izateko; agintaritza jakinarazleak erabakitzen duenean organismo jakinaraziak ez duela gaitasunik emandako ziurtagiriak babesteko, ziurtagiriak babesten duen sistemaren hornitzaileak idatziz egiaztatu beharko die egoitza soziala duen estatu kideko agintaritza nazional eskudunei, etena edo muga hasi eta hiru hilabeteko epean, beste organismo jakinarazi kualifikatu batek hartuko dituela bere gain, aldi baterako, ziurtagiriak gainbegiratzeko organismo jakinaraziaren eginkizunak, eta haien erantzule izango dela etenak edo mugak irauten duen bitartean.

9. Behar ez bezala emandako ziurtagirien kasuan izan ezik, eta izendapen bat kendu denean, ziurtagiriek baliozkoak izaten jarraituko dute, bederatzirako hilabetez, egoera hauetakoren bat betetzen denean:

a) ziurtagiriak babestutako arrisku handiko AA-sistemaren hornitzaileak egoitza soziala zer estatu kidean duen, estatu horretako agintaritza nazional eskudunak baieztatu badu, arrisku handiko AA-sistemari



fundamentales asociado al sistema de IA de alto riesgo de que se trate, y

otro organismo notificado ha confirmado por escrito que asumirá la responsabilidad inmediata de dichos sistemas de IA y completa su evaluación en el plazo de doce meses a partir de la retirada de la designación.

En las circunstancias a que se refiere el párrafo primero, la autoridad nacional competente del Estado miembro en el que tenga su domicilio social el proveedor del sistema cubierto por el certificado podrá prorrogar la validez provisional de los certificados por plazos adicionales de tres meses, sin exceder de doce meses en total.

La autoridad nacional competente o el organismo notificado que asuman las funciones del organismo notificado afectado por el cambio de la designación informarán de ello inmediatamente a la Comisión, a los demás Estados miembros y a los demás organismos notificados.

Artículo 37.– Cuestionamiento de la competencia de los organismos notificados

1. La Comisión investigará, cuando sea necesario, todos los casos en los que existan razones para dudar de la competencia de un organismo notificado o del cumplimiento continuo, por parte de un organismo notificado, de los requisitos establecidos en el artículo 31 y de sus responsabilidades aplicables.
2. La autoridad notificante facilitará a la Comisión, a petición de esta, toda la información pertinente relativa a la notificación o el mantenimiento de la competencia del organismo notificado de que se trate.
3. La Comisión garantizará el tratamiento confidencial de acuerdo con el artículo 78 de toda la información delicada recabada en el transcurso de sus investigaciones en virtud del presente artículo.
4. Cuando la Comisión determine que un organismo notificado no cumple o ha dejado de cumplir los requisitos para su notificación, informará al Estado miembro notificante en consecuencia y le solicitará que adopte las medidas correctoras necesarias, incluidas la suspensión o la retirada de la designación en caso necesario. Si el Estado miembro no adopta las medidas correctoras necesarias, la Comisión, mediante un acto de ejecución, podrá suspender, limitar o retirar la designación. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

dagokionez, ez dagoela inolako arriskurik osasunerako, segurtasunerako edo oinarritzko eskubideetarako, eta

beste organismo jakinarazi batek idatziz baieztatu badu bere gain hartuko duela AA-sistema horien berehalako erantzukizuna, eta izendapena kendu eta hamabi hilabeteko epean osatzen badu bere ebaluazioa.

Lehenengo paragrafoan aipatzen diren egoeretan, ziurtagiriak babestutako sistemaren hornitzaileak egoitza soziala zer estatu kidetan duen, estatu horretako agintaritza nazional eskudunak hiru hilabeteko luzapen gehigarriak eman ahal izango ditu ziurtagiriak behin-behineko baliozkoak izateko, guztira hamabi hilabeteko epea gainditu gabe.

Izendapena aldatzeak ukitutako organismo jakinaraziaren eginkizunak bere gain hartzen dituen organismo jakinaraziak edo agintaritza nazional eskudunak berehala emango die horren berri Batzordeari, gainerako estatu kideei eta gainerako organismo jakinaraziei.

37. artikulua.– Organismo jakinarazien eskumena zalantzan jartzea

1. Beharrezkoa denean, arrazoiren bat badago pentsatzeko organismo jakinarazi batek ez duela behar besteko eskumenik edo organismo jakinarazi batek etengabe ez dituela betetzen 31. artikuluan ezarritako betekizunak eta aplikatu behar zaizkion erantzukizunak, kasu guztiak ikertuko ditu Batzordeak.
2. Agintaritza jakinarazleak, Batzordeak eskatuz gero, jakinarazpenari edo organismo jakinaraziaren eskumena mantentzeko buruz beharrezko den informazio guztia emango dio Batzordeari.
3. Batzordeak berrmatuko du artikulua honen arabera ikerketetan bildu den eta bereziki babestu behar den informazio guztia konfidentzialtasunez tratatuko dela, 78. artikuluaaren arabera.
4. Batzordeak erabakitzen badu organismo jakinarazi batek ez dituela betetzen jakinarazpena jasotzeko betekizunak, edo betekizun horiek betetzeari utzi diola, horren berri emango dio estatu kide jakinarazleari, eta behar diren neurri zuzentzaileak hartzeko eskatuko dio, baita izendapena eteteko edo kentzeko ere, beharrezkoa izanez gero. Baldin eta estatu kideak ez baditu hartzen behar diren neurri zuzentzaileak, Batzordeak, betearazpen-egintza baten bidez, izendapena eten, mugatu edo kendu ahal izango du. Betearazpen-egintza hori 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko da.



Artículo 38.— Coordinación de los organismos notificados

1. La Comisión se asegurará de que se instaure y se mantenga convenientemente, en relación con los sistemas de IA de alto riesgo, una adecuada coordinación y cooperación entre los organismos notificados activos en los procedimientos de evaluación de la conformidad en virtud del presente Reglamento, en forma de grupo sectorial de organismos notificados.
2. Cada autoridad notificante se asegurará de que los organismos notificados por ella participen en el trabajo del grupo a que se refiere el apartado 1, directamente o por medio de representantes designados.
3. La Comisión dispondrá que se organicen intercambios de conocimientos y mejores prácticas entre autoridades notificantes.

Artículo 39.— Organismos de evaluación de la conformidad de terceros países

Los organismos de evaluación de la conformidad establecidos en virtud del Derecho de un tercer país con el que la Unión haya celebrado un acuerdo podrán ser autorizados a desempeñar las actividades de los organismos notificados con arreglo al presente Reglamento, siempre que cumplan los requisitos establecidos en el artículo 31 o garanticen un nivel equivalente de cumplimiento.

SECCIÓN 5

Normas, evaluación de la conformidad, certificados, registro

Artículo 40.— Normas armonizadas y documentos de normalización

1. Los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con normas armonizadas, o partes de estas, cuyas referencias estén publicadas en el Diario Oficial de la Unión Europea de conformidad con el Reglamento (UE) n.º 1025/2012 se presumirá que son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, en su caso, con las obligaciones establecidas en el capítulo V, secciones 2 y 3, del presente Reglamento, en la medida en que dichas normas contemplen estos requisitos u obligaciones.
2. De conformidad con el artículo 10 del Reglamento (UE) n.º 1025/2012, la Comisión formulará, sin demora indebida, peticiones de normalización que contemplen todos los requisitos establecidos en la sección 2 del presente capítulo y, según proceda, las peticiones de normalización que contemplen las obligaciones establecidas en el capítulo V, secciones 2 y 3, del

38. artikulua.— Organismo jakinarazien arteko koordinazioa

1. Arrisku handiko AA-sistemei dagokienez, Batzordeak ziurtatuko du koordinazio eta lankidetzaren egokia ezartzen eta behar bezala mantentzen dela, erregelamendu honi jarraikiz adostasuna ebaluatzen prozeduretan aktibo dauden organismo jakinarazien artean, organismo jakinarazien talde sektoriala osatuta.
2. Agintaritza jakinarazle bakoitzak ziurtatuko du berak jakinarazitako organismoek zuzenean edo ordezkari izendatuen bidez hartzen dutela parte 1. apartatuan aipatutako taldearen lanean.
3. Batzordeak erraztu egingo du agintaritza jakinarazleen artean ezagutzak eta jardunbide egokiak trukatu daitezela.

39. artikulua.— Hirugarren herrialdeetako adostasuna ebaluatzeneko organismoak

Batasunarekin akordio bat sinatu duen hirugarren herrialde bateko zuzenbideari jarraikiz ezarri diren adostasuna ebaluatzeneko organismo baimena eman ahal izango zaie erregelamendu honen arabera jakinarazitako organismoen jarduerak egiteko, betiere 31. artikuluan ezarritako betekizunak betetzen badituzte edo betetze-maila baliokidea bermatzen badute.

5. ATALA

Arauak, adostasuna ebaluatzea, ziurtagiriak, erregistroa

40. artikulua.— Arau harmonizatuak eta normalizazio-dokumentuak

1. Arrisku handiko AA-sistemak edo erabilera orokorreko AA-ereduak, arau harmonizatuarekin edo horien zatiekin bat badatoz —haien erreferentziak Europar Batasunaren Aldizkari Ofizialean argitaratuta daudela, (EB) 1025/2012 Erregelamenduaren arabera—, ulertuko da bat datozela kapitulu honetako 2. atalean ezarritako betekizunekin edo, hala badagokio, erregelamendu honen V. kapituluko 2. eta 3. atalean ezarritako betebeharrekin, arau horiek betekizun edo betebeharrak jasotzen dituzten heinean.
2. (EB) 1025/2012 Erregelamenduaren 10. artikuluekin bat etorriz, Batzordeak, bidegabeko atzerapenik gabe, kapitulu honetako 2. atalean ezarritako betekizun guztiak jasotzen dituzten normalizazio-eskaerak egingo ditu, bai eta, hala badagokio, erregelamendu honen V. kapituluko 2. eta 3. atalean ezarritako betebeharrak jasotzen dituzten



presente Reglamento. La petición de normalización también incluirá la solicitud de documentos sobre los procesos de presentación de información y documentación a fin de mejorar el funcionamiento de los sistemas de IA desde el punto de vista de los recursos, como la reducción del consumo de energía y de otros recursos del sistema de IA de alto riesgo durante su ciclo de vida, así como sobre el desarrollo eficiente desde el punto de vista energético de los modelos de IA de uso general. Cuando prepare una petición de normalización, la Comisión consultará al Consejo de IA y a las partes interesadas pertinentes, incluido el foro consultivo.

Cuando dirija una petición de normalización a las organizaciones europeas de normalización, la Comisión especificará que las normas deben ser claras, coherentes —también con las normas elaboradas en diversos sectores para los productos regulados por los actos legislativos de armonización de la Unión vigentes enumerados en el anexo I— y destinadas a garantizar que los sistemas de IA de alto riesgo o los modelos de IA de uso general introducidos en el mercado o puestos en servicio en la Unión cumplan los requisitos u obligaciones pertinentes establecidos en el presente Reglamento.

La Comisión solicitará a las organizaciones europeas de normalización que aporten pruebas de que han hecho todo lo posible por cumplir los objetivos a que se refieren los párrafos primero y segundo del presente apartado, de conformidad con el artículo 24 del Reglamento (UE) n.o 1025/2012.

3. Los participantes en el proceso de normalización tratarán de promover la inversión y la innovación en IA, también incrementando la seguridad jurídica, así como la competitividad y el crecimiento del mercado de la Unión, de contribuir al refuerzo de la cooperación mundial en pro de la normalización, teniendo en cuenta las normas internacionales existentes en el ámbito de la IA que son coherentes con los valores, derechos fundamentales e intereses de la Unión, y de mejorar la gobernanza multilateral, garantizando una representación equilibrada de los intereses y la participación efectiva de todas las partes interesadas pertinentes de conformidad con los artículos 5, 6 y 7 del Reglamento (UE) n.o 1025/2012.

Artículo 41.— Especificaciones comunes

1. La Comisión podrá adoptar actos de ejecución por los que se establezcan especificaciones comunes para los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, siempre que se hayan cumplido las siguientes condiciones:

normalizazio-eskaerak ere. Normalizazio-eskaeran, halaber, informazioa eta dokumentazioa aurkezteko prozesuei buruzko dokumentu-eskaera ere sartuko da, AA-sistemen funtzionamendua hobetzeko baliabideen ikuspegitik, hala nola arrisku handiko AA-sistemaren energia-kontsumoa eta beste baliabide batzuen kontsumoa murrizteko haren bizi-zikloan; halaber, erabilera orokorreko AA-ereduek energiaren ikuspegitik izan duten garapen eraginkorrari buruzko dokumentazioa ere aurkeztuko da. Normalizazio-eskaera bat prestatzen duenean, Batzordeak kontsulta egingo die AA-kontseiluari eta dagozkion alderdi interesdunei, kontsulta-foroa barne.

Normalizazio-eskaera Europako normalizazio-antolakundeentzat denean, Batzordeak zehaztuko du arauak argiak izan behar dutela, eta koherenteak —baita I. eranskinean zerrendatu diren Batasunaren harmonizazioko lege-egintzek araututako produktueterako hainbat sektoretan egindako arauekin ere—, eta bermatu behar dutela Batasunean merkatuan jarri edo zerbitzuan ipini diren arrisku handiko AA-sistemek edo erabilera orokorreko AA-ereduek erregelamendu honetan ezarritako betekizun edo betebeharrak betetzen dituztela.

Batzordeak frogak eskatuko dizkie Europako normalizazio-antolakundeei, apartatu honetako lehenengo eta bigarren paragrafoetan aipatzen diren helburuak betetzeko ahal izan duten guztia egin dutela frogatzeko, (EB) 1025/2012 Erregelamenduaren 24. artikulua arabera.

3. Normalizazio-prozesuan parte hartzen dutenek helburu izango dute AAn inbertsioa eta berrikuntza sustatzea, besteak beste ziurtasun juridikoa hobetuz, baita Batasuneko merkatuaren lehiakortasuna eta hazkundera ere; halaber, helburu hartuko dute normalizazioaren aldeko mundu-mailako lankidetzaren indartzea, AAren esparruan dauden nazioarteko arauak kontuan hartuta —zeinak koherenteak baitira Batasunaren balio, oinarritzko eskubide eta interesekin—, eta gobernantza multilateral hobetzea, interesen ordezkaritza orekatua eta interesdun guztien parte-hartze eraginkorra bermatuz, (EB) 1025/2012 Erregelamenduaren 5., 6. eta 7. artikuluekin bat etorritik.

41. artikulua.— Zehaztapen komunak

1. Batzordeak betearazpen-egintzak hartu ahal izango ditu zehaztapen komunak ezartzeko kapitulu honetako 2. atalean ezarritako betekizunetarako edo, dagokionaren arabera, V. kapituluko 2. eta 3. ataletan ezarritako betebeharrarako, betiere baldintza hauek bete badira:



a) la Comisión ha solicitado, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, a una o varias organizaciones europeas de normalización que elaboren una norma armonizada para los requisitos establecidos en la sección 2 del presente capítulo, o según corresponda, para las obligaciones establecidas en el capítulo V, secciones 2 y 3, y:

i) la solicitud no ha sido aceptada por ninguna de las organizaciones europeas de normalización, o

ii) las normas armonizadas que responden a dicha solicitud no se han entregado en el plazo establecido de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, o

iii) las normas armonizadas pertinentes responden de forma insuficiente a las preocupaciones en materia de derechos fundamentales, o

iv) las normas armonizadas no se ajustan a la solicitud, y

no se ha publicado en el Diario Oficial de la Unión Europea ninguna referencia a normas armonizadas que regulen los requisitos establecidos en la sección 2 del presente capítulo, o según proceda, las obligaciones a que se refiere el capítulo V, secciones 2 y 3, de conformidad con el Reglamento (UE) n.º 1025/2012 y no se prevé la publicación de tal referencia en un plazo razonable.

Al elaborar las disposiciones comunes, la Comisión consultará al foro consultivo a que se refiere el artículo 67.

Los actos de ejecución a que se refiere el párrafo primero del presente apartado se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 98, apartado 2.

2. Antes de elaborar un proyecto de acto de ejecución, la Comisión informará al comité a que se refiere el artículo 22 del Reglamento (UE) n.º 1025/2012 de que considera que se cumplen las condiciones establecidas en el apartado 1 del presente artículo.

3. Se presumirá que los sistemas de IA de alto riesgo o los modelos de IA de uso general que sean conformes con las especificaciones comunes a que se refiere el apartado 1, o partes de dichas especificaciones, son conformes con los requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, para cumplir con las obligaciones a que se refiere el capítulo V, secciones 2 y 3, en la medida en que dichas especificaciones comunes contemplen esos requisitos o esas obligaciones.

a) (EB) 1025/2012 Erregelamenduaren 10.1 artikularekin bat etorri, Batzordeak Europako normalizazio-antolakunde bati edo batzuei eskatu die arau harmonizatu bat egin dezatela kapitulu honetako 2. atalean ezarritako betekizunetarako, edo, dagokionaren arabera, V. kapituluko 2. eta 3. ataletan ezarritako betebeharrarako, eta:

i) Europako normalizazio-antolakunde batek ere ez du onartu eskaera, edo

ii) eskaera horri erantzuten dioten arau harmonizatuak ez dira aurkeztu (EB) 1025/2012 Erregelamenduaren 10.1 artikularen arabera ezarritako epean, edo

iii) arau harmonizatuak ez diete behar bezala erantzuten oinarritzko eskubideen arloko kezkei, edo

iv) arau harmonizatuak ez datoz bat eskaerarekin, eta

Europar Batasunaren Aldizkari Ofizialean ez da erreferentziarik argitaratu kapitulu honetako 2. atalean ezarritako betekizunak, edo, dagokionaren arabera, (EB) 1025/2012 Erregelamenduaren arabera V. kapituluko 2. eta 3. ataletan ezarritako betebeharrak arautzen dituzten arau harmonizatuak buruz, eta ez da aurreikusten halako erreferentziarik argitaratuko denik arrazoizko epe batean.

Zehaztapen komunak egitean, Batzordeak kontsulta egingo dio 67. artikuluan aipatzen den kontsulta-foroari.

Apartatu honetako lehenengo paragrafoak aipatzen dituen betearazpen-egintza horiek 98.2 artikuluan azaltzen den azterketa-prozedurari jarraituz hartuko dira.

2. Betearazpen-egintzaren proiektu bat egin aurretik, artikuluko honen 1. apartatuan ezarritako baldintzak betetzen direla uste duela jakinaraziko dio Batzordeak (EB) 1025/2012 Erregelamenduaren 22. artikuluan aipatzen den komiteari.

3. Baldin eta arrisku handiko AA-sistemak edo erabilera orokorreko AA-ereduak bat badatoz 1. apartatuan aipatzen diren zehaztapen komunekin edo zehaztapen horien zatiekin, ulertuko da bat datozela kapitulu honetako 2. atalean ezarritako betekizunekin edo, dagokionaren arabera, erregelamendu honen V. kapituluko 2. eta 3. ataletan ezarritako betebeharrekin, zehaztapen komun horiek betekizun edo betebeharrak jasotzen dituzten heinean.



4. Cuando una norma armonizada sea adoptada por una organización europea de normalización y propuesta a la Comisión con el fin de publicar su referencia en el Diario Oficial de la Unión Europea, la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n.º 1025/2012. Cuando la referencia a una norma armonizada se publique en el Diario Oficial de la Unión Europea, la Comisión derogará los actos de ejecución a que se refiere el apartado 1, o las partes de dichos actos que contemplen los mismos requisitos establecidos en la sección 2 del presente capítulo o, según corresponda, las mismas obligaciones establecidas en el capítulo V, secciones 2 y 3.

5. Cuando los proveedores de sistemas de IA de alto riesgo o los modelos de IA de uso general no cumplan las especificaciones comunes mencionadas en el apartado 1, justificarán debidamente que han adoptado soluciones técnicas que cumplan los requisitos a que se refiere la sección 2 del presente capítulo o, según corresponda, cumplan con las obligaciones establecidas en el capítulo V, secciones 2 y 3, en un nivel como mínimo equivalente a aquellos.

6. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en la sección 2, o, según corresponda, no cumple con las obligaciones establecidas en el capítulo V, secciones 2 y 3, informará de ello a la Comisión con una explicación detallada. La Comisión evaluará dicha información y, en su caso, modificará el acto de ejecución por el que se establece la especificación común de que se trate.

Artículo 42.— Presunción de conformidad con determinados requisitos

1. Se presumirá que los sistemas de IA de alto riesgo que hayan sido entrenados y probados con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto su uso cumplen los requisitos pertinentes establecidos en el artículo 10, apartado 4.

2. Se presumirá que los sistemas de IA de alto riesgo que cuenten con un certificado o una declaración de conformidad en virtud de un esquema de ciberseguridad con arreglo al Reglamento (UE) 2019/881 cuyas referencias estén publicadas en el Diario Oficial de la Unión Europea cumplen los requisitos de ciberseguridad establecidos en el artículo 15 del presente Reglamento en la medida en que el certificado de ciberseguridad o la declaración de conformidad, o partes de estos, contemplen dichos requisitos.

Artículo 43.— Evaluación de la conformidad

4. Europako normalizazio-antolakunde batek arau harmonizatu bat onartzen duenean eta Batzordeari proposatzen zaionean haren erreferentzia Europar Batasunaren Aldizkari Ofizialean argitaratzeko, Batzordeak arau harmonizatua ebaluatuko du (EB) 1025/2012 Erregelamenduaren arabera. Arau harmonizatu baten erreferentzia Europar Batasunaren Aldizkari Ofizialean argitaratzen denean, Batzordeak indargabetu egingo ditu 1. apartatuan aipatzen diren betearazpen-egintzak, edo egintza horien zatiak, baldin eta kapitulu honetako 2. atalean ezarritako betekizun berberak edo, dagokionaren arabera, V. kapituluko 2. eta 3. ataletan ezarritako betebeharrak berberak jasotzen badituzte.

5. Arrisku handiko AA-sistemek edo erabilera orokorreko AA-ereduek ez badituzte betetzen 1. apartatuan aipatzen diren zehaztapen komunak, behar bezala justifikatu beharko dute kapitulu honetako 2. atalean ezarritako betekizunak edo, dagokionaren arabera, V. kapituluko 2. eta 3. ataletan ezarritako betebeharrak betetzen dituzten soluzio teknikoak hartu dituztela, gutxienez zehaztapen horien maila baliokidean.

6. Estatu kide batek uste badu zehaztapen komun batek ez dituela guztiz betetzen 2. atalean ezarritako betekizunak edo, dagokionaren arabera, ez dituela betetzen V. kapituluko 2. eta 3. ataletan ezarritako betebeharrak, horren berri emango dio Batzordeari, azalpen zehatzak emanda. Batzordeak informazio hori ebaluatuko du, eta, hala badagokio, dagokion zehaztapen komuna ezartzen duen betearazpen-egintza aldatuko du.

42. artikulua.— Betekizun jakin batzuekiko adostasun-presuntzioa

1. Arrisku handiko AA-sistemak zer ingurunetan erabiltzea aurreikusten den, ingurune geografiko, konduktual, kontestual edo funtzional horixe islatzeko datuekin entrenatuta eta probatuta badaude, ulertuko da AA-sistema horiek bete egiten dituztela 10.4 artikuluan ezarritako betekizunak.

2. Baldin eta arrisku handiko AA-sistemek ziurtagiri edo adostasun-adierazpen bat badute —2019/881 (EB) Erregelamenduaren arabera zibersegurtasun-eskema bati jarraikiz— eta haien erreferentziak Europar Batasunaren Aldizkari Ofizialean argitaratu badira, ulertuko da bete egiten dituztela erregelamendu honen 15. artikuluan ezarritako zibersegurtasun-betekizunak, betekizun horiek zibersegurtasun-ziurtagirian edo adostasun-adierazpenean —edo haien zati batzuetan— jasota dauden heinean.

43. artikulua.— Adostasuna ebaluatzea



1. En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, punto 1, cuando, al demostrar el cumplimiento de los requisitos establecidos en la sección 2 por parte de un sistema de IA de alto riesgo, el proveedor haya aplicado las normas armonizadas a que se refiere el artículo 40, o bien, en su caso, las especificaciones comunes a que se refiere el artículo 41, el proveedor optará por uno de los procedimientos de evaluación de la conformidad siguientes:

a) el fundamentado en el control interno, mencionado en el anexo VI, o

el fundamentado en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica, con la participación de un organismo notificado, mencionado en el anexo VII.

Al demostrar el cumplimiento de los requisitos establecidos en la sección 2 por parte de un sistema de IA de alto riesgo, el proveedor se atenderá al procedimiento de evaluación de la conformidad establecido en el anexo VII cuando:

a) las normas armonizadas a que se refiere el artículo 40 no existan, y no se disponga de las especificaciones comunes a que se refiere el artículo 41;

el proveedor no haya aplicado la norma armonizada, o solo haya aplicado parte de esta;

existan las especificaciones comunes a que se refiere la letra a), pero el proveedor no las haya aplicado;

una o varias de las normas armonizadas a que se refiere la letra a) se hayan publicado con una limitación, y únicamente en la parte de la norma objeto de la limitación.

A efectos del procedimiento de evaluación de la conformidad mencionado en el anexo VII, el proveedor podrá escoger cualquiera de los organismos notificados. No obstante, cuando se prevea la puesta en servicio del sistema de IA de alto riesgo por parte de las autoridades garantes del cumplimiento del Derecho, las autoridades de inmigración o las autoridades de asilo, o por las instituciones, órganos u organismos de la Unión, la autoridad de vigilancia del mercado mencionada en el artículo 74, apartado 8 o 9, según proceda, actuará como organismo notificado.

2. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, los proveedores se atenderán al procedimiento de evaluación de la conformidad fundamentado en un

1. Erregelamendu honen III. eranskineko 1. puntuan zerrendatuta dauden arrisku handiko AA-sistemen kasuan, baldin eta hornitzaileak, arrisku handiko AA-sistema batek 2. atalean ezarritako betekizunak betetzen dituela egiaztatzean, 40. artikuluan aipatzen diren arau harmonizatuak edo, hala badagokio, 41. artikuluan aipatzen diren zehaztapen komunak aplikatu baditu, adostasuna ebaluatzen prozedura hauetako bat aukeratuko du hornitzaileak:

a) barne-kontrolen oinarritutakoa —VI. eranskinean dago aipatuta—, edo

kalitatea kudeatzeko sistemaren ebaluazioan eta dokumentazio teknikoaren ebaluazioan oinarritutakoa, organismo jakinarazi baten parte-hartzearekin —VII. eranskinean dago aipatuta—.

Arrisku handiko AA-sistema batek 2. atalean ezarritako betekizunak betetzen dituela egiaztatzean, kasu hauetan beteko du hornitzaileak VII. eranskinean ezarritako adostasuna ebaluatzen prozedura:

a) Erregelamendu honen 40. artikuluan aipatzen diren arau harmonizatuak eta 41. artikuluan aipatzen diren zehaztapen komunak ez daudenean;

hornitzaileak ez duenean aplikatu arau harmonizatua, edo arauaren zati bat baino ez duenean aplikatu;

nahiz eta a) letran aipatzen diren zehaztapen komunak egon, hornitzaileak aplikatu ez dituzten;

aurreko a) letran aipatzen diren arau harmonizatuetako bat edo batzuk mugaren batekin argitaratu direnean, eta mugaren xede izan den arauaren zatian bakarrik.

Erregelamendu honen VII. eranskinean aipatutako adostasuna ebaluatzen prozeduraren ondorioetarako, edozein organismo jakinarazi aukeratu ahal izango du hornitzaileak. Hala ere, aurreikusten denean zuzenbidea betearazteko agintaritzek, immigrazio-agintaritzek edo asilo-agintaritzek edo Batasuneko instituzio, organo edo organismoek ipiniko dutela zerbitzuan arrisku handiko AA-sistema, organismo jakinarazi gisa jardungo du 74. artikuluan —dagokionaren arabera, 8. edo 9. apartatuan— aipatutako merkatua zaintzeko agintaritzak.

2. Erregelamendu honen III. eranskineko 2. puntutik 8.era bitartean aipatutako arrisku handiko AA-sistemen kasuan, VI. eranskinean aipatzen den barne-kontrolen oinarritutako adostasuna ebaluatzen prozedura bete



control interno a que se refiere el anexo VI, que no contempla la participación de un organismo notificado.

3. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, el proveedor se atenderá al procedimiento de evaluación de la conformidad pertinente exigida por dichos actos legislativos. Los requisitos establecidos en la sección 2 del presente capítulo se aplicarán a dichos sistemas de IA de alto riesgo y formarán parte de dicha evaluación. Asimismo, se aplicarán los puntos 4.3, 4.4 y 4.5 del anexo VII, así como el punto 4.6, párrafo quinto, de dicho anexo.

A efectos de dicha evaluación, los organismos notificados que hayan sido notificados con arreglo a dichos actos legislativos dispondrán de la facultad de controlar la conformidad de los sistemas de IA de alto riesgo con los requisitos establecidos en la sección 2, a condición de que se haya evaluado el cumplimiento por parte de dichos organismos notificados de los requisitos establecidos en el artículo 31, apartados 4, 5, 10 y 11, en el contexto del procedimiento de notificación con arreglo a dichos actos legislativos.

Cuando un acto legislativo enumerado en el anexo I, sección A, permita al fabricante del producto prescindir de una evaluación de la conformidad de terceros, a condición de que el fabricante haya aplicado todas las normas armonizadas que contemplan todos los requisitos pertinentes, dicho fabricante solamente podrá recurrir a esta opción si también ha aplicado las normas armonizadas o, en su caso, las especificaciones comunes a que se refiere el artículo 41 que contemplan todos los requisitos establecidos en la sección 2 del presente capítulo.

4. Los sistemas de IA de alto riesgo que ya hayan sido objeto de un procedimiento de evaluación de la conformidad se someterán a un nuevo procedimiento de evaluación de la conformidad en caso de modificación sustancial, con independencia de si está prevista una distribución posterior del sistema modificado o de si este continúa siendo utilizado por el responsable del despliegue actual.

En el caso de los sistemas de IA de alto riesgo que continúen aprendiendo tras su introducción en el mercado o su puesta en servicio, los cambios en el sistema de IA de alto riesgo y su funcionamiento que hayan sido predeterminados por el proveedor en el momento de la evaluación inicial de la conformidad y figuren en la información recogida en la documentación técnica mencionada en el anexo IV, punto 2, letra f), no constituirán modificaciones sustanciales.

beharko dute hornitzaileek, eta hor ez da aurreikusten organismo jakinarazi batek parte-hartzea.

3. Batasunaren harmonizazioko lege-egintzek —I. eranskineko A atalean daude zerrendatuta— araututako arrisku handiko AA-sistemen kasuan, lege-egintza horiek eskatzen duten adostasuna ebaluatzeko prozedura bete beharko du hornitzaileak. Kapitulu honetako 2. atalean ezarritako betekizunak arrisku handiko AA-sistema horiei aplikatuko zaizkie, eta ebaluazio horren parte izango dira. Era berean, VII. eranskineko 4.3, 4.4 eta 4.5 puntuak aplikatuko dira, baita eranskin horretako 4.6 puntuko bosgarren paragrafoa ere.

Ebaluazio horren ondorioetarako, lege-egintza horien arabera jakinarazi diren organismo jakinaraziek ahalmena izango dute arrisku handiko AA-sistemak 2. atalean ezarritako betekizunekin bat datozen kontrolatzeko, baldin eta organismo jakinarazi horiek 31. artikuluko 4., 5., 10. eta 11. apartatuetan ezarritako betekizunak betetzen dituztela ebaluatu bada, lege-egintza horien arabera jakinarazpen-prozeduraren testuinguruan.

Erregelamendu honen I. eranskineko A atalean zerrendatu den lege-egintza batek aukera ematen badio produktuaren fabrikatzaileari alde batera uzteko hirugarrenen adostasunaren ebaluazioa, eta betiere fabrikatzaileak dagozkion betekizun guztiak jasotzen dituzten arau harmonizatu guztiak aplikatu baditu, arau harmonizatuak edo, hala badagokio, kapitulu honetako 2. atalean ezarritako betekizun guztiak jasotzen dituen 41. artikuluan aipatutako zehaztaperen komunak ere aplikatuz gero bakarrik erabili ahal izango du aukera hori fabrikatzaileak.

4. Dagoeneko adostasuna ebaluatzeko prozedura baten xede izan den arrisku handiko AA-sistemaren batek funtsezko aldaketaren bat izan badu, adostasuna ebaluatzeko beste prozedura bat aplikatuko zaio, kontuan hartu gabe ea aldatutako sistemaren ondorengo banaketa bat aurreikusita dagoen edo ea egungo hedapenaren arduradunak jarraitzen duen sistema hori erabiltzen.

Merkatuan jarri edo zerbitzuan ipini ostean ikasten jarraitzen duten arrisku handiko AA-sistemen kasuan, baldin eta hornitzaileak adostasunaren hasierako ebaluazioaren unean aldeztu aurretik zehaztu baditu arrisku handiko AA-sisteman eta haren funtzionamenduan egindako aldaketak, eta baldin eta jasota badaude IV. eranskineko 2. puntuko f) letran aipatutako dokumentazio teknikoan jasotako informazioan, aldaketa horiek ez dira funtsezko aldaketa izango.



5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar los anexos VI y VII actualizándolos a la luz del progreso técnico.

6. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar los apartados 1 y 2 del presente artículo a fin de someter a los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 2 a 8, al procedimiento de evaluación de la conformidad a que se refiere el anexo VII o a partes de este. La Comisión adoptará dichos actos delegados teniendo en cuenta la eficacia del procedimiento de evaluación de la conformidad fundamentado en un control interno mencionado en el anexo VI para prevenir o reducir al mínimo los riesgos para la salud, la seguridad y la protección de los derechos fundamentales que plantean estos sistemas, así como la disponibilidad de capacidades y recursos adecuados por parte de los organismos notificados.

Artículo 44.– Certificados

1. Los certificados expedidos por los organismos notificados con arreglo al anexo VII se redactarán en una lengua que las autoridades pertinentes del Estado miembro en el que esté establecido el organismo notificado puedan entender fácilmente.

2. Los certificados serán válidos para el período que indiquen, que no excederá de cinco años para los sistemas de IA contemplados en el anexo I, y cuatro años para los sistemas de IA contemplados en el anexo III. A solicitud del proveedor, la validez de un certificado podrá prorrogarse por períodos adicionales no superiores a cinco años para los sistemas de IA contemplados en el anexo I, y cuatro años para los sistemas de IA contemplados en el anexo III, sobre la base de una nueva evaluación con arreglo a los procedimientos de evaluación de la conformidad aplicables. Todo suplemento de un certificado mantendrá su validez a condición de que el certificado al que complementa sea válido.

3. Si un organismo notificado observa que un sistema de IA ya no cumple los requisitos establecidos en la sección 2, suspenderá o retirará, teniendo en cuenta el principio de proporcionalidad, el certificado expedido o le impondrá restricciones, a menos que se garantice el cumplimiento de dichos requisitos mediante medidas correctoras adecuadas adoptadas por el proveedor del sistema en un plazo adecuado determinado por el organismo notificado. El organismo notificado motivará su decisión.

5. Batzordeak ahalmena izango du 97. artikulua eraberrako egintza eskuordetuak hartzeko, VI. eta VII. eranskinak aldatu eta aurrerapen teknikoaren arabera eguneratze aldera.

6. Batzordeak ahalmena izango du 97. artikulua eraberrako egintza eskuordetuak hartzeko, artikulua honetako 1. eta 2. apartatuak aldatze aldera, III. eranskineko 2.etik 8.era bitarteko puntuetan aipatutako arrisku handiko AA-sistemak VII. eranskinean aipatzen den adostasuna ebaluatzeko prozeduraren edo horren zati batzuen mende jartzeko. Batzordeak, egintza eskuordetu horiek hartzean, kontuan hartuko du, batetik, ea VI. eranskinean aipatzen den barne-kontrollean oinarritutako adostasuna ebaluatzeko prozedura eraginkorra den prebenitzeko edo ahalik eta gehien murrizteko sistema horiek osasunerako, segurtasunerako eta oinarritzko eskubideen babeserako dakartzaten arriskuak, eta, bestetik, kontuan hartuko du ea organismo jakinaraziek gaitasun eta baliabide egokiak dituzten.

44. artikulua.– Ziurtagiriak

1. Organismo jakinarazia kokatuta dagoen estatu kideko agintaritzek erraz ulertzeko moduko hizkuntza batean idatziko dira organismo jakinaraziek VII. eranskinaren arabera emandako ziurtagiriak.

2. Ziurtagirietan adierazten den aldirako balioko dute ziurtagiriok; aldi hori bost urtekoa izango da, gehienez, I. eranskinean jasotako AA-sistemarako, eta lau urtekoa, gehienez, III. eranskinean jasotako AA-sistemarako. Hornitzaileak hala eskatuz gero, ziurtagiri baten baliozkotasuna beste bost urtez luzatu ahal izango da, gehienez, I. eranskinean jasotako AA-sistemarako, eta beste lau urtez, berriz, III. eranskinean jasotako AA-sistemarako, ebaluazio berri batean oinarrituta, aplikatzekoak diren adostasuna ebaluatzeko prozeduren arabera. Ziurtagiri baten luzapenak baliozkoak izaten jarraitu ahal izateko, ezinbestekoa izango da osatzen duten ziurtagiria baliozkoa izatea.

3. Organismo jakinarazi batek ikusten badu AA-sistema batek jada ez dituela betetzen 2. atalean ezarritako betekizunak, eten edo erretiratu egingo du, proportzionaltasun-printzipioa kontuan hartuta, emandako ziurtagiria, edo murrizketak ezarriko dizkio, non eta ez den bermatzen betekizun horiek betetzen direla organismo jakinaraziak zehaztu duen epe egoki batean sistemaren hornitzaileak hartutako neurri zuzentzaileen bidez. Organismo jakinaraziak bere erabakia arrazoituko du.



Existirá un procedimiento de recurso frente a las decisiones de los organismos notificados, también respecto a los certificados de conformidad expedidos.

Artículo 45.– Obligaciones de información de los organismos notificados

1. Los organismos notificados informarán a la autoridad notificante:

a) de cualquier certificado de la Unión de evaluación de la documentación técnica, de cualquier suplemento a dichos certificados y de cualesquiera aprobaciones de sistemas de gestión de la calidad expedidas con arreglo a los requisitos establecidos en el anexo VII;

de cualquier denegación, restricción, suspensión o retirada de un certificado de la Unión de evaluación de la documentación técnica o de una aprobación de un sistema de gestión de la calidad expedida con arreglo a los requisitos establecidos en el anexo VII;

de cualquier circunstancia que afecte al ámbito de aplicación o a las condiciones de notificación;

de cualquier solicitud de información sobre las actividades de evaluación de la conformidad que hayan recibido de las autoridades de vigilancia del mercado;

previa solicitud, de las actividades de evaluación de la conformidad realizadas dentro del ámbito de aplicación de su notificación y de cualquier otra actividad realizada, incluidas las actividades transfronterizas y las subcontrataciones.

2. Cada organismo notificado informará a los demás organismos notificados:

a) de las aprobaciones de sistemas de gestión de la calidad que haya rechazado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de gestión de la calidad que haya expedido;

de los certificados de la Unión de evaluación de la documentación técnica o los suplementos a dichos certificados que haya rechazado, retirado, suspendido o restringido de cualquier otro modo y, previa solicitud, de los certificados o los suplementos a estos que haya expedido.

3. Cada organismo notificado proporcionará a los demás organismos notificados que realicen actividades de evaluación de la conformidad similares y relativas a los mismos tipos de sistemas de IA información pertinente sobre cuestiones relacionadas con resultados

Organismo jakinarazien erabakien aurkako errekursoak jartzeko prozedura bat egongo da, baita emandako adostasun-ziurtagiriei dagokienez ere.

45. artikulua.– Organismo jakinarazien informatzeko betebeharrak

1. Organismo jakinaraziek alderdi hauen berri emango diote agintaritzak jakinarazleari:

a) dokumentazio teknikoa ebaluatzeko Batasunaren ziurtagiri oro, ziurtagiri horien gehigarri oro eta kalitatea kudeatzeko sistemen onarpen oro, VII. eranskinean ezarritako betekizunen arabera eman badira;

dokumentazio teknikoa ebaluatzeko Batasunaren ziurtagiri bat edo kalitatea kudeatzeko sistema baten onarpena ukatu, murriztu, eten edo erretiratzeko erabaki oro, VII. eranskinean ezarritako betekizunen arabera eman badira;

aplikazio-eremuari edo jakinarazpen-baldintzei eragiten dien inguruabar oro;

adostasuna ebaluatzeko jardueri buruz merkatua zaintzeko agintaritzengandik jasotako informazio-eskaera oro;

aldez aurretik eskatuz gero, bere jakinarazpenaren aplikazio-eremuaren barruan egindako adostasuna ebaluatzeko jardura oro eta egindako beste jardura oro, mugaz gaindiko jarduerak eta azpikontratazioak barne.

2. Organismo jakinarazi bakoitzak egoera hauek jakinaraziko dizkie gainerako organismo jakinaraziei:

a) baztertu, bertan behera utzi edo erretiratu dituen kalitatea kudeatzeko sistemen onarpenak eta, aldez aurretik eskatuz gero, eman dituen kalitatea kudeatzeko sistemen onarpenak;

dokumentazio teknikoa ebaluatzeko Batasunaren ziurtagiriak edo ziurtagiri horien gehigarriak —beste edozein modutan baztertu, bertan behera utzi edo erretiratu dituenak— eta, aldez aurretik eskatuz gero, eman dituen ziurtagiriak edo horien gehigarriak.

3. Organismo jakinarazi bakoitzak, gainera, informazio hau emango die mota bereko AA-sistemei buruzko adostasuna ebaluatzeko antzeko jarduerak egiten dituzten gainerako organismo jakinaraziei: adostasuna ebaluatzean lortutako emaitza negatiboekin zerikusia duten gaiei buruz beharrezko den informazioa eta, aldez



negativos y, previa solicitud, con resultados positivos de las evaluaciones de la conformidad.

4. Los organismos notificados preservarán la confidencialidad de la información obtenida, de conformidad con lo dispuesto en el artículo 78.

Artículo 46.– Exención del procedimiento de evaluación de la conformidad

1. Como excepción a lo dispuesto en el artículo 43 y previa solicitud debidamente motivada, cualquier autoridad de vigilancia del mercado podrá autorizar la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo específicos en el territorio del Estado miembro de que se trate por motivos excepcionales de seguridad pública o con el fin de proteger la vida y la salud de las personas, el medio ambiente o activos fundamentales de la industria y de las infraestructuras. Dicha autorización se concederá por un período limitado, mientras se lleven a cabo los procedimientos de evaluación de la conformidad necesarios, teniendo en cuenta los motivos excepcionales que justifiquen la exención. La conclusión de los procedimientos de que se trate se alcanzará sin demora indebida.

2. En una situación de urgencia debidamente justificada por motivos excepcionales de seguridad pública o en caso de amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas, las autoridades garantes del cumplimiento del Derecho o las autoridades de protección civil podrán poner en servicio un sistema de IA de alto riesgo específico sin la autorización a que se refiere el apartado 1, siempre que se solicite dicha autorización durante o después de la utilización sin demora indebida. Si se deniega la autorización a que se refiere el apartado 1, se suspenderá el uso del sistema de IA de alto riesgo con efecto inmediato y se desecharán inmediatamente todos los resultados y toda la información de salida producidos por dicho uso.

3. La autorización a que se refiere el apartado 1 solo se expedirá si la autoridad de vigilancia del mercado llega a la conclusión de que el sistema de IA de alto riesgo cumple los requisitos establecidos en la sección 2. La autoridad de vigilancia del mercado informará a la Comisión y a los demás Estados miembros de toda autorización expedida de conformidad con los apartados 1 y 2. Esta obligación no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho.

4. Si, en el plazo de quince días naturales tras la recepción de la información indicada en el apartado 3, ningún Estado miembro ni la Comisión presentan objeción alguna sobre una autorización expedida por

aurretik eskatuz gero, emaitza positiboekin zerikusia dutenei buruzkoa.

4. Organismo jakinaraziek lortutako informazioaren konfidentzialtasuna bermatuko dute, 78. artikuluan xedatutakoaren arabera.

46. artikulua.– Adostasuna ebaluatzeko prozeduratik salbuestea

1. Erregelamendu honen 43. artikuluan xedatutakoaren salbuespen gisa, eta behar bezala arrazoituta eskatuz gero, merkatua zaintzeko edozein agintaritzak baimena eman ahal izango du dagokion estatu kidearen lurraldean merkatuan jartzeko edo zerbitzuan ipintzeko arrisku handiko AA-sistema espezifikoak, segurtasun publikoko salbuespenezko arrazoi ondoz edo pertsonen, ingurumenaren edo industriaren eta azpiegituren funtsezko aktiboen bizitza eta osasuna babeste aldera. Baimen hori epe mugatu baterako emango da, adostasuna ebaluatzeko behar diren prozedurak egiten diren bitartean, salbuespena justifikatzen duten salbuespenezko arrazoiak kontuan hartuta. Bidegabeko atzerapenik gabe amaituko dira prozedurak.

2. Segurtasun publikoko salbuespenezko arrazoiak behar bezala justifikatutako urgentzia-egoera batean edo pertsona fisikoen bizitzarako edo segurtasun fisikorako mehatxu espezifiko, garrantzitsu eta berehalakorik egonez gero, zuzenbidea betearazteko agintaritzek edo babes zibileko agintaritzek 1. apartatuan aipatzen den baimenik gabe ipini ahal izango dute zerbitzuan arrisku handiko AA-sistema espezifiko bat, betiere horretarako baimena eskatzen bada erabiltzen den bitartean edo ondoren, bidegabeko atzerapenik gabe. Baldin eta 1. apartatuan aipatutako baimena ukatzen bada, berehala etengo da arrisku handiko AA-sistemaren erabilera, eta berehala baztertuko dira erabilera horrek eragindako emaitza guztiak eta irteera-informazio guztia.

3. Artikulu honen 1. apartatuan aipatzen den baimena soilik emango da baldin eta merkatua zaintzeko agintaritzak ondozotzatzen badu arrisku handiko AA-sistemak bete egiten dituela 2. atalean ezarritako betekizunak. Merkatua zaintzeko agintaritzak 1. eta 2. apartatuei jarraikiz emandako baimen guztien berri emango die Batzordeari eta gainerako estatu kideei. Betebehar horretan ez dira sartuko zuzenbidea betearazteko agintaritzen jarduerari buruzko bereziki babestutako datu operatiboak.

4. Baldin eta, 3. apartatuan adierazitako informazioa jaso eta hamabost egun naturaleko epean, Batzordeak edo estatu kide batek ere ez badu eragozpenik jartzen estatu kide bateko merkatua zaintzeko agintaritzak batek



una autoridad de vigilancia del mercado de un Estado miembro con arreglo al apartado 1, la autorización se considerará justificada.

5. Si, en el plazo de quince días naturales tras la recepción de la notificación a que se refiere el apartado 3, un Estado miembro formula objeciones contra una autorización expedida por una autoridad de vigilancia del mercado de otro Estado miembro, o si la Comisión considera que la autorización vulnera el Derecho de la Unión o que la conclusión de los Estados miembros relativa al cumplimiento del sistema a que se refiere el apartado 3 es infundada, la Comisión celebrará consultas con el Estado miembro pertinente sin demora. Se consultará a los operadores de que se trate y se les ofrecerá la posibilidad de exponer sus puntos de vista. En vista de todo ello, la Comisión decidirá si la autorización está justificada o no. La Comisión enviará su decisión al Estado miembro afectado y a los operadores pertinentes.

6. Si la Comisión considera que la autorización no está justificada, la autoridad de vigilancia del mercado del Estado miembro de que se trate la retirará.

7. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, solo se aplicarán las exenciones de la evaluación de la conformidad establecidas en dichos actos legislativos de armonización de la Unión.

Artículo 47.– Declaración UE de conformidad

1. El proveedor redactará una declaración UE de conformidad por escrito en un formato legible por máquina, con firma electrónica o manuscrita, para cada sistema de IA de alto riesgo y la mantendrá a disposición de las autoridades nacionales competentes durante un período de diez años a contar desde la introducción del sistema de IA de alto riesgo en el mercado o su puesta en servicio. En la declaración UE de conformidad se especificará el sistema de IA de alto riesgo para el que ha sido redactada. Se entregará una copia de la declaración UE de conformidad a las autoridades nacionales competentes pertinentes que lo soliciten.

2. En la declaración UE de conformidad constará que el sistema de IA de alto riesgo de que se trate cumple los requisitos establecidos en la sección 2. La declaración UE de conformidad contendrá la información indicada en el anexo V y se traducirá a una lengua que puedan entender fácilmente las autoridades nacionales competentes del Estado o Estados miembros en que se introduzca en el mercado o comercialice el sistema de IA de alto riesgo.

1. apartatuaren arabera emandako baimen bati buruz, justifikatutzat joko da baimena.

5. Baldin eta, 3. apartatuan aipatutako jakinarazpena jaso eta hamabost egun naturaleko epean, estatu kide batek eragozpenak jartzen baditu beste estatu kide bateko merkatua zaintzeko agintaritza batek emandako baimen baten aurka, edo Batzordeak uste badu baimenak Batasuneko zuzenbidea urratzen duela edo 3. apartatuan aipatutako sistema betetzeari buruz estatu kideek egindako ondorioa funsgabea dela, Batzordeak kontsultak egingo ditu dagokion estatu kidearekin, atzerapenik gabe. Kontsulta egingo zaie dagokien operadoreei, eta haien ikuspuntuak azaltzeko aukera emango zaie. Hori guztia ikusita, Batzordeak erabakiko du ea baimena justifikatuta dagoen ala ez. Ukitutako estatu kideari eta dagozkion operadoreei bidaliko die erabakia Batzordeak.

6. Batzordeak uste badu baimena ez dagoela justifikatuta, dagokion estatu kideko merkatua zaintzeko agintaritzak erretiratu egingo du.

7. Batasunaren harmonizazioko lege-egintzek —I. eranskinen A atalean daude zerrendatuta— araututako produktuei lotutako arrisku handiko AA-sistemen kasuan, Batasunaren harmonizazioko lege-egintza horietan ezarrita dauden adostasuna ebaluatzen salbuespenak baino ez dira aplikatuko.

47. artikulua.– EB adostasun-adierazpena

1. Hornitzaileak EB adostasun-adierazpen bat egingo du, idatziz, makina bidez irakur daitekeen formatu batean, elektronikoki edo eskuz sinatuta, arrisku handiko AA-sistema bakoitzerako, eta agintaritza nazional eskudunen eskura izango du hamar urtez, arrisku handiko AA-sistema merkatuan jartzen edo zerbitzuan ipintzen denetik aurrera. EB adostasun-adierazpenean zehatz adieraziko da arrisku handiko zer AA-sistemarentzat idatzi den. EB adostasun-adierazpenaren kopia bat emango zaie hala eskatzen duten agintaritza nazional eskudunei.

2. EB adostasun-adierazpenean, kasuan kasuko arrisku handiko AA-sistemak 2. atalean ezarritako betekizunak betetzen dituela jasoko da. EB adostasun-adierazpenak V. eranskinean adierazitako informazioa jasoko du. Halaber, arrisku handiko AA-sistema merkaturatzen duen edo merkatuan jartzen duen estatu kideko edo estatu kideetako agintaritza nazional eskudunek erraz ulertzeko moduko hizkuntza batera itzuliko da adierazpena.



3. Cuando los sistemas de IA de alto riesgo estén sujetos a otros actos legislativos de armonización de la Unión que también exijan una declaración UE de conformidad, se elaborará una única declaración UE de conformidad con respecto a todos el Derecho de la Unión aplicable al sistema de IA de alto riesgo. La declaración contendrá toda la información necesaria para determinar los actos legislativos de armonización de la Unión a los que se refiere la declaración.

4. Al elaborar la declaración UE de conformidad, el proveedor asumirá la responsabilidad del cumplimiento de los requisitos establecidos en la sección 2. El proveedor mantendrá actualizada la declaración UE de conformidad según proceda.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 al objeto de modificar el anexo V actualizando el contenido de la declaración UE de conformidad establecida en dicho anexo, con el fin de introducir elementos que resulten necesarios a la luz del progreso técnico.

Artículo 48.– Marcado CE

1. El marcado CE estará sujeto a los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008.

2. En el caso de los sistemas de IA de alto riesgo que se proporcionan digitalmente, se utilizará un marcado CE digital, únicamente si es fácilmente accesible a través de la interfaz desde la que se accede a dicho sistema o mediante un código fácilmente accesible legible por máquina u otros medios electrónicos.

3. El marcado CE se colocará de manera visible, legible e indeleble en los sistemas de IA de alto riesgo. Cuando esto no sea posible o no pueda garantizarse debido a la naturaleza del sistema de IA de alto riesgo, se colocará en el embalaje o en los documentos adjuntos, según proceda.

4. En su caso, el marcado CE irá seguido del número de identificación del organismo notificado responsable de los procedimientos de evaluación de la conformidad establecidos en el artículo 43. El número de identificación del organismo notificado lo colocará él mismo o, siguiendo sus instrucciones, el proveedor o el representante autorizado del proveedor. El número de identificación figurará también en todo el material publicitario en el que se mencione que el sistema de IA de alto riesgo cumple los requisitos de marcado CE.

5. Cuando los sistemas de IA de alto riesgo estén sujetos a otras disposiciones del Derecho de la Unión que también requieran la colocación del marcado CE,

3. Arrisku handiko AA-sistemak Batasunaren harmonizazioko beste lege-egintza batzuen mende daudenean, eta horiek ere EB adostasun-adierazpena behar dutenean, EB adostasun-adierazpen bakar bat egingo da arrisku handiko AA-sistemari aplikagarri zaizkion Batasuneko lege-egintza guztiei dagokienez. Adierazpenean aipatzen diren Batasunaren harmonizazioko lege-egintzak zehazteko behar den informazio guztia bilduko du adierazpenak.

4. EB adostasun-adierazpena egitean, hornitzaileak bere gain hartuko du 2. atalean ezarritako betekizunak betetzeko erantzukizuna. Hornitzaileak eguneratuta edukiko du EB adostasun-adierazpena, dagokionaren arabera.

5. Batzordeak ahalmena izango du 97. artikulua araberako egintza eskuordetuak hartzeko, V. eranskina aldatze aldera, eranskin horretako EB adostasun-adierazpenaren edukia eguneratuz, eta aurrerapen teknikoaren arabera beharrezkoak diren elementuak sartze aldera.

48. artikulua.– CE marka

1. CE markak (EE) 765/2008 Erregelamenduaren 30. artikuluan ezarritako printzipio orokorrak bete beharko ditu.

2. Digitalki ematen diren arrisku handiko AA-sistemen kasuan, CE marka digitala erabiliko da, soilik baldin eta erraz eskuratzeko modukoa bada sistema horretara sartzeko erabiltzen den interfazearen bidez edo makina batek zein beste bitarteko elektroniko batzuek erraz eskuratu eta irakurtzeko moduko kode baten bidez.

3. Behar bezala ikusi, irakurri eta ez ezabatzeko moduan jarriko da CE marka arrisku handiko AA-sistemetan. Arrisku handiko AA-sistemaren izaera dela-eta CE marka modu horretara jartzea ezinezkoa bada edo ezin bada bermatu hala egingo denik, enbalajea edo erantsitako dokumentuetan jarriko da, dagokionaren arabera.

4. Hala badagokio, CE markaren ondoren, 43. artikuluan ezarritako adostasuna ebaluatzeko prozeduren ardura duen organismo jakinaraziaren identifikazio-zenbakia ipiniko da. Organismo jakinaraziaren identifikazio-zenbakia organismoak berak jarriko du, edo, haren jarraibideei jarraituz, hornitzaileak edo hornitzailearen ordezkari baimenduak. Arrisku handiko AA-sistemak CE markaren betekizunak betetzen dituela adierazten duen publizitate-material guztian ere agertuko da identifikazio-zenbakia.

5. Arrisku handiko AA-sistemak Batasuneko zuzenbideko beste xedapen batzuen mende daudenean eta horiek ere CE marka jartzea eskatzen dutenean,



este indicará que los sistemas de IA de alto riesgo también cumplen los requisitos de esas otras disposiciones.

Artículo 49.— Registro

1. Antes de introducir en el mercado o de poner en servicio un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, el proveedor o, en su caso, el representante autorizado, registrarán su sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

2. Antes de introducir en el mercado o poner en servicio un sistema de IA sobre el que el proveedor haya llegado a la conclusión de que no es de alto riesgo de conformidad con el artículo 6, apartado 3, dicho proveedor o, en su caso, el representante autorizado, registrarán ese sistema y a ellos mismos en la base de datos de la UE a que se refiere el artículo 71.

3. Antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos de la UE a que se refiere el artículo 71.

4. En el caso de los sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, el registro a que se refieren los apartados 1, 2 y 3 del presente artículo se efectuará en una sección segura no pública de la base de datos de la UE a que se refiere el artículo 71 e incluirá únicamente la información, según proceda, a la que se hace referencia en:

- a) el anexo VIII, sección A, puntos 1 a 10, con excepción de los puntos 6, 8 y 9;
- b) el anexo VIII, sección B, puntos 1 a 5 y puntos 8 y 9;
- c) el anexo VIII, sección C, puntos 1 a 3;
- d) el anexo IX, puntos 1, 2, 3 y 5.

Únicamente la Comisión y las autoridades nacionales a que se refiere el artículo 74, apartado 8, tendrán acceso a las secciones restringidas respectivas de la base de

arrisku handiko AA-sistemek beste xedapen horietako betekizunak ere betetzen dituztela adieraziko da.

49. artikulua.— Erregistroa

1. Erregelamendu honen III. eranskinean zerrendatutako arrisku handiko AA-sistema bat merkatuan jarri edo zerbitzuan ipini aurretik, III. eranskineko 2. puntuan aipatutako arrisku handiko AA-sistemak izan ezik, 71. artikuluan aipatzen den EBren datu-basean erregistratu beharko dira bai hornitzailea edo, hala badagokio, ordezkari baimendua, bai sistema bera.

2. Hornitzaileak ondorioztatu badu AA-sistema bat ez dela arrisku handikoa —6.3 artikuluan ezarritakoaren arabera—, sistema hori merkatuan jarri edo zerbitzuan ipini aurretik, 71. artikuluan aipatzen den EBren datu-basean erregistratu beharko dira bai hornitzailea edo, hala badagokio, ordezkari baimendua, bai sistema bera.

3. Erregelamendu honen III. eranskinean zerrendatutako arrisku handiko AA-sistema bat zerbitzuan ipini edo erabili aurretik, III. eranskineko 2. puntuan aipatutako arrisku handiko AA-sistemak izan ezik, 71. artikuluan aipatzen den EBren datu-basean erregistratu beharko dira arrisku handiko AA-sistemen hedapenaren arduradun diren agintaritza publikoak, Batasuneko instituzio, organo edo organismoak edo haien izenean jarduten duten pertsonak, eta sistema hautatu eta haren erabilera erregistratu beharko dute.

4. Erregelamendu honen III. eranskineko 1., 6. eta 7. puntuetan aipatutako arrisku handiko AA-sistemen kasuan, zuzenbidea betearaztearen, migrazioaren, asiloaren eta muga-kontrolaren kudeaketaren eremuetan, 71. artikuluan aipatzen den EBren datu-baseko atal ez-publiko seguru batean egingo da artikuluko 1., 2. eta 3. apartatuetan aipatzen den erregistroa, eta puntu hauetan aipatzen den informazioa baino ez du jasoko, dagokionaren arabera:

- a) VIII. eranskineko A ataleko 1etik 10erako puntuak, 6., 8. eta 9. puntuak izan ezik;
- b) VIII. eranskineko B ataleko 1etik 5erako puntuak eta 8. eta 9. puntuak;
- c) VIII. eranskineko C ataleko 1etik 3rako puntuak;
- d) IX. eranskineko 1., 2., 3. eta 5. puntuak.

Batzordeak eta 74.8 artikuluan aipatzen diren agintaritza nazionalak baino ez dute sarbidea izango apartatu



datos de la UE enumeradas en el párrafo primero del presente apartado.

5. Los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, se registrarán a nivel nacional.

CAPÍTULO IV

OBLIGACIONES DE TRANSPARENCIA DE LOS PROVEEDORES Y RESPONSABLES DEL DESPLIEGUE DE DETERMINADOS SISTEMAS DE IA

Artículo 50.— Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA

1. Los proveedores garantizarán que los sistemas de IA destinados a interactuar directamente con personas físicas se diseñen y desarrollen de forma que las personas físicas de que se trate estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización. Esta obligación no se aplicará a los sistemas de IA autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros, salvo que estos sistemas estén a disposición del público para denunciar un delito penal.

2. Los proveedores de sistemas de IA, entre los que se incluyen los sistemas de IA de uso general, que generen contenido sintético de audio, imagen, vídeo o texto, velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial. Los proveedores velarán por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes. Esta obligación no se aplicará en la medida en que los sistemas de IA desempeñen una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada facilitados por el responsable del despliegue o su semántica, o cuando estén autorizados por ley para detectar, prevenir, investigar o enjuiciar delitos.

3. Los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica informarán del funcionamiento del sistema a las personas físicas expuestas a él y tratarán sus datos personales de conformidad con los

honetako lehenengo paragrafoan zerrendatutako EBren datu-baseko atal mugatuak ikusteko.

5. Erregelamendu honen III. eranskineko 2. puntuari aipatzen diren arrisku handiko AA-sistemak nazio-mailan erregistratuko dira.

IV. KAPITULUA

AA-SISTEMA JAKIN BATZUEN HORNITZAILEEN ETA HEDAPENAREN ARDURADUNEN GARDENTASUN-BETEBEHARRAK

50. artikulua.— AA-sistema jakin batzuen hornitzaileen eta hedapenaren arduradunen gardentasun-betebeharrak

1. Pertsona fisikoei zuzenean elkarerraginean aritzeko AA-sistemak diseinatu eta garatzeko orduan, hornitzaileek bermatuko dute kasuan kasuko pertsona fisikoei jakitera emango zaiela AA-sistema batekin elkarerragiten ari direla, salbu eta agerikoa denean, pertsona fisiko zentzuz informatu, erne eta zoli baten ikuspegitik, erabilera-testuingurua eta inguruabarrak kontuan hartuta. Betebehar hori ez zaie aplikatuko delituak detektatu, prebenitu, ikertu edo epaitzeko lege baimenduta dauden AA-sistemei, hirugarrenen eskubide eta askatasunetarako berme egokien mende dauden heinean, salbu eta sistema horiek herritarren eskura badaude delitu penal bat salatzeko.

2. Audio, irudi, bideo edo testuko eduki sintetikoak sortzen duten AA-sistemen hornitzaileek —horien artean daude erabilera orokorreko AA-sistemak— berariaz zainduko dute AA-sistemaren irteera-emaitzak makinek irakurtzeko moduko formatu batean markatuta daudela eta detektatu daitekeela artifizialki sortu edo manipulatu direla. Hornitzaileek berariaz zainduko dute beren soluzio teknikoak eraginkorrak, elkarerragingarriak, sendoak eta fidagarriak izan daitezen, teknikoki bideragarria den neurrian, kontuan hartuta eduki mota desberdinen berezitasunak eta mugak, aplikazio-kostuak eta oro har aitortutako teknikaren uneko egoera, dagozkion arau teknikoetan islatutakoaren arabera. Betebehar hori ez da aplikatuko AA-sistemen edizio estandarrari laguntzeko eginkizuna betetzen dutenean, edo ez dituztenean funtsean aldatzen hedapenaren arduradunak emandako sarrera-datuak edo haien semantika, edo lege baimenduta daudenean delituak detektatu, prebenitu, ikertu edo epaitzeko.

3. Emozioak ezagutzeko sistema baten edo kategorizazio biometrikoko sistema baten hedapenaren arduradunek sistemaren funtzionamenduaren berri emango diete haren eraginpean dauden pertsona fisikoei, eta (EB) 2016/679 eta (EB) 2018/1725



Reglamentos (UE) 2016/679 y (UE) 2018/1725 y con la Directiva (UE) 2016/680, según corresponda. Esta obligación no se aplicará a los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones que hayan sido autorizados por ley para detectar, prevenir e investigar delitos, con sujeción a las garantías adecuadas para los derechos y libertades de terceros y de conformidad con el Derecho de la Unión.

4. Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial. Esta obligación no se aplicará cuando la ley autorice su uso para detectar, prevenir, investigar o enjuiciar delitos. Cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, las obligaciones de transparencia establecidas en el presente apartado se limitarán a la obligación de hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra.

Los responsables del despliegue de un sistema de IA que genere o manipule texto que se publique con el fin de informar al público sobre asuntos de interés público divulgarán que el texto se ha generado o manipulado de manera artificial. Esta obligación no se aplicará cuando el uso esté autorizado por ley para detectar, prevenir, investigar o enjuiciar delitos, o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial por la publicación del contenido.

5. La información a que se refieren los apartados 1 a 4 se facilitará a las personas físicas de que se trate de manera clara y distinguible a más tardar con ocasión de la primera interacción o exposición. La información se ajustará a los requisitos de accesibilidad aplicables.

6. Los apartados 1 a 4 no afectarán a los requisitos y obligaciones establecidos en el capítulo III y se entenderán sin perjuicio de otras obligaciones de transparencia establecidas en el Derecho nacional o de la Unión para los responsables del despliegue de sistemas de IA.

7. La Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión para promover la aplicación efectiva de las obligaciones relativas a la detección y el etiquetado de contenidos generados o manipulados de manera artificial. La Comisión podrá adoptar actos de ejecución

erregelamenduekin eta (EB) 2016/680 Zuzentarauarekin bat etorri tratatuko dituzte haien datu pertsonalak, dagokionaren arabera. Betebehar hori ez zaie aplikatuko delituak detektatu, prebenitu eta ikertzeko lege baimendu diren eta kategorizazio biometrikorako eta emozioak ezagutzeko erabiltzen diren AA-sistemei, hirugarrenen eskubide eta askatasunetarako berme egokiak mende egonda eta Batasuneko zuzenbidearekin bat etorri.

4. Faltsutze sakon bat eragiten duten audio- edo bideo-edukiak edo irudiak sortzen edo manipulatzeko dituen AA-sistema baten hedapenaren arduradunek jakitera emango dute eduki edo irudi horiek artifizialki sortu edo manipulatu direla. Betebehar hori ez da aplikatuko legeak baimena ematen duenean delituak detektatu, prebenitu, ikertu edo epaitzeko erabiltzeko. Argi eta garbi sormenezkoak, satirikoak, artistikoak, fikziozkoak edo antzekoak diren obra edo programa baten parte denean edukia, honetara mugatuko dira apartatu honetan ezarritako gardentasun-betebeharrak: behar bezala jakinaraziko da artifizialki sortutako edo manipulaturako edukia daukala, baina obra erakustea edo gozatzea zaildu gabe.

Herritarrei interes publikoko gaiak buruzko informazioa emateko argitaratzen diren testuak sortu edo manipulatzeko dituzten AA-sistemei dagokienez, hedapenaren arduradunek zabaldu egingo dute testua artifizialki sortu edo manipulatu dela. Betebehar hori ez da aplikatuko erabilera lege baimenduta dagoen delituak detektatu, prebenitu, ikertu edo epaitzeko, edo AA sortutako edukia gizakiak berrikusi badu edo argitalpen-kontrola igaro badu eta pertsona fisiko edo juridiko batek eduki horren argitalpen-erantzukizuna badu.

5. Artikulu honen 1. apartatutik 4.era bitartean aipatzen den informazioa argi eta garbi emango zaie pertsona fisikoei, lehen interakzioa edo esposizioa gertatzen denean, beranduenez. Aplikatzekoak diren irisgarritasun-betekizunen arabera izango da informazioa.

6. Artikulu honen 1. apartatutik 4.era bitartekoek ez diete eragingo III. kapituluaren ezarritako betekizun eta betebeharrak, eta ez dituzte eragotziko Batasuneko zuzenbidean edo zuzenbide nazionalen AA-sistemen hedapenaren arduradunentzat ezarritako beste gardentasun-betebehar batzuk.

7. AA-bulegoak Batasunaren mailan jardunbide egokiak kodeak egitea sustatu eta erraztuko du, artifizialki sortutako edo manipulaturako edukiak detektatu eta etiketatzeari buruzko betebeharrak eraginkortasunez aplikatu daitezela sustatzeko. Batzordeak betearazpen-egintzak hartu ahal izango ditu



a fin de aprobar dichos códigos de buenas prácticas, de conformidad con el procedimiento establecido en el artículo 56, apartado 6. Si considera que el código no es adecuado, la Comisión podrá adoptar un acto de ejecución que especifique normas comunes para el cumplimiento de las citadas obligaciones de conformidad con el procedimiento de examen establecido en el artículo 98, apartado 2.

CAPÍTULO V

MODELOS DE IA DE USO GENERAL

SECCIÓN 1

Reglas de clasificación

Artículo 51.— Reglas de clasificación de los modelos de IA de uso general como modelos de IA de uso general con riesgo sistémico

1. Un modelo de IA de uso general se clasificará como modelo de IA de uso general con riesgo sistémico si reúne alguna de las siguientes condiciones:

a) tiene capacidades de gran impacto evaluadas a partir de herramientas y metodologías técnicas adecuadas, como indicadores y parámetros de referencia;

b) con arreglo a una decisión de la Comisión, adoptada de oficio o a raíz de una alerta cualificada del grupo de expertos científicos, tiene capacidades o un impacto equivalente a los establecidos en la letra a), teniendo en cuenta los criterios establecidos en el anexo XIII.

2. Se presumirá que un modelo de IA de uso general tiene capacidades de gran impacto con arreglo al apartado 1, letra a), cuando la cantidad acumulada de cálculo utilizada para su entrenamiento, medida en operaciones de coma flotante, sea superior a 1025.

3. La Comisión adoptará actos delegados de conformidad con el artículo 97 para modificar los umbrales a que se refieren los apartados 1 y 2 del presente artículo, así como para complementar los parámetros de referencia e indicadores en función de los avances tecnológicos, como las mejoras algorítmicas o la mayor eficiencia del hardware, cuando sea necesario, para que los umbrales reflejen el estado actual de la técnica.

Artículo 52.— Procedimiento

1. Cuando un modelo de IA de uso general cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), el proveedor pertinente lo notificará a la

jardunbide egokien kode horiek onartze aldera, 56.6 artikuluan ezarritako prozedurari jarraikiz. Kodea egokia ez dela iritziz gero, Batzordeak betearazpen-egintza bat hartu ahal izango du, eta, horrekin, betebeharrak horiek 98.2 artikuluan ezarritako azterketa-prozeduraren arabera betetzeko arau erkideak zehaztu.

V. KAPITULUA

ERABILERA OROKORREKO AA-EREDUAK

1. ATALA

Sailkatzeko arauak

51. artikulua.— Erabilera orokorreko AA-ereduak arrisku sistemikoa dakarten erabilera orokorreko AA-eredu gisa sailkatzeko arauak

1. Erabilera orokorreko AA-eredu bat arrisku sistemikoa dakarren erabilera orokorreko AA-eredu gisa sailkatuko da baldintza hauetakoren bat betetzen badu:

a) inpaktu handiko gaitasunak ditu, tresna eta metodologia tekniko egokietatik abiatuta ebaluatuta, hala nola adierazleak eta erreferentziazko parametroak;

b) Batzordeak ofizioz edo aditu zientifikoen taldearen alerta kualifikatu baten ondorioz hartutako erabaki baten arabera, a) letran ezarritako gaitasunak edo antzeko inpaktua ditu, XIII. eranskinean ezarritako irizpideak kontuan hartuta.

2. Erabilera orokorreko AA-eredu batek inpaktu handiko gaitasunak dituela ulertuko da —1.a) apartatuaren arabera— entrenatzeko erabilitako kalkulu-kopuru metatua 10^{25} baino handiagoa denean, koma mugikorrek eragiketetan neurtua.

3. Batzordeak 97. artikuluan arabera egintza eskuordetuak hartuko ditu artikuluko honen 1. eta 2. apartatuaren aipatzen diren atalaseak aldatzeko, bai eta erreferentziazko parametroak eta adierazleak osatzeko ere aurrerapen teknologikoen ondorioz —hala nola hobekuntza algoritmikoak edo hardwarearen efizientzia handiagoa—, beharrezkoa denean, atalaseek teknikaren egungo egoera isla dezaten.

52. artikulua.— Prozedura

1. Erabilera orokorreko AA-eredu batek 51.1.a) artikuluan aipatzen den baldintza betetzen duenean, dagokion hornitzaileak Batzordeari jakinaraziko dio



Comisión sin demora y, en cualquier caso, antes de transcurridas dos semanas desde que se cumpla dicho requisito o desde que se sepa que va a cumplirse. Dicha notificación incluirá la información necesaria para demostrar que se cumple el requisito pertinente. Si la Comisión tiene conocimiento de un modelo de IA de uso general que presenta riesgos sistémicos y que no ha sido notificado, podrá decidir designarlo como modelo con riesgo sistémico.

2. El proveedor de un modelo de IA de uso general que cumpla la condición a que se refiere el artículo 51, apartado 1, letra a), podrá presentar, junto con su notificación, argumentos suficientemente fundamentados que demuestren que, excepcionalmente, aunque el modelo de IA de uso general cumple dicho requisito, no presenta riesgos sistémicos, debido a sus características específicas, y no debe clasificarse, por tanto, como modelo de IA de uso general con riesgo sistémico.

3. Cuando la Comisión concluya que los argumentos presentados con arreglo al apartado 2 no están suficientemente fundamentados y que el proveedor pertinente no ha sido capaz de demostrar que el modelo de IA de uso general no presenta, debido a sus características específicas, riesgos sistémicos, rechazará dichos argumentos y el modelo de IA de uso general se considerará un modelo de IA de uso general con riesgo sistémico.

4. La Comisión podrá determinar que un modelo de IA de uso general presenta riesgos sistémicos, de oficio o a raíz de una alerta cualificada del grupo de expertos científicos con arreglo al artículo 90, apartado 1, letra a), a partir de los criterios establecidos en el anexo XIII.

La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 al objeto de modificar el anexo XIII especificando y actualizando los criterios establecidos en dicho anexo.

5. Previa solicitud motivada de un proveedor cuyo modelo haya sido designado como modelo de IA de uso general con riesgo sistémico con arreglo al apartado 4, la Comisión tendrá en cuenta la solicitud y podrá decidir reevaluar si puede seguir considerándose que el modelo de IA de uso general presenta riesgos sistémicos con arreglo a los criterios establecidos en el anexo XIII. Dicha solicitud contendrá motivos objetivos, detallados y nuevos que hayan surgido desde la decisión de designación. Los proveedores no podrán solicitar la reevaluación antes de transcurridos seis meses desde la decisión de designación. Si tras la reevaluación la Comisión decide mantener la designación como modelo de IA de uso general con riesgo sistémico, los

atzerapenik gabe, eta, nolanahi ere, bi aste igaro aurretik betekizun hori betetzen denetik edo beteko dela jakiten denetik. Jakinarazpen horretan, aipatutako betekizuna betetzen dela frogatzeko behar den informazioa jasoko da. Baldin eta Batzordeak jakiten badu arrisku sistemikoak dakartzan erabilera orokorreko AA-eredu baten berri eman ez dela, arrisku sistemikoa dakarren eredu gisa izendatzea erabaki ahal izango du.

2. Erregelamendu honen 51.1.a) artikuluan aipatzen den baldintza betetzen duen erabilera orokorreko AA-eredu baten hornitzaileak, jakinarazpenarekin batera, behar bezala oinarritutako argudioak aurkeztu ahal izango ditu frogatzeko, salbuespen gisa, erabilera orokorreko AA-ereduak betekizun hori betetzen badu ere, ez dakarrela arrisku sistemikorik bere ezaugarri espezifikoak kontuan hartuta, eta, beraz, ez dela sailkatu behar arrisku sistemikoa dakarren erabilera orokorreko AA-eredu gisa.

3. Batzordeak ondorioztatzen badu 2. apartatuaren arabera aurkeztutako argudioak ez daudela behar bezala arrazoituta eta hornitzailea ez dela gai izan frogatzeko erabilera orokorreko AA-ereduak, bere ezaugarri espezifikoak kontuan hartuta, ez dakarrela arrisku sistemikorik, baztertu egingo ditu argudio horiek, eta arrisku sistemikoa dakarren erabilera orokorreko AA-eredutzat hartuko da erabilera orokorreko AA-eredua.

4. Batzordeak erabaki ahal izango du erabilera orokorreko AA-eredu batek arrisku sistemikoak dakartzala, ofizioz edo aditu zientifikoen taldearen alerta kualifikatu baten ondorioz, 90.1.a) artikuluaaren arabera, XIII. eranskinean ezarritako irizpideak oinarri hartuta.

Batzordeak ahalmena izango du 97. artikuluaaren arabera egintza eskuordetuak hartzeko, XIII. eranskina aldatze aldera, eranskin horretan ezarritako irizpideak zehaztu eta eguneratuz.

5. Artikulu honen 4. apartatuaren arabera arrisku sistemikoa dakarren erabilera orokorreko AA-eredu gisa sailkatutako ereduaren hornitzaile batek arrazoituta eskatuz gero, Batzordeak kontuan hartuko du eskaera, eta berriz ebaluatu ahal izango du ea erabilera orokorreko AA-ereduak arrisku sistemikoak dakartzan oraindik, XIII. eranskinean ezarritako irizpideen arabera. Hala izendatzeko erabakia hartu zenetik sortu diren arrazoi objektibo, zehatz eta berriak jasoko dira eskaera horretan. Hornitzaileek ezin izango dute berriz ebaluatzeko eskaerarik egin hala izendatzeko erabakia hartu eta sei hilabete igaro arte. Berriz ebaluatu ondoren ere Batzordeak erabakitzen badu arrisku sistemikoa dakarren erabilera orokorreko AA-ereduaren izendapenari eutsi behar diola, erabakia hartu eta sei



proveedores no podrán solicitar otra reevaluación hasta transcurridos seis meses desde dicha decisión.

6. La Comisión velará por que se publique una lista de modelos de IA de uso general con riesgo sistémico, que mantendrá actualizada, sin perjuicio de la necesidad de respetar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional.

SECCIÓN 2

Obligaciones de los proveedores de modelos de IA de uso general

Artículo 53.– Obligaciones de los proveedores de modelos de IA de uso general

1. Los proveedores de modelos de IA de uso general:

a) elaborarán y mantendrán actualizada la documentación técnica del modelo, incluida la información relativa al proceso de entrenamiento y realización de pruebas y los resultados de su evaluación, que contendrá, como mínimo, la información establecida en el anexo XI con el fin de facilitarla, previa solicitud, a la Oficina de IA y a las autoridades nacionales competentes;

b) elaborarán y mantendrán actualizada información y documentación y la pondrán a disposición de los proveedores de sistemas de IA que tengan la intención de integrar el modelo de IA de uso general en sus sistemas de IA. Sin perjuicio de la necesidad de observar y proteger los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de conformidad con el Derecho de la Unión y nacional, dicha información y documentación:

i) permitirá a los proveedores de sistemas de IA entender bien las capacidades y limitaciones del modelo de IA de uso general y cumplir sus obligaciones en virtud del presente Reglamento, y

ii) contendrá, como mínimo, los elementos previstos en el anexo XII;

c) establecerán directrices para cumplir el Derecho de la Unión en materia de derechos de autor y derechos afines, y en particular, para detectar y cumplir, por ejemplo, a través de tecnologías punta, una reserva de derechos expresada de conformidad con el artículo 4, apartado 3, de la Directiva (UE) 2019/790;

hilabete igaro arte itxaron beharko dute hornitzaileek berriro eskatu ahal izateko berriz ebaluatzeko.

6. Batzordea arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen zerrenda bat argitaratzeaz arduratuko da, eta eguneratuta mantenduko du, hargatik eragotzi gabe jabetza intelektual eta industrialeko eskubideak eta enpresa-informazio konfidentziala edo merkataritza-sekretuak errespetatu eta babesteko beharra, Batasuneko zuzenbidearekin eta zuzenbide nazionalarekin bat etorritz.

2. ATALA

Erabilera orokorreko AA-ereduen hornitzaileen betebeharrak

53. artikulua.– Erabilera orokorreko AA-ereduen hornitzaileen betebeharrak

1. Zeregin hauek egingo dituzte erabilera orokorreko AA-ereduen hornitzaileek:

a) ereduaren dokumentazio teknikoa egin eta eguneratuta edukiko dute, entrenatzeko prozesuari eta probak egiteari buruzko informazioa eta ebaluazioaren emaitzak barne. Dokumentazio horretan, gutxienez, XI. eranskinean ezarritako informazioa jasoko da, hala eskatuz gero AA-bulegoari eta agintaritza nazional eskudunei emateko;

b) informazioa eta dokumentazioa prestatu eta eguneratuta edukiko dituzte, eta beren AA-sistemetan erabilera orokorreko AA-eredua integratzeko asmoa duten AA-sistemen hornitzaileen esku jarriko dituzte. Jabetza intelektual eta industrialeko eskubideak eta enpresa-informazio konfidentziala edo merkataritza-sekretuak zaindu eta babesteko beharra alde batera utzi gabe, Batasuneko zuzenbidearekin eta zuzenbide nazionalarekin bat etorritz, informazio eta dokumentazio horrek:

i) aukera emango die AA-sistemen hornitzaileei erabilera orokorreko AA-ereduaren gaitasunak eta mugak ondo ulertzeko eta erregulamendu honen arabera dituzten betebeharrak betetzeko, eta

ii) XII. eranskinean aurreikusitako elementuak izango ditu gutxienez;

c) gidalerroak ezarriko dituzte egile-eskubideen eta antzeko eskubideen arloan Batasuneko zuzenbidea betetzeko, eta, bereziki, (EB) 2019/790 Zuzentarauaren 4.3 artikuluaaren arabera adierazitako eskubide-erreserba detektatzeko eta betetzeko, adibidez, puntako teknologien bidez;



d) elaborarán y pondrán a disposición del público un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general, con arreglo al modelo facilitado por la Oficina de IA.

2. Las obligaciones establecidas en el apartado 1, letras a) y b), no se aplicarán a los proveedores de modelos de IA que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público. Esta excepción no se aplicará a los modelos de IA de uso general con riesgo sistémico.

3. Los proveedores de modelos de IA de uso general cooperarán con la Comisión y las autoridades nacionales competentes, según sea necesario, en el ejercicio de sus competencias y facultades en virtud del presente Reglamento.

4. Los proveedores de modelos de IA de uso general podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.

5. A fin de facilitar el cumplimiento de lo dispuesto en el anexo XI, en particular en su punto 2, letras d) y e), la Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 para detallar las metodologías de medición y cálculo con vistas a que la documentación sea comparable y verificable.

6. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97, apartado 2, para modificar los anexos XI y XII en función de los avances tecnológicos.

7. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

d) erabilera orokorreko AA-eredua entrenatzeko erabilitako edukiaren laburpen zehatza egin eta herritarren eskura jarriko dute, AA-bulegoak emandako ereduen arabera.

2. Artikulu honen 1. apartatuko a) eta b) letretan ezarritako betebeharrak ez zaizkie aplikatuko lizentzia libre eta kode ireki baten arabera zabaltzen diren AA-ereduen hornitzaileei, baldin eta lizentzia horrek eredua eskuratu, erabili, aldatu eta banatzea ahalbidetzen badu eta haren parametroak —pisuak, ereduen arkitekturari buruzko informazioa eta ereduen erabilerari buruzko informazioa barne— herritarren eskura jartzen badira. Salbuespen hori ez zaie aplikatuko arrisku sistemikoa dakarten erabilera orokorreko AA-ereduei.

3. Erabilera orokorreko AA-ereduen hornitzaileak lankidetzan arituko dira Batzordearekin eta agintaritz nazional eskudunekin, beharrezkoa denean, erregelamendu honen arabera dituzten eskumenak eta ahalmenak gauzatzeko.

4. Erabilera orokorreko AA-ereduen hornitzaileek jardunbide egokien kodeak erabili ahal izango dituzte, 56. artikuluan xedatutakoaren ildotik, artikulu honen 1. apartatuan ezarritako betebeharrak betetzen dituztela frogatzeko, arau harmonizatu bat argitaratu arte. Europako arau harmonizatuak betetzeak adostasun-presuntzioa ematen die hornitzaileei, arau horiek aipatutako betebeharrak erregulatzen baitituzte. Onartutako jardunbide egokien kode bati atxikitzen ez zaizkion edo Europako arau harmonizatu bat betetzen ez duten erabilera orokorreko AA-ereduen hornitzaileek bitarteko alternatibo egokien bidez frogatu beharko dute beren betebeharrak betetzen dituztela, Batzordeak ebaluatu ditzan.

5. XI. eranskinean eta bereziki 2. puntuko d) eta e) letretan xedatutakoa betetzea errazteko, Batzordeak ahalmena izango du 97. artikulua araberako egintza eskuordetuak hartzeko, neurketa- eta kalkulu-metodologiak zehazte aldera, dokumentazioa konparagarria eta egiaztagarria izan dadin.

6. Batzordeak ahalmena izango du 97.2 artikulua araberako egintza eskuordetuak hartzeko, XI. eta XII. eranskinak aldatzeko aurrerapen teknologikoen arabera.

7. Artikulu honen arabera lortutako informazio eta dokumentazio guztia, merkataritza-sekretuak barne, 78. artikuluan ezarritako konfidentzialtasun-betebeharren arabera tratatuko da.



Artículo 54.– Representantes autorizados de los proveedores de modelos de IA de uso general

1. Antes de introducir en el mercado de la Unión un modelo de IA de uso general, los proveedores establecidos en terceros países tendrán que nombrar, mediante un mandato escrito, a un representante autorizado que esté establecido en la Unión.
2. Los proveedores permitirán que su representante autorizado pueda efectuar las tareas especificadas en el mandato recibido del proveedor.
3. Los representantes autorizados efectuarán las tareas especificadas en el mandato recibido del proveedor. Facilitarán a la Oficina de IA, cuando lo solicite, una copia del mandato en una de las lenguas oficiales de las instituciones de la Unión. A los efectos del presente Reglamento, el mandato habilitará al representante autorizado para realizar las tareas siguientes:

a) comprobar que se ha elaborado la documentación técnica que se indica en el anexo XI y que el proveedor cumple todas las obligaciones a que se refiere el artículo 53 y, en su caso, el artículo 55;

b) conservar una copia de la documentación técnica que se indica en el anexo XI a disposición de la Oficina de IA y de las autoridades nacionales competentes por un período de diez años a partir de la introducción en el mercado del modelo de IA de uso general, y de los datos de contacto del proveedor que haya designado al representante autorizado;

c) facilitar a la Oficina de IA, previa solicitud motivada, toda la información y documentación, incluidas la información y documentación mencionadas en la letra b), que sean necesarias para demostrar el cumplimiento de las obligaciones establecidas en el presente capítulo;

d) cooperar con la Oficina de IA y las autoridades competentes, previa solicitud motivada, en cualquier acción que emprendan en relación con el modelo de IA de uso general, también cuando el modelo esté integrado en un sistema de IA introducido en el mercado o puesto en servicio en la Unión.

4. El mandato habilitará al representante autorizado para que la Oficina de IA o las autoridades competentes se pongan en contacto con él, además de con el proveedor o en lugar de con el proveedor, con referencia a todas las cuestiones relacionadas con la garantía del cumplimiento del presente Reglamento.

54. artikulua.– Erabilera orokorreko AA-ereduen hornitzaileen ordezkari baimenduak

1. Erabilera orokorreko AA-eredu bat Batasuneko merkatuan jarri aurretik, hirugarren herrialderen batean kokatutako hornitzaileek, idatzizko mandatu baten bidez, Batasunean kokatuta dagoen ordezkari baimendu bat izendatu beharko dute.
2. Hornitzailearengandik jasotako mandatuan zehaztutako lanak egiteko aukera emango diete hornitzaileek ordezkari baimenduei.
3. Hornitzailearengandik jasotako mandatuan zehaztutako lanak egingo dituzte ordezkari baimenduek. AA-bulegoak hala eskatuz gero, mandatuaren kopia bat emango diote, Batasuneko instituzioetako hizkuntza ofizialeko batean. Erregelamendu honen ondorioetarako, lan hauek egiteko baimena emango dio mandatuak ordezkari baimenduari:

a) egiaztatzea ea egin den XI. eranskinean adierazten den dokumentazio teknikoa eta ea hornitzaileak betetzen dituen 53. artikuluan eta, hala badagokio, 55. artikuluan aipatzen diren betebeharrak guztiak;

b) XI. eranskinean aipatzen den dokumentazio teknikoaren kopia bat gordetzea AA-bulegoaren eta agintaritza nazional eskudunen eskura, hamar urteko epean, erabilera orokorreko AA-eredua merkatuan jartzen denetik aurrera, eta ordezkari baimendua izendatu duen hornitzailearekin harremanetan jartzeko datuak gordetzea;

c) AA-bulegoak arrazoituta eskatuz gero, AA-bulegoari ematea kapitulu honetan ezarritako betebeharrak betetzen direla frogatzeko behar den informazio eta dokumentazio guztia, b) letran aipatutako informazioa eta dokumentazioa barne;

d) AA-bulegoarekin eta agintaritza eskudunekin lankidetzan aritzea, aldeztu aurretik arrazoituta eskatuz gero, erabilera orokorreko AA-ereduarekin lotuta egiten duten edozein ekintzatan, baita eredua Batasunean merkatuan jarritako edo zerbitzuan ipinitako AA-sistema batean integratuta dagoenean ere.

4. Mandatuak ordezkari baimendua gaituko du AA-bulegoa edo agintaritza eskudunak harekin jar daitezen harremanetan —hornitzailearekin jarri beharrean harremanetan edo hornitzailearekin jartzeaz gain— erregelamendu hau betetzearekin zerikusia duten gai guztiei dagokienez.



5. El representante autorizado pondrá fin al mandato si considera o tiene motivos para considerar que el proveedor contraviene sus obligaciones en virtud del presente Reglamento. En tal caso, también informará inmediatamente a la Oficina de IA del fin del mandato y de los motivos para ello.

6. La obligación establecida en el presente artículo no se aplicará a los proveedores de modelos de IA de uso general que se divulguen con arreglo a una licencia libre y de código abierto que permita el acceso, la utilización, la modificación y la distribución del modelo y cuyos parámetros, incluidos los pesos, la información sobre la arquitectura del modelo y la información sobre el uso del modelo, se pongan a disposición del público, salvo si los citados modelos de IA de uso general presentan riesgos sistémicos.

SECCIÓN 3

Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico

Artículo 55.— Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico

1. Además de las obligaciones enumeradas en los artículos 53 y 54, los proveedores de modelos de IA de uso general con riesgo sistémico:

a) evaluarán los modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, lo que incluye la realización y documentación de pruebas de simulación de adversarios con el modelo con vistas a detectar y mitigar riesgos sistémicos;

b) evaluarán y mitigarán los posibles riesgos sistémicos a escala de la Unión que puedan derivarse del desarrollo, la introducción en el mercado o el uso de modelos de IA de uso general con riesgo sistémico, así como el origen de dichos riesgos;

c) vigilarán, documentarán y comunicarán, sin demora indebida, a la Oficina de IA y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctoras para resolverlos;

d) velarán por que se establezca un nivel adecuado de protección de la ciberseguridad para el modelo de IA de uso general con riesgo sistémico y la infraestructura física del modelo.

2. Los proveedores de modelos de IA de uso general con riesgo sistémico podrán recurrir a códigos de buenas prácticas en el sentido de lo dispuesto en el

5. Ordezkarari baimenduak mandatua amaituko du baldin eta uste badu hornitzaileak urratu egiten dituela erregelamendu honen arabera dituen betebeharrak, edo hori pentsatzeko arrazoiak baditu. Kasu horretan, berehala jakinaraziko dio AA-bulegoari mandatua amaitu duela, eta horretarako arrazoiak berri ere emango dio.

6. Artikulu honetan ezarritako betebeharra ez zaie aplikatuko lizentzia libre eta kode ireki baten arabera zabaltzen diren erabilera orokorreko AA-ereduen hornitzaileei, baldin eta lizentzia horrek ereduak eskuratu, erabili, aldatu eta banatzea ahalbidetzen badu eta haren parametroak —pisuak, ereduaren arkitekturari buruzko informazioa eta ereduaren erabilerari buruzko informazioa barne— herritarren eskura jartzen badira, salbu eta erabilera orokorreko AA-eredu horiek arrisku sistemikoak badakartzate.

3. ATALA

Arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen hornitzaileen betebeharrak

55. artikulua.— Arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen hornitzaileen betebeharrak

1. Erregelamendu honen 53. eta 54. artikuluetan zerrendatutako betebeharez gain, lan hauek egingo dituzte arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen hornitzaileek:

a) ereduak ebaluatuko dituzte, teknikaren egoera islatzen duten protokolo eta tresna normalizatuen arabera, eta horren barruan sartzen da ereduaren aurkaritza-probak egitea eta dokumentatzea, arrisku sistemikoak detektatzeko eta arintzeko;

b) ebaluatu eta arinduko dituzte arrisku sistemikoa dakarten erabilera orokorreko AA-ereduak garatzetik, merkatuan jartzetik edo erabiltzetik erator daitezkeen Batasunaren mailako arrisku sistemikoak, bai eta arrisku horien jatorria ere;

c) gorabehera larriei eta horiek zuzentzeko har daitezkeen neurri zuzentzaileei buruz beharrezko den informazioa zaindu, dokumentatu eta jakinaraziko diote, bidegabeko atzerapenik gabe, AA-bulegoari eta, hala badagokio, agintaritza nazional eskudunei;

d) zainduko dute zibersegurtasunaren babes-maila egokia ezartzen dela arrisku sistemikoa dakarren erabilera orokorreko AA-eredurako eta ereduaren azpiegitura fisikorako.

2. Arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen hornitzaileek jardunbide egokien kodeak erabili ahal izango dituzte, 56. artikuluan xedatutakoaren



artículo 56 para demostrar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo, hasta que se publique una norma armonizada. El cumplimiento de las normas armonizadas europeas otorga a los proveedores presunción de conformidad en la medida en que tales normas regulen dichas obligaciones. Los proveedores de modelos de IA de uso general que no se adhieran a un código de buenas prácticas aprobado o no cumplan una norma armonizada europea deberán demostrar que cumplen sus obligaciones por medios alternativos adecuados para su evaluación por parte de la Comisión.

3. Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

SECCIÓN 4

Códigos de buenas prácticas

Artículo 56.– Códigos de buenas prácticas

1. La Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la Unión a fin de contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta los planteamientos internacionales.

2. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas comprendan al menos las obligaciones establecidas en los artículos 53 y 55, entre las que se incluyen las cuestiones siguientes:

a) los medios para garantizar que la información a que se refiere el artículo 53, apartado 1, letras a) y b), se mantenga actualizada con respecto a la evolución del mercado y los avances tecnológicos;

b) el nivel adecuado de detalle por lo que respecta al resumen sobre el contenido utilizado para el entrenamiento;

c) la determinación del tipo y la naturaleza de los riesgos sistémicos a escala de la Unión, incluido su origen, cuando proceda;

d) las medidas, procedimientos y modalidades de evaluación y gestión de los riesgos sistémicos a escala de la Unión, incluida su documentación, que serán proporcionales a los riesgos y tendrán en cuenta su gravedad y probabilidad y las dificultades específicas para hacerles frente, habida cuenta de la manera en que dichos riesgos pueden surgir y materializarse a lo largo de la cadena de valor de la IA.

ildotik, artikuluko honen 1. apartatuan ezarritako betebeharrak betetzen dituztela frogatzeko, arau harmonizatu bat argitaratu arte. Europako arau harmonizatuak betetzeak adostasun-presuntzioa ematen die hornitzaileei, arau horiek aipatutako betebeharrak erregulatzen baitituzte. Onartutako jardunbide egokien kode bati atxikitzen ez zaizkion edo Europako arau harmonizatu bat betetzen ez duten erabilera orokorreko AA-ereduen hornitzaileek bitarteko alternatibo egokien bidez frogatu beharko dute beren betebeharrak betetzen dituztela, Batzordeak ebaluatu ditzan.

3. Artikulu honen arabera lortutako informazio eta dokumentazio guztia, merkataritza-sekretuak barne, 78. artikuluan ezarritako konfidentzialtasun-betebeharren arabera tratatuko da.

4. ATALA

Jardunbide egokien kodeak

56. artikulua.– Jardunbide egokien kodeak

1. AA-bulegoak Batasunaren mailan jardunbide egokien kodeak egitea sustatu eta erraztuko du, erregelamendu hau behar bezala aplikatzen laguntzeko, nazioarteko planteamenduak kontuan hartuta.

2. AA-bulegoak eta AA-kontseiluak zaindu egingo dute jardunbide egokien kodeak, gutxienez, 53. eta 55. artikuluetan ezarritako betebeharrak jasotzen dituztela; hauek dira, besteak beste:

a) bitartekoak ezarriko dituzte 53.1 artikuluko a) eta b) letretan aipatzen den informazioa merkatuaren bilakaerari eta aurrerapen teknologikoei dagokienez eguneratuta mantentzen dela bermatzeko;

b) xehetasun-maila egokia emango dute entrenatzeko erabili den edukiari buruzko laburpenari dagokionez;

c) Batasunaren mailako arrisku sistemikoen mota eta izaera zehaztuko dituzte, jatorria barne, hala dagokionean;

d) Batasunaren mailako arrisku sistemikoak eta haien dokumentazioa ebaluatzen eta kudeatzeko neurri, prozedura eta modalitateak ezarriko dituzte. Arriskuekiko proportzionalak izango dira, eta kontuan hartuko dituzte haien larritasuna eta probabilitatea, bai eta horiei aurre egiteko zailtasun espezifikoak ere, kontuan hartuta nola sor eta gauza daitezkeen arrisku horiek AAren balio-katean.



3. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general, así como a las autoridades nacionales competentes pertinentes, a participar en la elaboración de códigos de buenas prácticas. Las organizaciones de la sociedad civil, la industria, el mundo académico y otras partes interesadas pertinentes, como los proveedores posteriores y los expertos independientes, podrán contribuir al proceso.

4. La Oficina de IA y el Consejo de IA velarán por que los códigos de buenas prácticas establezcan claramente sus objetivos específicos y contengan compromisos o medidas, como, por ejemplo, indicadores clave de rendimiento, si procede, para garantizar la consecución de dichos objetivos, y que tengan debidamente en cuenta las necesidades e intereses de todas las partes interesadas, incluidas las personas afectadas, a escala de la Unión.

5. La Oficina de IA velará por que los participantes en los códigos de buenas prácticas informen periódicamente a la Oficina de IA sobre la aplicación de los compromisos y las medidas adoptadas y sus resultados, lo que incluye su evaluación con respecto a los indicadores clave de rendimiento, si procede. Los indicadores clave de rendimiento y los compromisos de presentación de información reflejarán las diferencias de tamaño y capacidad entre los distintos participantes.

6. La Oficina de IA y el Consejo de IA supervisarán y evaluarán periódicamente la consecución de los objetivos de los códigos de buenas prácticas por parte de los participantes y su contribución a la correcta aplicación del presente Reglamento. La Oficina de IA y el Consejo de IA evaluarán si los códigos de buenas prácticas incluyen las obligaciones establecidas en los artículos 53 y 55, y supervisarán y evaluarán periódicamente la consecución de sus objetivos. Publicarán su evaluación de la adecuación de los códigos de buenas prácticas.

La Comisión podrá, mediante un acto de ejecución, aprobar un código de buenas prácticas y conferirle una validez general dentro de la Unión. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen contemplado en el artículo 98, apartado 2.

7. La Oficina de IA podrá invitar a todos los proveedores de modelos de IA de uso general a adherirse a los códigos de buenas prácticas. En el caso de los proveedores de modelos de IA de uso general que no presenten riesgos sistémicos, esta adhesión podrá limitarse a las obligaciones previstas en el artículo 53, salvo que declaren expresamente su interés en adherirse al código completo.

3. AA-bulegoak gonbit egin ahal izango die erabilera orokorreko AA-ereduen hornitzaile guztiei, bai eta agintaritzaz nazional eskudunei ere, jardunbide egokien kodeak egiten parte har dezaten. Prozesu horretan, laguntzaile izan daitezke gizarte zibileko antolakundeak, industria, mundu akademikoa eta beste alderdi interesdun batzuk, hala nola ondorengo hornitzaileak eta aditu independenteak.

4. AA-bulegoak eta AA-kontseiluak zainduko dute jardunbide egokien kodeek argi eta garbi ezartzen dituztela beren helburu espezifikoak, eta konpromisoak edo neurriak jasotzen dituztela helburu horiek lortzen direla bermatzeko, hala nola errendimenduari buruzko funtsezko adierazleak, hala badagokio; halaber, zainduko dute behar bezala kontuan hartzen dituztela alderdi interesdun guztien premiak eta interesak, baita ukitutako pertsonenak ere, Batasunaren mailan.

5. AA-bulegoak zainduko du jardunbide egokien kodeetan parte hartzen duten konpromisoen aplikazioari eta hartutako neurriei eta horien emaitzei buruzko informazioa emango diotela, aldian-aldian, AA-bulegoari, errendimenduaren funtsezko adierazleei buruzko ebaluazioa barne, hala badagokio. Errendimenduari buruzko funtsezko adierazleak eta informazioa aurkezteko konpromisoek tamainaren eta gaitasunaren arteko aldeak islatuko dituzte parte-hartzaileen artean.

6. AA-bulegoak eta AA-kontseiluak aldian behin gainbegiratu eta ebaluatuko dute parte-hartzaileek jardunbide egokien kodeen helburuak betetzen dituzten eta erregelamendu hau behar bezala aplikatzen laguntzen duten. AA-bulegoak eta AA-kontseiluak ebaluatuko dute ea 53. eta 55. artikuluetan ezarritako betebeharrak jasotzen diren jardunbide egokien kodeetan, eta aldian behin gainbegiratu eta ebaluatuko dute bertako helburuak betetzen dituzten. Jardunbide egokien kodeen egokitasunari buruz egiten duten ebaluazioa argitaratuko dute.

Batzordeak, betearazpen-egintza baten bidez, jardunbide egokien kode bat onartu ahal izango du, eta balio orokorra eman ahal izango dio Batasunaren barruan. Betearazpen-egintza hori 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko da.

7. AA-bulegoak erabilera orokorreko AA-ereduen hornitzaile guztiak gonbidatu ahal izango ditu jardunbide egokien kodeei atxikitzen. Arrisku sistemikorik ez dakarten erabilera orokorreko AA-ereduen hornitzaileen kasuan, 53. artikuluan aurreikusitako betebeharrak mugatu ahal izango da atxikimendu hori, salbu eta berariaz adierazten badute kode osoari atxikitzeko interesa dutela.



8. La Oficina de IA también fomentará y facilitará, según proceda, la revisión y la adaptación de los códigos de buenas prácticas, en particular teniendo en cuenta las normas emergentes. La Oficina de IA asistirá en la evaluación de las normas disponibles.

9. Los códigos de buenas prácticas estarán finalizados a más tardar el 2 de mayo de 2025. La Oficina de IA adoptará las medidas necesarias, lo que incluye invitar a los proveedores a adherirse a los códigos de buenas prácticas con arreglo a lo dispuesto en el apartado 7.

Si un código de buenas prácticas no se ha podido finalizar a más tardar el 2 de agosto de 2025, o si la Oficina de IA lo considera inadecuado tras su evaluación con arreglo al apartado 6 del presente artículo, la Comisión podrá establecer, mediante actos de ejecución, normas comunes para el cumplimiento de las obligaciones establecidas en los artículos 53 y 55, que incluyan las cuestiones establecidas en el apartado 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO VI

MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 57.– Espacios controlados de pruebas para la IA

1. Los Estados miembros velarán por que sus autoridades competentes establezcan al menos un espacio controlado de pruebas para la IA a escala nacional, que estará operativo a más tardar el 2 de agosto de 2026. Dicho espacio controlado de pruebas también podrá establecerse conjuntamente con las autoridades competentes de otros Estados miembros. La Comisión podrá proporcionar apoyo técnico, asesoramiento y herramientas para el establecimiento y el funcionamiento de los espacios controlados de pruebas para la IA.

La obligación prevista en el párrafo primero también podrá cumplirse mediante la participación en un espacio controlado de pruebas existente en la medida en que dicha participación proporcione un nivel de cobertura nacional equivalente a los Estados miembros participantes.

2. También podrán establecerse espacios controlados de pruebas para la IA adicionales a escala regional o local o conjuntamente con las autoridades competentes de otros Estados miembros.

3. El Supervisor Europeo de Protección de Datos también podrá establecer un espacio controlado de

8. AA-bulegoak, halaber, jardunbide egokien kodeak berrikusi eta egokitzea sustatu eta erraztuko du, dagokionaren arabera, batez ere arau emergenteak kontuan hartuta. AA-bulegoak laguntza emango du dauden arauak ebaluatzeko.

9. Jardunbide egokien kodeak 2025eko maiatzaren 2rako amaituko dira, beranduenez. AA-bulegoak behar diren neurriak hartuko ditu, eta horren barruan sartzen da hornitzaileak gonbidatzea jardunbide egokien kodeei atxikitsera, 7. zenbakian xedatutakoaren arabera.

Jardunbide egokien kode bat ezin izan bada amaitu 2025eko abuztuaren 2rako, edo AA-bulegoak desagokitzat jotzen badu artikulua honen 6. apartatuan ezarritakoaren arabera ebaluatu ondoren, Batzordeak, betearazpen-egintzen bidez, arau komunak ezarri ahal izango ditu 53. eta 55. artikuluetan ezarritako betebeharrak betetzeko, artikulua honen 2. apartatuan ezarritako gaiak barne hartuta. Betearazpen-egintza horiek 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko dira.

VI. KAPITULUA

BERRIKUNTZARI LAGUNTZEKO NEURRIAK

57. artikulua.– AArako proba-ingurune arautuak

1. Estatu kideek zainduko dute beren agintaritza eskudunek AArako proba-ingurune arautu bat ezartzen dutela, gutxienez, nazio-mailan, eta 2026ko abuztuaren 2rako egongo dela martxan, beranduenez. Proba-ingurune arautu hori, halaber, beste estatu kide batzuetako agintaritza eskudunekin batera ezarri ahal izango da. Batzordeak laguntza teknikoa, aholkularitza eta tresnak eman ahal izango ditu AArako proba-ingurune arautuak ezarri eta funtzionamenduan jartzeko.

Lehenengo paragrafoan aurreikusitako betebeharra dagoeneko badagoen proba-ingurune arautu batean parte hartuz ere bete ahal izango da, parte-hartze horrek estaldura-maila baliokidea ematen baitie estatu kide parte-hartzaileei.

2. Erregio- edo toki-mailan ere ezarri ahal izango dira AArako proba-ingurune arautuak, edo beste estatu kide batzuetako agintaritza eskudunekin batera.

3. Datuak Babesteko Europako Ikusatzatzaileak AArako proba-ingurune arautu bat ezarri ahal izango du



pruebas para la IA para las instituciones, órganos y organismos de la Unión, y podrá ejercer las funciones y tareas de las autoridades nacionales competentes de conformidad con el presente capítulo.

4. Los Estados miembros velarán por que las autoridades competentes a que se refieren los apartados 1 y 2 asignen recursos suficientes para cumplir lo dispuesto en el presente artículo de manera efectiva y oportuna. Cuando proceda, las autoridades nacionales competentes cooperarán con otras autoridades pertinentes y podrán permitir la participación de otros agentes del ecosistema de la IA. El presente artículo no afectará a otros espacios controlados de pruebas establecidos en virtud del Derecho de la Unión o nacional. Los Estados miembros garantizarán un nivel adecuado de cooperación entre las autoridades que supervisan esos otros espacios controlados de pruebas y las autoridades nacionales competentes.

5. Los espacios controlados de pruebas para la IA establecidos de conformidad con el apartado 1 proporcionarán un entorno controlado que fomente la innovación y facilite el desarrollo, el entrenamiento, la prueba y la validación de sistemas innovadores de IA durante un período limitado antes de su introducción en el mercado o su puesta en servicio, con arreglo a un plan del espacio controlado de pruebas específico acordado entre los proveedores o proveedores potenciales y la autoridad competente. Tales espacios controlados de pruebas podrán incluir pruebas en condiciones reales supervisadas dentro de ellos.

6. Las autoridades competentes proporcionarán, en su caso, orientación, supervisión y apoyo dentro del espacio controlado de pruebas para la IA con vistas a determinar los riesgos, en particular para los derechos fundamentales, la salud y la seguridad, a las pruebas y a las medidas de reducción y su eficacia en relación con las obligaciones y los requisitos del presente Reglamento y, cuando proceda, de otras disposiciones de Derecho de la Unión y nacional cuya observancia se supervise en el espacio controlado de pruebas.

7. Las autoridades competentes proporcionarán a los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA orientaciones sobre las expectativas en materia de regulación y la manera de cumplir los requisitos y obligaciones establecidos en el presente Reglamento.

A petición del proveedor o proveedor potencial del sistema de IA, la autoridad competente aportará una prueba escrita de las actividades llevadas a cabo con éxito en el espacio controlado de pruebas. La autoridad

Batasuneko instituzio, organo eta organismoentzat, eta agintaritza nazional eskudunen eginkizun eta zereginak bete ahal izango ditu, kapitulu honetan ezarritakoaren arabera.

4. Estatu kideek zainduko dute 1. eta 2. apartatuetan aipatzen diren agintaritza eskudunek behar adina baliabide esleitzen dituztela eraginkortasunez eta egoki betetzeko artikuluko honetan xedatutakoa. Hala dagokionean, agintaritza nazional eskudunak lankidetzan arituko dira beste agintaritza batzuekin, eta AAren ekosistemako beste eragile batzuek parte hartzea baimendu ahal izango dute. Artikulu honek ez du eraginik izango Batasuneko zuzenbidearen edo zuzenbide nazionalaren arabera ezarritako beste proba-ingurune arautu batzuetan. Estatu kideek lankidetz-maila egokia bermatuko dute beste proba-ingurune arautu horiek ikuskatzen dituzten agintaritzen eta agintaritza nazional eskudunen artean.

5. Artikulu honen 1. apartatuaren arabera ezarritako AArako proba-ingurune arautuek inguru arautu bat emango dute berrikuntza sustatzeko eta AA-sistema berritzaileen garapena, entrenamendua, proba eta balioztatzea errazteko, epe mugatu batean, merkatuan jarri edo zerbitzuan ipini aurretik, hornitzaileen edo hornitzaile potentzialen eta agintaritza eskudunaren artean adostutako proba-ingurunearen plan espezifiko baten arabera. Proba-ingurune arautu horietan, baldintza errealeko probak sartu ahal izango dira, ingurune horien barruan gainbegiratuta.

6. Agintaritza eskudunek, hala badagokio, orientazioa, gainbegiratzeko eta laguntza emango dute AArako proba-ingurune arautuaren barruan, zehazteko zein izan daitezkeen bai arriskuak —bereziki oinarritzko eskubideetarako, osasunerako eta segurtasunerako—, bai probak, bai, halaber, arriskuak murrizteko neurriak, eta, horrekin batera, zehazteko ea neurri horiek eraginkorrak izango diren erregelamendu honetako betebeharrak eta betekizunei dagokienez, eta, hala dagokionean, proba-ingurune arautuan gainbegiratzen diren Batasuneko zuzenbidearen edo zuzenbide nazionalaren beste xedapen batzuei dagokienez.

7. Agintaritza eskudunek erregulazioaren arloko aukerei buruzko eta erregelamendu honetan ezarritako betekizunak eta betebeharrak betetzeko moduari buruzko orientabideak emango dizkiete AArako proba-ingurune arautuan parte hartzen duten hornitzaileei edo hornitzaile potentzialei.

AA-sistemaren hornitzaileak edo hornitzaile potentzialak eskatuz gero, agintaritza eskudunak idatzizko froga bat aurkeztuko du proba-ingurune arautuan arrakastaz egindako jardueren inguruan. Agintaritza eskudunak,



competente también proporcionará un informe de salida en el que se detallen las actividades llevadas a cabo en el espacio controlado de pruebas y los resultados y resultados del aprendizaje correspondientes. Los proveedores podrán utilizar esta documentación para demostrar su cumplimiento del presente Reglamento mediante el proceso de evaluación de la conformidad o las actividades de vigilancia del mercado pertinentes. A este respecto, las autoridades de vigilancia del mercado y los organismos notificados tendrán en cuenta positivamente los informes de salida proporcionados y las pruebas escritas aportadas por la autoridad nacional competente, con vistas a acelerar los procedimientos de evaluación de la conformidad en una medida razonable.

8. Con sujeción a las disposiciones de confidencialidad del artículo 78 y con el acuerdo del proveedor o proveedor potencial, la Comisión y el Consejo de IA estarán autorizados a acceder a los informes de salida y los tendrán en cuenta, según proceda, en el ejercicio de sus funciones en virtud del presente Reglamento. Si tanto el proveedor o proveedor potencial como la autoridad nacional competente dan expresamente su acuerdo para ello, el informe de salida podrá hacerse público a través de la plataforma única de información a que se refiere el presente artículo.

9. El establecimiento de espacios controlados de pruebas para la IA tendrá por objeto contribuir a los siguientes objetivos:

a) mejorar la seguridad jurídica para lograr el cumplimiento del presente Reglamento o, en su caso, de otras disposiciones de Derecho de la Unión y nacional aplicable;

b) apoyar el intercambio de mejores prácticas mediante la cooperación con las autoridades que participan en el espacio controlado de pruebas para la IA;

c) fomentar la innovación y la competitividad y facilitar el desarrollo de un ecosistema de la IA;

d) contribuir a un aprendizaje normativo basado en datos contrastados;

e) facilitar y acelerar el acceso al mercado de la Unión de los sistemas de IA, en particular cuando los proporcionen pymes, incluidas las empresas emergentes.

10. Las autoridades nacionales competentes velarán por que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes que proporcionen o respalden el acceso a los datos, las

halaber, irteera-txosten bat emango du, proba-ingurune arautuan egindako jarduerak eta dagozkien ondorioak eta ikaskuntzak zehaztuta. Hornitzaileek erregelamendu hau betetzen dutela frogatzeko erabili ahal izango dute dokumentazio hori, adostasuna ebaluatzeko prozesuaren bidez edo merkatua zaintzeko kasuan kasuko jardueren bidez. Horri dagokionez, merkatua zaintzeko agintaritzek eta organismo jakinaraziek kontuan hartuko dituzte agintaritza nazional eskudunak emandako irteera-txostenak eta aurkeztutako proba idatziak, adostasuna ebaluatzeko prozedurak zentzuzko epe batean bizkortzeko.

8. Erregelamendu honen 78. artikuluko konfidentzialtasun-xedapenak betez eta hornitzailea edo hornitzaile potentziala ados egonda, Batzordeak eta AA-kontseiluak irteera-txostenak eskuratzeko baimena izango dute, eta kontuan hartuko dituzte, dagokionaren arabera, erregelamendu honen arabera dituzten eginkizunak betetzean. Bai hornitzaileak edo hornitzaile potentzialak, bai agintaritza nazional eskudunak berariaz adierazten badute ados daudela, artikulua honetan aipatzen den informazio-plataforma bakarraren bidez eman ahal izango da jakitera irteera-txostena.

9. AArako proba-ingurune arautuak ezartzearen xedea helburu hauek lortzen laguntzea izango da:

a) segurtasun juridikoa hobetzea, erregelamendu hau edo, hala badagokio, aplikatzekoa den Batasuneko zuzenbideko edo zuzenbide nazionalako beste xedapen batzuk betetzea lortzeko;

b) jardunbide egokien trukea bultzatzea, AArako proba-ingurune arautuan parte hartzen duten agintaritzekin lankidetzan arituz;

c) berrikuntza eta lehiakortasuna sustatzea eta AAren ekosistema baten garapena erraztea;

d) datu egiaztatuetan oinarritutako arau-ikaskuntza bultzatzea;

e) AA-sistemak Batasuneko merkatuan jartzea erraztu eta bizkortzea, bereziki ETEek ematen dituztenean —enpresa emergenteek barne—.

10. AA-sistema berritzaileek datu pertsonalen tratamendua inplikatzeko duten neurrian edo beste agintaritza nazional batzuen edo datuetarako sarbidea ematen edo babesten duten beste agintaritza eskudun batzuen gainbegiratze-eremuaren barruan dauden heinean, agintaritza nazional eskudunek zaindu egingo



autoridades nacionales de protección de datos y las demás autoridades nacionales o competentes estén ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y competencias.

11. Los espacios controlados de pruebas para la IA no afectarán a las facultades de supervisión o correctoras de las autoridades competentes que supervisan los espacios controlados de pruebas, tampoco a escala regional o local. Cualquier riesgo considerable para la salud, la seguridad y los derechos fundamentales detectado durante el proceso de desarrollo y prueba de estos sistemas de IA dará lugar a una reducción adecuada. Las autoridades nacionales competentes estarán facultadas para suspender temporal o permanentemente el proceso de prueba, o la participación en el espacio controlado de pruebas si no es posible una reducción efectiva, e informarán a la Oficina de IA de dicha decisión. Con el objetivo de apoyar la innovación en materia de IA en la Unión, las autoridades nacionales competentes ejercerán sus facultades de supervisión dentro de los límites del Derecho pertinente y harán uso de su potestad discrecional a la hora de aplicar disposiciones jurídicas en relación con un proyecto específico de espacio controlado de pruebas para la IA.

12. Los proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA responderán, con arreglo al Derecho de la Unión y nacional en materia de responsabilidad, de cualquier daño infligido a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas. Sin embargo, siempre que los proveedores potenciales respeten el plan específico y las condiciones de su participación y sigan de buena fe las orientaciones proporcionadas por la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracciones del presente Reglamento. En los casos en que otras autoridades competentes responsables de otras disposiciones del Derecho de la Unión y nacional hayan participado activamente en la supervisión del sistema de IA en el espacio controlado de pruebas y hayan proporcionado orientaciones para el cumplimiento, no se impondrán multas administrativas en relación con dichas disposiciones.

13. Los espacios controlados de pruebas para la IA serán diseñados y puestos en práctica de tal manera que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes.

dute datuak babesteko agintaritza nazionalak eta gainerako agintaritza nazional edo eskudunak lotuta daudela AArako proba-ingurune arautuaren funtzionamenduarekin eta inplikatura daudela alderdi horiek gainbegiratzearekin, dagozkien eginkizun eta eskumenek ahalbidetzen duten neurrian.

11. AArako proba-ingurune arautuek ez dute eraginik izango proba-ingurune arautuak gainbegiratzen dituzten agintaritza eskudunen gainbegiratzeko edo zuzentzeko ahalmenetan, ezta erregio- edo toki-mailan ere. AA-sistema horiek garatzeko eta probatzeko prozesuan zehar arrisku nabarmenen bat ikusten bada osasunerako, segurtasunerako eta oinarritzko eskubideetarako, behar den murrizketa egin beharko da. Agintaritza nazional eskudunek ahalmena izango dute proba-prozesua aldi baterako edo betiko eteteko, edo, bestela, benetan murriztu ezin bada, proba-ingurune arautuan parte hartzeko, eta horren berri emango diote AA-bulegoari. Batasunean AAren arloko berrikuntza babesteko helburuarekin, agintaritza nazional eskudunek dagozkien zuzenbidearen mugen barruan gauzatuko dituzte beren gainbegiratze-ahalmenak, eta beren ahalmen diskrezionala erabiliko dute AArako proba-ingurune arautuko proiektu espezifiko bati xedapen juridikoak aplikatzeko orduan.

12. Baldin eta hirugarrenei kalteren bat eragiten bazaie proba-ingurune arautuan egindako esperimentazioaren ondorioz, AArako proba-ingurune arautuan parte hartzen duten hornitzaileak eta hornitzaile potentzialak izango dira arduradun, erantzukizun-arloko Batasuneko zuzenbidearen eta zuzenbide nazionalaren arabera. Hala eta guztiz ere, hornitzaile potentzialek plan espezifiko eta parte hartzeko baldintzak errespetatzen badituzte, eta fede onez jarraitzen badiete agintaritza nazional eskudunak emandako orientabideei, agintaritzek ez dute administrazio-isunik ezarriko erregelamendu hau urratzeagatik. Batasuneko zuzenbidearen eta zuzenbide nazionalaren beste xedapen batzuen ardura duten beste agintaritza eskudun batzuek aktiboki parte hartu badute proba-ingurune arautuan AA-sistema gainbegiratzen eta arauak betetzeko orientabideak eman badituzte, ez da administrazio-isunik ezarriko xedapen horiekin lotuta.

13. AArako proba-ingurune arautuak diseinatu eta praktikan jartzean kontuan hartuko da, hala dagoakionean, mugaz gaindiko lankidetzaz erraztu beharko dutela agintaritza nazional eskudunen artean.



14. Las autoridades nacionales competentes coordinarán sus actividades y cooperarán en el marco del Consejo de IA.

15. Las autoridades nacionales competentes informarán a la Oficina de IA y al Consejo de IA del establecimiento de un espacio controlado de pruebas y podrán solicitarles apoyo y orientación. La Oficina de IA pondrá a disposición del público una lista de los espacios controlados de pruebas previstos y existentes y la mantendrá actualizada con el fin de fomentar una mayor interacción en los espacios controlados de pruebas para la IA, así como la cooperación transfronteriza.

16. Las autoridades nacionales competentes presentarán informes anuales a la Oficina de IA y al Consejo de IA, por primera vez un año después del establecimiento del espacio controlado de pruebas para la IA y, posteriormente, cada año hasta su terminación, así como un informe final. Dichos informes proporcionarán información sobre el progreso y los resultados de la puesta en práctica de dichos espacios controlados de pruebas, incluidos mejores prácticas, incidentes, enseñanzas extraídas y recomendaciones acerca de su configuración y, en su caso, acerca de la aplicación y posible revisión del presente Reglamento, incluidos sus actos delegados y de ejecución, y sobre la aplicación de otras disposiciones de Derecho de la Unión, supervisada por las autoridades competentes en el marco del espacio controlado de pruebas. Las autoridades nacionales competentes pondrán dichos informes anuales, o resúmenes de estos, a disposición del público, en línea. La Comisión tendrá en cuenta, cuando proceda, los informes anuales en el ejercicio de sus funciones en virtud del presente Reglamento.

17. La Comisión desarrollará una interfaz única y específica que contenga toda la información pertinente relacionada con los espacios controlados de pruebas para la IA para que las partes interesadas puedan interactuar con los espacios controlados de pruebas para la IA y plantear consultas a las autoridades competentes, así como pedir orientaciones no vinculantes sobre la conformidad de productos, servicios y modelos de negocio innovadores que incorporen tecnologías de IA, de conformidad con el artículo 62, apartado 1, letra c). La Comisión se coordinará de forma proactiva con las autoridades nacionales competentes, cuando proceda.

Artículo 58.– Disposiciones detalladas relativas a los espacios controlados de pruebas para la IA y al funcionamiento de dichos espacios

1. A fin de evitar que se produzca una fragmentación en la Unión, la Comisión adoptará actos de ejecución que especifiquen las disposiciones detalladas para el

14. Agintaritz nazional eskudunek beren jarduerak koordinatuko dituzte eta lankidetzan jardungo dute AA-kontseiluaren esparruan.

15. Agintaritz nazional eskudunek AA-bulegoari eta AA-kontseiluari jakinaraziko diete proba-ingurune arautu bat ezarri dela, eta laguntza eta orientazioa eskatu ahal izango diete. AA-bulegoak herritarren eskura jarriko du dagoeneko badauden eta aurreikusi diren proba-ingurune arautuen zerrenda bat, eta eguneratuta edukiko du, elkarreragin handiagoa eta mugaz gaindiko lankidetz sustatzeko AArako proba-ingurune arautuetan.

16. Agintaritz nazional eskudunek urteko txostenak aurkeztuko dizkiete AA-bulegoari eta AA-kontseiluari, AArako proba-ingurune arautua ezarri eta urtebetera lehen aldiz, eta, ondoren, urtero, amaitu arte; azken txosten bat ere aurkeztuko diete. Txosten horiek informazioa emango dute proba-ingurune arautu horiek praktikan jarrita zer aurrerapen eta zer-nolako emaitzak lortu diren azaltzeko, jardunbide egokienak, gorabeherak, lortutako irakaskuntzak eta haien konfigurazioari buruzko gomendioak barne, eta, hala badagokio, erregelamendu honen aplikazioa eta balizko berrikuspena ere jasoko du, egintza eskuordetuak eta betearazpen-egintzak barne, baita Batasuneko zuzenbideko beste xedapen batzuen aplikazioa ere, agintaritz eskudunek gainbegiratuta proba-ingurune arautuaren esparruan. Agintaritz nazional eskudunek herritarren eskura jarriko dituzte, linean, urteko txosten horiek edo haien laburpenak. Hala dagokionean, Batzordeak kontuan hartuko ditu urteko txostenak, erregelamendu honen arabera dagozkion eginkizunak betetzeari.

17. Batzordeak interfaze bakar eta espezifiko bat garatuko du AArako proba-ingurune arautuekin lotuta beharrezko den informazio guztia jasotzeko. Bertan, AArako proba-ingurune arautuekin elkarreragiteko aukera izango dute alderdi interesdunek, baita agintaritz eskudunei kontsultak egiteko eta AArako teknologiak txertatzen dituzten produktu, zerbitzu eta negozio-eredu berritzaileen adostasunari buruzko orientabide ez-lotesleak eskatzeko ere, 62.1.c) artikuluekin bat etorritik. Batzordea modu proaktiboan koordinatuko da agintaritz nazional eskudunekin, hala dagokionean.

58. artikulua.– AArako proba-ingurune arautuei eta ingurune horien funtzionamenduari buruzko xedapen zehatzak

1. Batasunean zatiketarik gerta ez dadin, Batzordeak betearazpen-egintzak hartuko ditu, xedapen zehatzak eman ditzaten AArako proba-ingurune arautuen



establecimiento, el desarrollo, la puesta en práctica, el funcionamiento y la supervisión de los espacios controlados de pruebas para la IA. Los actos de ejecución incluirán principios comunes sobre las siguientes cuestiones:

a) los criterios de admisibilidad y selección para participar en el espacio controlado de pruebas para la IA;

b) los procedimientos para la solicitud, la participación, la supervisión, la salida y la terminación del espacio controlado de pruebas para la IA, incluidos el plan del espacio controlado de pruebas y el informe de salida;

c) las condiciones aplicables a los participantes.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. Los actos de ejecución mencionados en el apartado 1 garantizarán:

a) que los espacios controlados de pruebas para la IA estén abiertos a cualquier proveedor o proveedor potencial de un sistema de IA que presente una solicitud y cumpla los criterios de admisibilidad y selección, que serán transparentes y equitativos, y también que las autoridades nacionales competentes informen a los solicitantes de su decisión en un plazo de tres meses a partir de la presentación de la solicitud;

b) que los espacios controlados de pruebas para la IA permitan un acceso amplio e igualitario y se adapten a la demanda de participación; los proveedores y proveedores potenciales también podrán presentar solicitudes en asociación con responsables del despliegue y con otros terceros pertinentes;

c) que las disposiciones detalladas y las condiciones relativas a los espacios controlados de pruebas para la IA propicien, en la medida de lo posible, que las autoridades nacionales competentes dispongan de flexibilidad para establecer y gestionar sus espacios controlados de pruebas para la IA;

d) que el acceso a los espacios controlados de pruebas para la IA sea gratuito para las pymes, incluidas las empresas emergentes, sin perjuicio de los costes excepcionales que las autoridades nacionales competentes puedan recuperar de una forma justa y proporcionada;

e) que se facilite a los proveedores y proveedores potenciales, mediante los resultados del aprendizaje de

ezarpen, garapen, praktikan jartze, funtzionamendu eta ikuskaritzari buruz. Betearazpen-egintzek gai hauei buruzko printzipio komunak jasoko dituzte:

a) AArako proba-ingurune arautuan parte hartzeko onargarritasun- eta hautaketa-irizpideak;

b) AArako proba-ingurune arautua eskatzeko, bertan parte hartzeko, gainbegiratzeko, irteteko eta amaitzeko prozedurak, proba-ingurunearen plana eta irteera-txostena barne;

c) parte-hartzaileei aplikatu behar zaizkien baldintzak.

Betearazpen-egintza horiek 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko dira.

2. Artikulu honen 1. apartatuan aipatutako betearazpen-egintzek alderdi hauek bermatuko dituzte:

a) AArako proba-ingurune arautuak irekita egongo direla eskaera bat aurkezten duen eta onargarritasun- eta hautaketa-irizpideak betetzen dituen AA-sistema baten hornitzaileentzat edo hornitzaile potentzialentzat —irizpideok gardenak eta bidezkoak izango dira—, eta, era berean, agintaritza nazional eskudunek hiru hilabeteko epean emango dietela erabakiaren berri eskatzaileei, eskaera aurkezten denetik aurrera;

b) AArako proba-ingurune arautuek sarbide zabala eta berdintasunezkoa ahalbidetuko dutela eta parte-hartzearen eskarira egokituko direla; hornitzaileek edo hornitzaile potentzialek hedapenaren arduradunekin eta beste hirugarren egoki batzuekin batera ere aurkeztu ahal izango dituzte eskaerak;

c) AArako proba-ingurune arautuei buruzko xedapen zehatzek eta baldintzek, ahal den neurrian, erraztu egingo dutela agintaritza nazional eskudunek malgutasuna izatea AArako proba-ingurune arautuak ezartzeko eta kudeatzeko;

d) AArako proba-ingurune arautuetarako sarbidea doakoa izango dela ETEentzat —enpresa emergenteentzat barne—, alde batera utzi gabe agintaritza nazional eskudunek modu zuzen eta proportzionatuan berreskuratu ditzaketen ezohiko kostuak;

e) hornitzaileei edo hornitzaile potentzialeei erraztasunak emango zaizkiela, AArako proba-ingurune



los espacios controlados de pruebas para la IA, el cumplimiento de las obligaciones de evaluación de la conformidad en virtud del presente Reglamento y la aplicación voluntaria de los códigos de conducta a que se refiere el artículo 95;

f) que los espacios controlados de pruebas para la IA faciliten la participación de otros agentes pertinentes del ecosistema de la IA, como los organismos notificados y los organismos de normalización, las pymes, incluidas las empresas emergentes, las empresas, los agentes innovadores, las instalaciones de ensayo y experimentación, los laboratorios de investigación y experimentación y los centros europeos de innovación digital, los centros de excelencia y los investigadores, a fin de permitir y facilitar la cooperación con los sectores público y privado;

g) que los procedimientos, procesos y requisitos administrativos para la solicitud, la selección, la participación y la salida del espacio controlado de pruebas para la IA sean sencillos y fácilmente inteligibles y se comuniquen claramente, a fin de facilitar la participación de las pymes, incluidas las empresas emergentes, con capacidades jurídicas y administrativas limitadas, y se racionalicen en toda la Unión, a fin de evitar la fragmentación y de que la participación en un espacio controlado de pruebas para la IA establecido por un Estado miembro o por el Supervisor Europeo de Protección de Datos esté reconocida mutua y uniformemente y tenga los mismos efectos jurídicos en toda la Unión;

h) que la participación en el espacio controlado de pruebas para la IA se limite a un período que se ajuste a la complejidad y la escala del proyecto, y que podrá ser prorrogado por la autoridad nacional competente;

i) que los espacios controlados de pruebas para la IA faciliten el desarrollo de herramientas e infraestructuras para la prueba, la evaluación comparativa, la evaluación y la explicación de las dimensiones de los sistemas de IA pertinentes para el aprendizaje normativo, como la precisión, la solidez y la ciberseguridad, así como de medidas para mitigar los riesgos para los derechos fundamentales y la sociedad en su conjunto.

3. Se ofrecerán a los proveedores potenciales que participen en los espacios controlados de pruebas para la IA, en particular a las pymes y las empresas emergentes, cuando proceda, servicios previos al despliegue, como orientaciones sobre la aplicación del presente Reglamento, otros servicios que aportan valor añadido, como ayuda con los documentos de normalización y la certificación, y acceso a las instalaciones de ensayo y experimentación, los centros

arautuetako ikaskuntzen bidez, erregelamendu honi jarraikiz adostasuna ebaluatzeko betebeharrak betetzeko eta 95. artikuluan aipatzen diren jokabide-kodeak borondatez aplikatzeko;

f) AArako proba-ingurune arautuek erraztu egingo dutela AAren ekosistemako beste eragile egoki batzuek parte hartzea, hala nola organismo jakinaraziek eta normalizazio-organismoek, ETEek —enpresa emergenteak barne—, enpresek, eragile berritzaileek, saiakuntza- eta esperimendazio-instalazioek, ikerketa- eta esperimendazio-laborategiek eta berrikuntza digitaleko Europako guneek, bikaintasun-zentroek eta ikertzaileek, sektore publikoarekiko eta pribatuarekiko lankidetzak ahalbidetzeko eta errazteko helburuz;

g) AArako proba-ingurune arautua eskatzeko, hautatzeko, bertan parte hartzeko eta irteteko administrazio-prozedura, -prozesu eta -betekizunak errazak eta erraz ulertzeko modukoak izango direla, eta argi eta garbi komunikatuko direla, gaitasun juridiko eta administrazio mugatuak dituzten ETEen parte-hartzea errazteko —enpresa emergentea barne—, eta Batasun osoan arrazionalizatu daitezkeen, zatiketarik gerta ez dadin eta estatu kide batek edo Datuak Babesteko Europako Ikuskatzaileak ezarritako AArako proba-ingurune arautu bateko parte hartzea elkarri eta uniformeke aitortuta egon dadin, eta ondorio juridiko berberak izan ditzan Batasun osoan;

h) AArako proba-ingurune arautuko parte-hartzea proiektuaren konplexutasunari eta eskalari egokitzen zaion aldi batera mugatuko dela, eta agintaritzak nazional eskudunak aldi hori luzatu ahal izango duela;

i) AArako proba-ingurune arautuek erraztu egingo dutela, batetik, tresna eta azpiegituren garapena, horiekin arau-ikaskuntzarako egokiak diren AA-sistemen proba, ebaluazio konparatibo, ebaluazio eta dimentsioen azalpena egiteko —hala nola zehaztasuna, sendotasuna eta zibersegurtasuna—, eta, bestetik, oinarritzko eskubideetarako eta gizarte osorako arriskurik arintzeko neurrien garapena.

3. AArako proba-ingurune arautuetan parte hartzen duten hornitzaile potentzialak, bereziki ETEak eta enpresa emergenteak, bideratu egingo dira, hala dagokionean, hedatu aurreko zerbitzuetara —esaterako, erregelamendu honen aplikazioari buruzko orientabideetara—, balio erantsia ematen duten beste zerbitzu batzuetara —hala nola normalizazio- eta ziurtapen-dokumentuetarako laguntzarako—, eta saiakuntza- eta esperimendazio-instalazioetarako



europesos de innovación digital y los centros de excelencia.

4. Cuando las autoridades nacionales competentes estudien autorizar la realización de pruebas en condiciones reales supervisadas en el marco de un espacio controlado de pruebas para la IA que se establecerá en virtud del presente artículo, acordarán específicamente las condiciones de dichas pruebas y, en particular, las garantías adecuadas con los participantes, con vistas a proteger los derechos fundamentales, la salud y la seguridad. Cuando proceda, cooperarán con otras autoridades nacionales competentes con el fin de garantizar la coherencia de las prácticas en toda la Unión.

Artículo 59.— Tratamiento ulterior de datos personales para el desarrollo de determinados sistemas de IA en favor del interés público en el espacio controlado de pruebas para la IA

1. En el espacio controlado de pruebas, los datos personales recabados lícitamente con otros fines podrán tratarse únicamente con el objetivo de desarrollar, entrenar y probar determinados sistemas de IA en el espacio controlado de pruebas cuando se cumplan todas las condiciones siguientes:

a) que los sistemas de IA se desarrollen para que una autoridad pública u otra persona física o jurídica proteja un interés público esencial en uno o varios de los siguientes ámbitos:

i) la seguridad y la salud públicas, incluidos la detección, el diagnóstico, la prevención, el control y el tratamiento de enfermedades y la mejora de los sistemas sanitarios,

ii) un elevado nivel de protección y mejora de la calidad del medio ambiente, la protección de la biodiversidad, la protección contra la contaminación, las medidas de transición ecológica, la mitigación del cambio climático y las medidas de adaptación a este,

iii) la sostenibilidad energética,

iv) la seguridad y la resiliencia de los sistemas de transporte y la movilidad, las infraestructuras críticas y las redes,

v) la eficiencia y la calidad de la administración pública y de los servicios públicos;

b) que los datos tratados resulten necesarios para cumplir uno o varios de los requisitos mencionados en el capítulo III, sección 2, cuando dichos requisitos no puedan cumplirse efectivamente mediante el tratamiento

sarbidera, berrikuntza digitaleko Europako guneeetara eta bikaintasun-zentroetara.

4. Agintaritza nazional eskudunek AArako proba-ingurune arautu baten esparruan baldintza errealeko probak gainbegiratura egiteko baimena ematea aztertzen dutenean —artikulu honen arabera ezarriko da hori—, zehazki adostuko dituzte parte-hartzaileekin proba horiek egiteko baldintzak eta, bereziki, berme egokiak, oinarritzko eskubideak, osasuna eta segurtasuna babeste aldera. Hala dagokionean, lankidetzan arituko dira beste agintaritza nazional eskudun batzuekin, Batasun osoan jardunbideak koherenteak izango direla bermatzeko.

59. artikulua.— Datu pertsonalen geroko tratamendua, AA-sistema jakin batzuk garatzeko AArako proba-ingurune arautuan interes publikoaren alde

1. Proba-ingurune arautuan, honetarako bakarrik tratatu ahal izango dira beste helburu batzuetarako legez bildu diren datu pertsonalak: AA-sistema jakin batzuk proba-ingurune arautuan garatzeko, entrenatzeko eta probatzeko. Horretarako, baldintza hauek guztiak bete beharko dira:

a) AA-sistemak garatzen direnean, helburua izan dadila agintaritza publiko batek edo beste pertsona fisiko edo juridiko batek funtsezko interes publiko bat babes dezala eremu hauetako batean edo batzuetan:

i) segurtasun eta osasun publikoak, barne hartuta gaixotasunen detekzioa, diagnostikoa, prebentzioa, kontrola eta tratamendua eta osasun-sistemen hobekuntza,

ii) ingurumenaren kalitatea hobetu eta babesteko maila handia, biodibertsitatea babestea, kutsaduraren aurkako babesa, trantsizio ekologikorako neurriak, klima-aldaketa arintzea eta horretara egokitzeko neurriak,

iii) jasangarritasun energetikoa,

iv) garraio-sistemen segurtasuna eta erresilientzia, eta mugikortasuna, azpiegitura kritikoak eta sareak,

v) administrazio publikoaren eta zerbitzu publikoen efizientzia eta kalitatea;

b) tratatutako datuak beharrezkoak izatea III.2 kapituluaren aipatutako betekizunetako bat edo batzuk betetzeko, baldin eta betekizun horiek ezin badira modu



de datos anonimizados o sintéticos o de otro tipo de datos no personales;

c) que existan mecanismos de supervisión eficaces para detectar si pueden producirse durante la experimentación en el espacio controlado de pruebas riesgos elevados para los derechos y libertades de los interesados, mencionados en el artículo 35 del Reglamento (UE) 2016/679 y en el artículo 39 del Reglamento (UE) 2018/1725, así como mecanismos de respuesta para mitigar sin demora dichos riesgos y, en su caso, detener el tratamiento;

d) que los datos personales que se traten en el contexto del espacio controlado de pruebas se encuentren en un entorno de tratamiento de datos funcionalmente separado, aislado y protegido, bajo el control del proveedor potencial, y que únicamente las personas autorizadas tengan acceso a dichos datos;

e) que los proveedores solo puedan compartir los datos recabados originalmente de conformidad con el Derecho de la Unión en materia de protección de datos; los datos personales creados en el espacio controlado de pruebas no pueden salir del espacio controlado de pruebas;

f) que el tratamiento de datos personales en el contexto del espacio controlado de pruebas no dé lugar a medidas o decisiones que afecten a los interesados ni afecte a la aplicación de sus derechos establecidos en el Derecho de la Unión en materia de protección de datos personales;

g) que los datos personales tratados en el contexto del espacio controlado de pruebas se protejan mediante medidas técnicas y organizativas adecuadas y se eliminen una vez concluida la participación en dicho espacio o cuando los datos personales lleguen al final de su período de conservación;

h) que los archivos de registro del tratamiento de datos personales en el contexto del espacio controlado de pruebas se conserven mientras dure la participación en el espacio controlado de pruebas, salvo que se disponga otra cosa en el Derecho de la Unión o el Derecho nacional;

i) que se conserve una descripción completa y detallada del proceso y la lógica subyacentes al entrenamiento, la prueba y la validación del sistema de IA junto con los resultados del proceso de prueba como parte de la documentación técnica a que se refiere el anexo IV;

j) que se publique una breve síntesis del proyecto de IA desarrollado en el espacio controlado de pruebas, junto con sus objetivos y resultados previstos, en el sitio

efektiboan bete datu anonimizatu edo sintetikoen edo bestelako datu ez-pertsonalen tratamenduaren bidez;

c) gainbegiratzeko-mekanismo eraginkorrak egotea detektatzeko ea proba-ingurune arautuan esperimendatu bitartean arrisku handiak gerta daitezkeen interesdunen eskubide eta askatasunetarako —(EB) 2016/679 Erregelamenduaren 35. artikuluan eta (EB) 2018/1725 Erregelamenduaren 39. artikuluan aipatutakoak—, eta erantzun-mekanismoak egotea arrisku horiek atzerapenik gabe arintzeko eta, hala badagokio, tratamendua eteteko;

d) funtzionalki bereizita, isolatuta eta babestuta dagoen datu-tratamenduko ingurune batean egotea proba-ingurune arautuaren testuinguruan tratatzen diren datu pertsonalak, hornitzaile potentzialaren kontrolpean, eta baimendutako pertsonen soilik izatea datu horietarako irispidea;

e) hornitzaileek jatorrian datuen babesaren arloko Batasuneko zuzenbidearen arabera bildutako datuak soilik partekatu ahal izatea; proba-ingurune arautuan sortutako datu pertsonalak ezin dira proba-ingurune araututik irten;

f) proba-ingurune arautuaren testuinguruan datu pertsonalak tratatzeak ez dezala ekarri interesdunei eragiten dien neurri edo erabakirik, eta ez diezaiola eragin datu pertsonalen babesaren arloan Batasuneko zuzenbidean ezarritako eskubideak aplikatzeari;

g) proba-ingurune arautuaren testuinguruan tratatutako datu pertsonalak neurri teknikoaren eta antolakuntzakoaren bidez babestea, eta ezabatzea ingurune horretan parte hartzen amaitzean edo datu pertsonalak gordetzeko aldia amaitzen denean;

h) proba-ingurune arautuaren testuinguruko datu pertsonalen tratamenduaren erregistro-artxiboak proba-ingurune arautuan parte hartzen den bitartean gordetzea, salbu eta besterik xedatzen badu Batasuneko zuzenbideak edo zuzenbide nazionalak;

i) prozesuaren deskribapen osoa eta zehatza gordetzea, eta AA-sistemaren entrenamendu, proba eta balioztatzearen logika gordetzea, baita proba-prozesuaren emaitzak ere, IV. eranskinean aipatzen den dokumentazio teknikoaren zati gisa;

j) proba-ingurune arautuan garatutako AA-proiektuaren laburpen bat argitaratzea, helburuak eta emaitza aurreikusiak ere adierazteko, agintaritzaz



web de las autoridades competentes; esta obligación no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control fronterizo, de la inmigración o del asilo.

2. Cuando se lleve a cabo con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, y bajo el control y la responsabilidad de las autoridades garantes del cumplimiento del Derecho, el tratamiento de datos personales en los espacios controlados de pruebas para la IA se basará en un Derecho específico, de la Unión o nacional y cumplirá las condiciones acumulativas que se indican en el apartado 1.

3. El apartado 1 se entiende sin perjuicio del Derecho de la Unión o nacional que proscriba el tratamiento de datos personales con fines distintos de los expresamente mencionados en dichos actos, así como sin perjuicio del Derecho de la Unión o nacional que establezca las bases para el tratamiento de datos personales necesario para desarrollar, probar o entrenar sistemas innovadores de IA o de cualquier otra base jurídica, de conformidad con el Derecho de la Unión en materia de protección de datos personales.

Artículo 60.— Pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA

1. Los proveedores o proveedores potenciales de sistemas de IA de alto riesgo enumerados en el anexo III podrán realizar pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA de conformidad el presente artículo y con el plan de la prueba en condiciones reales a que se refiere el presente artículo, sin perjuicio de las prohibiciones establecidas en el artículo 5.

La Comisión adoptará, mediante un acto de ejecución, los elementos detallados del plan de la prueba en condiciones reales. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

El presente apartado se entiende sin perjuicio del Derecho de la Unión o nacional en materia de pruebas en condiciones reales de sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I.

2. Los proveedores o proveedores potenciales podrán realizar pruebas de los sistemas de IA de alto riesgo

eskudunen webgunean; betebeharrak horretan ez dira sartuko zuzenbidea betearazteaz, muga-kontrolaz, immigrazioaz edo asiloaz arduratzen diren agintaritzen jarduerari buruzko bereziki babestutako datu operatiboak.

2. Delituak prebenitu, ikertu, detektatu edo epaitzeko edo zehapen penalak betearazteko egiten denean, barne hartuta segurtasun publikorako mehatxuen aurkako babesa eta mehatxu horien prebentzioa, eta kontrola eta erantzukizuna zuzenbidea betearazteko agintaritzena dela, datu pertsonalen tratamendua, AArako proba-ingurune arautuetan, zuzenbide espezifiko batean —Batasunekoan edo nazionalen— oinarrituko da, eta 1. apartatuan adierazten diren baldintza metagarriak beteko ditu.

3. Artikulu honen 1. apartatuak ez dio kalterik egingo datu pertsonalen tratamendua egintza horietan berariaz aipatutakoez bestelako helburuetarako debekatzen duen Batasuneko zuzenbideari edo zuzenbide nazionalari, ez eta AA-sistema berritzaileak garatu, probatu edo entrenatzeko behar diren datu pertsonalen tratamendurako oinarriak ezartzen dituen Batasuneko zuzenbideari edo zuzenbide nazionalari, ez beste edozein oinarri juridikori ere, bat etorritik Batasuneko zuzenbideak datu pertsonalen babesaren arloan ezarritakoarekin.

60. artikulua.— Arrisku handiko AA-sistemen baldintza errealeko probak, AArako proba-ingurune arautuetatik kanpo

1. Erregelamendu honen III. eranskinean zerrendatuta dauden arrisku handiko AA-sistemen hornitzaileak edo hornitzaile potentzialek arrisku handiko AA-sistemen baldintza errealeko probak egin ahal izango dituzte AArako proba-ingurune araututik kanpo, bat etorritik artikulu honekin eta artikulu honetan aipatzen den baldintza errealeko probaren planarekin, hargatik eragotzi gabe 5. artikuluan ezarritako debekuak.

Batzordeak, betearazpen-egintza baten bidez, baldintza errealeko probaren planean zehaztutako elementuak onartuko ditu. Betearazpen-egintza horiek 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko dira.

Apartatu honek ez dio kalterik egingo Batasunaren harmonizazioko lege-egintzek (I. eranskina) arautzen dituzten produktuei lotutako arrisku handiko AA-sistemen baldintza errealeko proben arloko Batasuneko zuzenbideari edo zuzenbide nazionalari.

2. Hornitzaileak edo hornitzaile potentzialek III. eranskinean aipatutako arrisku handiko AA-sistemen



mencionados en el anexo III en condiciones reales en cualquier momento antes de la introducción en el mercado o la puesta en servicio del sistema de IA por cuenta propia o en asociación con uno o varios responsables del despliegue o responsables del despliegue potenciales.

3. Las pruebas de sistemas de IA de alto riesgo en condiciones reales con arreglo al presente artículo se entenderán sin perjuicio de cualquier revisión ética que se exija en el Derecho de la Unión o nacional.

4. Los proveedores o proveedores potenciales podrán realizar pruebas en condiciones reales solamente cuando se cumplan todas las condiciones siguientes:

a) el proveedor o proveedor potencial ha elaborado un plan de la prueba en condiciones reales y lo ha presentado a la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales;

b) la autoridad de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales ha aprobado las pruebas en condiciones reales y el plan de la prueba en condiciones reales; si la autoridad de vigilancia del mercado no responde en un plazo de treinta días, se entenderá que las pruebas en condiciones reales y el plan de la prueba en condiciones reales han sido aprobados; cuando el Derecho nacional no contemple una aprobación tácita, las pruebas en condiciones reales estarán sujetas a una autorización también en este caso;

c) el proveedor o proveedor potencial, con excepción de los proveedores o proveedores potenciales de sistemas de IA de alto riesgo mencionados en el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, así como de los sistemas de IA de alto riesgo mencionados en el punto 2 del anexo III ha registrado las pruebas en condiciones reales de conformidad con el artículo 71, apartado 4, con un número de identificación único para toda la Unión y la información indicada en el anexo IX; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 y 7, en los ámbitos de la garantía del cumplimiento del Derecho, la migración, el asilo y la gestión del control fronterizo, ha registrado las pruebas en condiciones reales en la parte no pública de la base de datos de la UE de conformidad con el artículo 49, apartado 4, letra d), con un número de identificación único para toda la Unión y la información indicada en este; el proveedor o proveedor potencial de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 2, ha registrado las

baldintza errealeko probak egin ahal izango dituzte, AA-sistema merkatuan jarri edo zerbitzuan ipini aurreko edozein unetan, beren kontura edo hedapenaren arduradun batekin edo batzuekin edo hedapenaren arduradun potentzialekin elkartuta.

3. Arrisku handiko AA-sistemen baldintza errealeko probek, artikuluko honen arabera, ez dute eragotziko Batasuneko zuzenbidean edo zuzenbide nazionalen eskatzen den edozein berrikuspen etiko.

4. Baldintza hauek guztiak betetzen direnean bakarrik egin ahal izango dituzte baldintza errealeko probak hornitzaileek edo hornitzaile potentzialak:

a) hornitzaileak edo hornitzaile potentzialak baldintza errealeko probaren plan bat egin du, eta baldintza errealeko probak egingo diren estatu kideko merkatua zaintzeko agintaritzari aurkeztu dio;

b) baldintza errealeko probak egingo diren estatu kideko merkatua zaintzeko agintaritzak onartu egin ditu baldintza errealeko probak eta baldintza errealeko probaren plana; baldin eta merkatua zaintzeko agintaritzak hogeita hamar eguneko epean erantzuten ez badu, ulertuko da baldintza errealeko probak eta baldintza errealeko probaren plana onartu direla; baldin eta zuzenbide nazionalak ez badu isilbidezko onarpenik aurreikusten, baldintza errealeko probek kasu horretan ere izan beharko dute baimena;

c) hornitzaileak edo hornitzaile potentzialak, salbuespen direla III. eranskineko 1., 6. eta 7. puntuetan aipatu diren arrisku handiko AA-sistemen hornitzaileak edo hornitzaile potentzialak, zuzenbidea betearaztearen, migrazioaren, asiloaren eta muga-kontrolaren kudeaketaren eremuetan, eta III. eranskineko 2. puntuan aipatutako arrisku handiko AA-sistemak, baldintza errealeko probak erregistratu ditu 71.4 artikulua arabera, Batasun osorako identifikazio-zenbaki bakarrarekin eta IX. eranskinean adierazitako informazioarekin; III. eranskineko 1., 6. eta 7. puntuetan aipatu diren arrisku handiko AA-sistemen hornitzaileak edo hornitzaile potentzialak, zuzenbidea betearaztearen, migrazioaren, asiloaren eta muga-kontrolaren kudeaketaren eremuetan, baldintza errealeko probak erregistratu ditu EBren datu-basearen atal ez-publikoan, 49.4.d) artikulua arabera, Batasun osorako identifikazio-zenbaki bakarrarekin eta bertan adierazitako informazioarekin; III. eranskineko 2. puntuan aipatutako arrisku handiko AA-sistemen hornitzaileak edo hornitzaile potentzialak, baldintza errealeko probak erregistratu ditu 49.5 artikulua arabera;



pruebas en condiciones reales de conformidad con el artículo 49, apartado 5;

d) el proveedor o proveedor potencial que realiza las pruebas en condiciones reales está establecido en la Unión o ha designado a un representante legal que está establecido en la Unión;

e) los datos recabados y tratados a efectos de las pruebas en condiciones reales únicamente se transferirán a terceros países si se aplican las garantías adecuadas y aplicables en virtud del Derecho de la Unión;

f) las pruebas en condiciones reales no duran más de lo necesario para lograr sus objetivos y, en cualquier caso, no más de seis meses, que podrán prorrogarse por un período adicional de seis meses, con sujeción al envío de una notificación previa por parte del proveedor o proveedor potencial a la autoridad de vigilancia del mercado, acompañada por una explicación de la necesidad de dicha prórroga;

g) los sujetos de las pruebas en condiciones reales que sean personas pertenecientes a colectivos vulnerables debido a su edad o a una discapacidad cuentan con protección adecuada;

h) cuando un proveedor o proveedor potencial organice las pruebas en condiciones reales en cooperación con uno o varios responsables del despliegue o responsables del despliegue potenciales, estos últimos habrán sido informados de todos los aspectos de las pruebas que resulten pertinentes para su decisión de participar y habrán recibido las instrucciones de uso pertinentes del sistema de IA a que se refiere el artículo 13; el proveedor o proveedor potencial y el responsable del despliegue o responsable del despliegue potencial alcanzarán un acuerdo en que se detallan sus funciones y responsabilidades con vistas a garantizar el cumplimiento de las disposiciones relativas a las pruebas en condiciones reales con arreglo al presente Reglamento y a otras disposiciones de Derecho de la Unión y nacional aplicable;

i) los sujetos de las pruebas en condiciones reales han dado su consentimiento informado de conformidad con el artículo 61 o, en el ámbito de la garantía del cumplimiento del Derecho, en el que intentar obtener el consentimiento informado impediría que se probara el sistema de IA, las pruebas en sí y los resultados de las pruebas en condiciones reales no tendrán ningún efecto negativo sobre los sujetos, cuyos datos personales se suprimirán una vez realizada la prueba;

j) las pruebas en condiciones reales son supervisadas de manera efectiva por el proveedor o el

d) baldintza errealeko probak egiten dituen hornitzailea edo hornitzaile potentziala Batasunean dago ezarrita, edo Batasunean ezarrita dagoen legezko ordezkari bat izendatu du;

e) Batasuneko zuzenbidearen arabera egokiak eta aplikatzekoak diren bermeak aplikatzen badira bakarrik transferituko dira hirugarren herrialdeetara baldintza errealeko proben ondorioetarako bildutako eta tratatutako datuak;

f) baldintza errealeko probek ez dute irauten beren helburuak lortzeko beharrezkoa dena baino gehiago, eta, nolahi ere, sei hilabete gehienez; halaber, beste sei hilabetez luzatu ahal izango dira, eta, horretarako, hornitzaileak edo hornitzaile potentzialak aldeztu aurretik jakinarazpen bat bidali behar dio merkatua zaintzeko agintaritzari, zergatik luzatu behar den azaltzeko;

g) baldintza errealeko probetako parte-hartzaileek, baldin eta kolektibo kaltebera batekoak badira adinaren edo desgaitasunen baten ondorioz, babes egokia dute;

h) hornitzaile batek edo hornitzaile potentzial batek baldintza errealeko probak lankidetzan antolatzen dituztenean hedapenaren arduradun batekin edo batzuekin edo hedapenaren arduradun potentzial batekin edo batzuekin, azken horiek informazio egokia jaso beharko dute parte hartu ala ez erabakitzeko beharrezkotzat jotzen diren proben alderdi guztiei buruz, eta 13. artikuluan aipatzen den AA-sistema erabiltzeko erabilera-jarraibide egokiak ere jaso beharko dituzte; hornitzaileak edo hornitzaile potentzialak eta hedapenaren arduradunak edo hedapenaren arduradun potentzialak akordio bat egingo dute, bakoitzaren eginkizunak eta erantzukizunak zehaztuta, baldintza errealeko probei buruzko xedapenak erregelamendu honen eta aplikatzekoak diren Batasuneko zuzenbideko edo zuzenbide nazionalako beste xedapen batzuen arabera beteko direla bermatzeko;

i) baldintza errealeko probetako parte-hartzaileek adostasun informatua eman dute 61. artikulua arabera, edo, zuzenbidea betearaztearen eremuan, non baimen informatua lortzen saiatzeak eragotzi egingo bailuke AA-sistema frogatzea, probek eta proben emaitzek, baldintza errealean, ez dute inolako ondorio negatiborik izango parte-hartzaileengan, eta haien datu pertsonalak proba egin ondoren ezabatuko dira;

j) baldintza errealeko probak modu eraginkorrean ikuskatzen dituzte hornitzaileak edo hornitzaile



proveedor potencial y por los responsables del despliegue o los responsables del despliegue potenciales mediante personas adecuadamente cualificadas en el ámbito pertinente y con la capacidad, formación y autoridad necesarias para realizar sus tareas;

k) se pueden revertir y descartar de manera efectiva las predicciones, recomendaciones o decisiones del sistema de IA.

5. Cualquier sujeto de las pruebas en condiciones reales o su representante legalmente designado, según proceda, podrá, sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación, abandonar las pruebas en cualquier momento retirando su consentimiento informado y solicitar la supresión inmediata y permanente de sus datos personales. La retirada del consentimiento informado no afectará a las actividades ya completadas.

6. De conformidad con el artículo 75, los Estados miembros conferirán a sus autoridades de vigilancia del mercado poderes para exigir a los proveedores y proveedores potenciales que faciliten información, realizar sin previo aviso inspecciones a distancia o in situ y controlar la realización de las pruebas en condiciones reales y los sistemas de IA de alto riesgo relacionados. Las autoridades de vigilancia del mercado harán uso de dichos poderes para garantizar que las pruebas en condiciones reales se desarrollen de manera segura.

7. Se informará de cualquier incidente grave detectado en el transcurso de las pruebas en condiciones reales a la autoridad nacional de vigilancia del mercado de conformidad con el artículo 73. El proveedor o proveedor potencial adoptará medidas de reducción inmediatas o, en su defecto, suspenderá las pruebas en condiciones reales hasta que se produzca dicha reducción o pondrá fin a las pruebas. El proveedor o proveedor potencial establecerá un procedimiento para la rápida recuperación del sistema de IA en caso de que se ponga fin a las pruebas en condiciones reales.

8. El proveedor o proveedor potencial notificará a la autoridad nacional de vigilancia del mercado del Estado miembro en que se vayan a realizar las pruebas en condiciones reales la suspensión o la terminación de las pruebas en condiciones reales y los resultados finales.

9. El proveedor o proveedor potencial será responsable, conforme al Derecho de la Unión y nacional en materia de responsabilidad aplicable, de cualquier daño causado en el transcurso de sus pruebas en condiciones reales.

potentzialek, bai eta hedapenaren arduradunek edo hedapen arduradun potentzialek ere, dagokien eremuan behar bezala kualifikatuta dauden eta beren zereginak egiteko behar diren gaitasun, prestakuntza eta aginpidea duten pertsonen bidez;

k) AA-sistemaren iragarpenak, gomendioak edo erabakiak modu eraginkorrean irauli eta baztertu daitezke.

5. Baldintza errealeko proben edozein parte-hartzailek, edo haren legezko ordezkariak, dagokionaren arabera, edozein unetan utzi ahal izango ditu probak, inolako kalterik jasan gabe eta inolako justifikaziorik eman beharrik gabe; horretarako, adostasun informatua erretiratu beharko du, eta bere datu pertsonalak berehala eta modu iraunkorrean ezabatzeko eskatu. Adostasun informatua erretiratzek ez du eraginik izango dagoeneko amaituta dauden jardueretan.

6. Erregelamendu honen 75. artikuluaaren arabera, estatu kideek merkatua zaintzeko agintaritzek ahalak emango dizkiete hornitzaileei edo hornitzaile potentzialei informazioa emateko eskatzeko, aurrez abisatu gabe ikuskapenak egiteko, urrutitik zein *in situ*, eta baldintza errealeko probak egiten diren begiratzeko eta haiekin lotutako arrisku handiko AA-sistemak kontrolatzeko. Merkatua zaintzeko agintaritzek ahal horiek erabiliko dituzte baldintza errealeko probak modu seguruan garatzen direla bermatzeko.

7. Baldintza errealeko proba egin bitartean gorabehera larriren bat detektatzen bada, horren berri emango zaio merkatua zaintzeko agintaritzari nazionalari, 73. artikuluaaren arabera. Hornitzaileak edo hornitzaile potentzialak berehalako murrizketa-neurriak hartuko ditu, edo, halakorik ezean, eten egingo ditu baldintza errealeko probak murrizketa hori gertatu arte, edo, bestela, probak amaituko ditu. Baldintza errealeko probak amaituz gero, AA-sistema azkar berreskuratzeko prozedura bat ezarriko du hornitzaileak edo hornitzaile potentzialak.

8. Hornitzaileak edo hornitzaile potentzialak baldintza errealeko probak egingo diren estatu kideko merkatua zaintzeko agintaritzari nazionalari jakinaraziko dio baldintza errealeko probak eten edo amaitu egin direla, eta azken emaitzen berri emango dio.

9. Hornitzailea edo hornitzaile potentziala izango da baldintza errealeko probetan eragindako kalte guztien erantzule, erantzukizun-arloko Batasuneko zuzenbidearekin edo zuzenbide nazionalarekin bat etorritik.



Artículo 61.— Consentimiento informado para participar en pruebas en condiciones reales fuera de los espacios controlados de pruebas para la IA

1. A los efectos de las pruebas en condiciones reales con arreglo al artículo 60, se obtendrá de los sujetos de las pruebas un consentimiento informado dado libremente antes de participar en dichas pruebas y después de haber recibido información concisa, clara, pertinente y comprensible en relación con:

a) la naturaleza y los objetivos de las pruebas en condiciones reales y los posibles inconvenientes asociados a su participación;

b) las condiciones en las que se van a llevar a cabo las pruebas en condiciones reales, incluida la duración prevista de la participación del sujeto o los sujetos;

c) sus derechos y las garantías relativas a su participación, en particular su derecho a negarse a participar y el derecho a abandonar las pruebas en condiciones reales en cualquier momento sin sufrir por ello perjuicio alguno y sin tener que proporcionar ninguna justificación;

d) las disposiciones para solicitar la reversión o el descarte de las predicciones, recomendaciones o decisiones del sistema de IA;

e) el número de identificación único para toda la Unión de la prueba en condiciones reales de conformidad con el artículo 60, apartado 4, letra c), y la información de contacto del proveedor o de su representante legal, de quien se puede obtener más información.

2. El consentimiento informado estará fechado y documentado, y se entregará una copia a los sujetos de la prueba o a sus representantes legales.

Artículo 62.— Medidas dirigidas a proveedores y responsables del despliegue, en particular pymes, incluidas las empresas emergentes

1. Los Estados miembros adoptarán las medidas siguientes:

a) proporcionarán a las pymes, incluidas las empresas emergentes, que tengan un domicilio social o una sucursal en la Unión un acceso prioritario a los espacios controlados de pruebas para la IA, siempre que cumplan las condiciones de admisibilidad y los criterios de selección; el acceso prioritario no impedirá que otras pymes, incluidas las empresas emergentes, distintas de las mencionadas en el presente apartado accedan al espacio controlado de pruebas para la IA,

61. artikulua.— AArako proba-ingurune arautuetatik kanpo baldintza errealeko probetan parte hartzeko adostasun informatua

1. Erregelamendu honen 60. artikuluan arautu diren baldintza errealeko proben ondorioetarako, proben parte-hartzaileek adostasun informatu bat eman ahal izango dute, proba horietan parte hartu aurretik eta gai hauei buruzko informazio labur, argi, esanguratsu eta ulergarria jaso ondoren:

a) zein diren baldintza errealeko proben izaera eta helburuak, eta zein eragozpen ekar dezakeen probetan parte hartzeak;

b) zer baldintzatan egingo diren baldintza errealeko probak, eta zenbat denborarako aurreikusi den parte-hartzea;

c) zer eskubide eta berme duten parte hartzearen ondorioz, bereziki azalduta parte hartzeari uko egiteko eskubidea eta baldintza errealeko probak edozein unetan uzteko eskubidea, inolako kalterik jasan gabe eta inolako justifikaziorik eman beharrik gabe;

d) zein diren AA-sistemaren iragarpenak, gomendioak edo erabakiak itzultzeko edo baztertzeko eskatzeko xedapenak;

e) zein den baldintza errealeko proben Batasun osorako identifikazio-zenbaki bakarra, 60.4.c) artikuluaekin bat etorritik, eta nola jar daitezkeen harremanetan hornitzailearekin edo haren legezko ordezkariarekin informazio gehiago lortzeko.

2. Adostasun informatua datatu eta erregistratu egingo da, eta kopia bana emango zaie probaren parte-hartzaileei edo haien legezko ordezkariari.

62. artikulua.— Hornitzaileentzako eta hedapenaren arduradunentzako neurriak, bereziki ETEak —enpresa emergenteak barne—

1. Estatu kideek neurri hauek hartuko dituzte:

a) AArako proba-ingurune arautuetara sartzeko lehenasunezko sarbidea emango diete egoitza sozial bat edo sukurtsal bat Batasunean duten ETEei —enpresa emergenteak barne—, betiere onargarritasun-baldintzak eta hautaketa-irizpideak betetzen badituzte; lehenasunezko sarbideak ez du eragotziko apartatu honetan aipatutakoez bestelako ETEak —enpresa emergenteak barne— AArako proba-ingurune arautura



siempre que también cumplan las condiciones de admisibilidad y los criterios de selección;

b) organizarán actividades de sensibilización y formación específicas sobre la aplicación del presente Reglamento adaptadas a las necesidades de las pymes, incluidas las empresas emergentes, los responsables del despliegue y, en su caso, las autoridades públicas locales;

c) utilizarán canales específicos existentes y establecerán, en su caso, nuevos canales para la comunicación con las pymes, incluidas las empresas emergentes, los responsables del despliegue y otros agentes innovadores, así como, en su caso, las autoridades públicas locales, a fin de proporcionar asesoramiento y responder a las dudas planteadas acerca de la aplicación del presente Reglamento, también en relación con la participación en los espacios controlados de pruebas para la IA;

d) fomentarán la participación de las pymes y otras partes interesadas pertinentes en el proceso de desarrollo de la normalización.

2. Se tendrán en cuenta los intereses y necesidades específicos de los proveedores que sean pymes, incluidas las empresas emergentes, a la hora de fijar las tasas para la evaluación de la conformidad en virtud del artículo 43, y se reducirán dichas tasas en proporción a su tamaño, al tamaño del mercado y a otros indicadores pertinentes.

3. La Oficina de IA adoptará las medidas siguientes:

a) proporcionará modelos normalizados para los ámbitos regulados por el presente Reglamento, tal como especifique el Consejo de IA en su solicitud;

b) desarrollará y mantendrá una plataforma única de información que proporcione información fácil de usar en relación con el presente Reglamento destinada a todos los operadores de la Unión;

c) organizará campañas de comunicación adecuadas para sensibilizar sobre las obligaciones derivadas del presente Reglamento;

d) evaluará y fomentará la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA.

Artículo 63.— Excepciones para operadores específicos

1. Las microempresas en el sentido de la Recomendación 2003/361/CE podrán cumplir determinados elementos del sistema de gestión de la

sartzea, betiere haiek ere onargarritasun-baldintzak eta hautaketa-irizpideak betetzen badituzte;

b) sentsibilizazio- eta prestakuntza-jarduera espezifikoak antolatuko dituzte erregelamendu honen aplikazioari buruz, eta egokitu egingo dituzte ETEen — eta enpresa emergenteen—, hedapenaren arduradunen eta, hala badagokio, tokiko agintaritza publikoen beharrianetara;

c) lehendik dauden kanal espezifikoak erabiliko dituzte eta, hala badagokio, kanal berriak ezarriko dituzte ETEekin —baita enpresa emergenteekin ere—, hedapenaren arduradunekin eta beste eragile berritzaile batzuekin komunikatzeko, bai eta, hala badagokio, tokiko agintaritza publikoekin ere, erregelamendu honen aplikazioari buruz eta AArako proba-ingurune arautuetan parte hartzeari buruz sortzen diren zalantzei erantzuteko eta aholkularitza emateko;

d) ETEek eta beste alderdi interesdun egoki batzuek normalizazioaren garapen-prozesuan parte hartzea sustatuko dute.

2. Erregelamendu honen 43. artikulua araberako adostasuna ebaluatzeko tasak ezartzeko orduan, kontuan hartuko dira ETE diren hornitzaileen interes eta beharrian espezifikoak —enpresa emergenteenak barne—, eta duten tamainaren, merkatuaren tamainaren eta beste adierazle egoki batzuen araberako murriztuko dira tasa horiek.

3. AA-bulegoak neurri hauek hartuko ditu:

a) eredu normalizatuak emango ditu erregelamendu honetan araututako eremuetarako, AA-kontseiluak bere eskaeran zehaztuko duenari jarraituz;

b) informazio-plataforma bakar bat garatu eta mantenduko du, erraz erabiltzeko moduko informazioa emango duena, erregelamendu honi dagokionez, Batasuneko operadore guztientzat;

c) komunikazio-kanpaina egokiak antolatuko ditu erregelamendu honetatik eratorritako betebeharrei buruz sentsibilizatzeko;

d) AA-sistemei dagokionez, kontratazio publikoko prozeduretan jardunbide egokiaren bateratasuna ebaluatu eta sustatuko du.

63. artikulua.— Operadore espezifikoentzako salbuespenak

1. 2003/361/EE Gomendioaren arabera mikroenpresek modu sinplifikatuan bete ahal izango dituzte erregelamendu honen 17. artikulua eskatzen



calidad exigido por el artículo 17 del presente Reglamento de manera simplificada, siempre que no tengan empresas asociadas o empresas vinculadas en el sentido de dicha Recomendación. A tal fin, la Comisión elaborará directrices sobre los elementos del sistema de gestión de la calidad que puedan cumplirse de manera simplificada teniendo en cuenta las necesidades de las microempresas sin que ello afecte al nivel de protección ni a la necesidad de cumplir los requisitos relativos a los sistemas de IA de alto riesgo.

2. El apartado 1 del presente artículo no se interpretará en el sentido de que exime a dichos operadores de cumplir cualquier otro requisito u obligación establecidos en el presente Reglamento, incluidos aquellos que figuran en los artículos 9, 10, 11, 12, 13, 14, 15, 72 y 73.

CAPÍTULO VII

GOBERNANZA

SECCIÓN 1

Gobernanza a escala de la Unión

Artículo 64.— Oficina de IA

1. La Comisión desarrollará los conocimientos especializados y las capacidades de la Unión en el ámbito de la IA mediante la Oficina de IA.
2. Los Estados miembros facilitarán las tareas encomendadas a la Oficina de IA, que están reflejadas en el presente Reglamento.

Artículo 65.— Creación y estructura del Consejo Europeo de Inteligencia Artificial

1. Se crea un Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»).
2. El Consejo de IA estará compuesto de un representante por Estado miembro. El Supervisor Europeo de Protección de Datos participará en calidad de observador. La Oficina de IA también asistirá a las reuniones del Consejo de IA sin participar en las votaciones. El Consejo de IA podrá invitar a otras autoridades, organismos o expertos nacionales y de la Unión a las reuniones en función de cada situación concreta, cuando los temas tratados sean relevantes para ellos.
3. Cada representante será designado por su Estado miembro por un período de tres años, renovable una vez.

duen kalitatea kudeatzeko sistemaren elementu jakin batzuk, betiere ez badute enpresarik elkartuta edo lotuta gomendio horretan azaldutakoaren arabera. Horretarako, Batzordeak gidalerroak prestatuko ditu modu sinplifikatuan bete daitezkeen kalitatea kudeatzeko sistemaren elementuei buruz, mikroenpresen beharrianak kontuan hartuta, baina inolako eraginik izan gabe, ez babes-mailan, ez eta arrisku handiko AA-sistemei buruzko betekizunak betetzeko premian ere.

2. Artikulu honen 1. apartatuarekin ez da interpretatuko operadore horiek salbuetsita daudenik erregelamendu honetan ezarritako beste edozein betekizun edo betebeharrak betetzetik, 9., 10., 11., 12., 13., 14., 15., 72. eta 73. artikuluetan jasotakoak barne.

VII. KAPITULUA

GOBERNANTZA

1. ATALA

Batasunaren mailako gobernantza

64. artikulua.— AA-bulegoa

1. Batzordeak AA-bulegoaren bitartez garatuko ditu Batasunak AAren eremuan dituen ezagutza espezializatuak eta gaitasunak.
2. Estatu kideek erraztu egingo dituzte AA-bulegoari agindutako zereginak —erregelamendu honetan daude jasota—.

65. artikulua.— Adimen Artifizialaren Europako Kontseilua sortzea eta haren egitura zehaztea

1. Adimen Artifizialaren Europako Kontseilua sortzen da (aurrerantzean, «AA-kontseilua»).
2. Estatu kide bakoitzak ordezkari bat izango du AA-kontseiluan. Datuak Babesteko Europako Ikuskatzaileak behatzaile gisa hartuko du parte. AA-bulegoa ere AA-kontseiluaren bileretara joango da, baina ez du bozketetan parte hartuko. AA-kontseiluak beste agintaritzak, organismo edo aditu batzuk —Batasunekoak edo nazionalak— gonbidatu ahal izango ditu bileretara, landu behar den egoera zehatzaren arabera, aztertutako gaiak garrantzitsuak direnean haientzat.
3. Estatu kide bakoitzak hiru urterako izendatuko du bere ordezkaria, eta behin berritu ahal izango da izendapena.



4. Los Estados miembros se asegurarán de que sus representantes en el Consejo de IA:

a) tengan las competencias y los poderes pertinentes en su Estado miembro para poder contribuir activamente al cumplimiento de las funciones del Consejo de IA a que se refiere el artículo 66;

b) sean designados como punto de contacto único respecto del Consejo de IA y, en su caso, teniendo en cuenta las necesidades de los Estados miembros, como punto de contacto único para las partes interesadas;

c) estén facultados para facilitar la coherencia y la coordinación entre las autoridades nacionales competentes en su Estado miembro en relación con la aplicación del presente Reglamento, también mediante la recopilación de datos e información pertinentes para cumplir sus funciones en el Consejo de IA.

5. Los representantes designados de los Estados miembros adoptarán el Reglamento Interno del Consejo de IA por mayoría de dos tercios. El Reglamento Interno establecerá, en particular, los procedimientos para el proceso de selección, la duración del mandato y las especificaciones de las funciones de la presidencia, las modalidades de votación detalladas y la organización de las actividades del Consejo de IA y de sus subgrupos.

6. El Consejo de IA establecerá dos subgrupos permanentes a fin de proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y de notificar a las autoridades cuestiones relacionadas con la vigilancia del mercado y los organismos notificados, respectivamente.

El subgrupo permanente de vigilancia del mercado debe actuar como grupo de cooperación administrativa (ADCO) para el presente Reglamento en el sentido del artículo 30 del Reglamento (UE) 2019/1020.

El Consejo de IA puede establecer otros subgrupos de carácter permanente o temporal, según proceda, para examinar asuntos específicos. Cuando proceda, se podrá invitar a representantes del foro consultivo a que se refiere el artículo 67 a dichos subgrupos o a reuniones específicas de dichos subgrupos en calidad de observadores.

7. El Consejo de IA se organizará y gestionará de manera que se preserve la objetividad e imparcialidad de sus actividades.

8. El Consejo de IA estará presidido por uno de los representantes de los Estados miembros. La Oficina de IA asumirá las labores de secretaría del Consejo de IA, convocará las reuniones a petición de la presidencia y

4. Estatu kideek inguruabar hauek ziurtatuko dituzte AA-kontseiluan dituzten ordezkariak dagokienez:

a) AA-kontseiluaren eginkizunak —66. artikuluan aipatzen dira— betetzen aktiboki lagundu ahal izateko eskumen eta ahalak dituztela beren estatu kidean;

b) AA-kontseiluarekiko harremanetarako gune bakar izendatu direla eta, hala badagokio, estatu kideen beharrak kontuan hartuta, alderdi interesdunentzako harremanetarako gune bakar izendatu direla;

c) ahalmena dutela beren estatu kideko agintaritzak nazional eskudunen artean koherentzia eta koordinazioa errazteko erregelamendu hau aplikatzeari dagokionez, baita AA-kontseiluan dituzten eginkizunak betetzeko beharrezkoak diren datuak eta informazioa biltzeko ere.

5. Estatu kideek izendatutako ordezkarien bi hereneko gehiengoak onartu beharko du AA-kontseiluaren barne-erregelamendua. Barne-erregelamenduak hauek ezarriko ditu bereziki: hautaketa-prozesurako prozedurak, presidentearen agintaldiaren iraupena eta eginkizunen zehaztapenak, bozketa-modalitate zehatzak eta AA-kontseiluaren eta haren azpitaldeen jardueren antolaketa.

6. AA-kontseiluak bi azpitalde iraunkor ezarriko ditu, merkatua zaintzeko agintaritzek eta agintaritzak jakinarazleek lankidetzarako eta trukatutako plataforma bat izan dezaten hurrenez hurren merkatuaren zaintzarekin eta organismo jakinaraziekin lotutako gaiak jorratzeko.

Merkatua zaintzeko azpitalde iraunkorrak administratzioko lankidetzarako talde gisa (ADCO) jardun behar du erregelamendu honetarako, (EB) 2019/1020 Erregelamenduaren 30. artikuluan ezarritakoaren arabera.

AA-kontseiluak beste azpitalde batzuk ezar ditzake, iraunkorrak edo aldi baterakoak, dagokionaren arabera, gai espezifikoak aztertzeko. Hala dagokionean, 67. artikuluan aipatzen den kontsulta-foroko ordezkariak gonbidatu ahal izango dira azpitalde horietara edo azpitalde horien bilera espezifikoetara, behatzaile gisa.

7. AA-kontseilua antolatu eta kudeatzean, zaindu egingo dira bere jardueren objektibotasuna eta inpartzialtasuna.

8. Estatu kideen ordezkarietako bat izango da AA-kontseiluko burua. AA-bulegoak zeregin hauek izango ditu: AA-kontseiluaren idazkaritza-lanak egin, bileretarako deia egin presidenteari eskatuz gero, eta



elaborará el orden del día de conformidad con las funciones del Consejo de IA en virtud del presente Reglamento y de su Reglamento Interno.

Artículo 66.– Funciones del Consejo de IA

El Consejo de IA prestará asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la aplicación coherente y eficaz del presente Reglamento. A tal fin, el Consejo de IA podrá, en particular:

a) contribuir a la coordinación entre las autoridades nacionales competentes responsables de la aplicación del presente Reglamento y, en cooperación con las autoridades de vigilancia del mercado de que se trate y previo acuerdo de estas, apoyar las actividades conjuntas de las autoridades de vigilancia del mercado a que se refiere el artículo 74, apartado 11;

b) recopilar y compartir conocimientos técnicos y reglamentarios y mejores prácticas entre los Estados miembros;

c) ofrecer asesoramiento sobre la aplicación del presente Reglamento, en particular en lo relativo al cumplimiento de las normas sobre modelos de IA de uso general;

d) contribuir a la armonización de las prácticas administrativas en los Estados miembros, también en relación con la exención de los procedimientos de evaluación de la conformidad a que se refiere el artículo 46, el funcionamiento de los espacios controlados de pruebas para la IA y las pruebas en condiciones reales a que se refieren los artículos 57, 59 y 60;

e) previa solicitud de la Comisión o por iniciativa propia, emitir recomendaciones y dictámenes por escrito en relación con cualquier asunto pertinente relacionado con la ejecución del presente Reglamento y con su aplicación coherente y eficaz, por ejemplo:

i) sobre la elaboración y aplicación de códigos de conducta y códigos de buenas prácticas con arreglo al presente Reglamento, así como de las directrices de la Comisión,

ii) sobre la evaluación y revisión del presente Reglamento con arreglo al artículo 112, también en lo que respecta a los informes de incidentes graves a que se refiere el artículo 73, y el funcionamiento de la base de datos de la UE a que se refiere el artículo 71, la preparación de los actos delegados o de ejecución, y en lo que respecta a las posibles adaptaciones del presente Reglamento a los actos legislativos de armonización de la Unión enumerados en el anexo I,

gai-zerrenda prestatu, erregelamendu honen eta barne-erregelamenduaren arabera AA-kontseiluak dituen eginkizunen arabera.

66. artikulua.– AA-kontseiluaren eginkizunak

AA-kontseiluak aholkularitza eta laguntza emango die Batzordeari eta estatu kideei, erregelamendu hau modu koherente eta eraginkorrean aplikatzea errazteko. Horretarako, AA-kontseiluak, bereziki, eginkizun hauek egin ahal izango ditu:

a) erregelamendu hau aplikatzeko ardura duten agintaritza nazional eskudunen arteko koordinazioan lagundu eta, kasuan kasuko merkatua zaintzeko agintaritzekin lankidetzan eta haiekin aldez aurretik adostuta, 74.11 artikuluan aipatzen diren merkatua zaintzeko agintaritzen baterako jarduerak babestu;

b) ezagutza teknikoak eta erregelamenduzkoak eta jardunbide egokienak bildu eta partekatu estatu kideen artean;

c) erregelamendu honen aplikazioari buruzko aholkularitza eskaini, erabilera orokorreko AA-ereduei buruzko arauak betetzeari dagokionez bereziki;

d) Estatu kideetan administrazio-jarduerak harmonizatzen lagundu, baita 46. artikuluan aipatzen diren adostasuna ebaluatzeko prozeduren salbuespenari, AArako proba-ingurune arautuen funtzionamenduari eta baldintza errealeko probei dagokionez ere (57., 59. eta 60. artikuluetan daude zehaztuta);

e) Batzordeak aldez aurretik eskatuta edo bere ekimenez, gomendioak eta irizpenak eman, idatziz, erregelamendu hau betearaztearekin eta haren aplikazio koherente eta eraginkorrearekin lotutako edozein gairi buruz, adibidez:

i) jokabide-kodeak eta jardunbide egokien kodeak erregelamendu honen eta Batzordearen gidalerroen arabera egiteari eta aplikatzeari buruz,

ii) erregelamendu honen ebaluazioari eta berrikuspenari buruz (112. artikuluan arabera), baita gorabehera larriei buruzko txostenei dagokionez ere (73. artikulua), eta EBren datu-basearen funtzionamenduari buruz (71. artikulua), egintza eskuordetuak edo betearazpen-egintzak prestatzeki buruz eta erregelamendu hau I. eranskinean zerrendatutako Batasunaren harmonizazioko lege-egintzetara egokitzeko aukerari buruz,



iii) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el capítulo III, sección 2,

iv) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41,

v) sobre tendencias, como la competitividad de Europa a escala mundial en materia de IA, la adopción de la IA en la Unión y el desarrollo de capacidades digitales,

vi) sobre tendencias en la tipología cambiante de las cadenas de valor de la IA, en particular sobre las implicaciones resultantes en términos de rendición de cuentas,

vii) sobre la posible necesidad de modificar el anexo III de conformidad con el artículo 7 y sobre la posible necesidad de revisar el artículo 5 con arreglo al artículo 112, teniendo en cuenta las pruebas disponibles pertinentes y los últimos avances tecnológicos;

f) apoyar a la Comisión en la promoción de la alfabetización en materia de IA, la sensibilización del público y la comprensión de las ventajas, los riesgos, las salvaguardias y los derechos y obligaciones en relación con la utilización de sistemas de IA;

g) facilitar el desarrollo de criterios comunes y la comprensión compartida entre los operadores del mercado y las autoridades competentes de los conceptos pertinentes previstos en el presente Reglamento, por ejemplo, contribuyendo al desarrollo de parámetros de referencia;

h) cooperar, en su caso, con otras instituciones, órganos y organismos de la Unión, así como con grupos de expertos y redes pertinentes de la Unión, en particular en los ámbitos de la seguridad de los productos, la ciberseguridad, la competencia, los servicios digitales y de medios de comunicación, los servicios financieros, la protección de los consumidores, y la protección de datos y de los derechos fundamentales;

i) contribuir a la cooperación efectiva con las autoridades competentes de terceros países y con organizaciones internacionales;

j) asistir a las autoridades nacionales competentes y a la Comisión en el desarrollo de los conocimientos técnicos y organizativos necesarios para la aplicación del presente Reglamento, por ejemplo, contribuyendo a la evaluación de las necesidades de formación del

iii) III. kapituluko 2. atalean ezarritako betekizunei buruzko zehaztapen teknikoei edo araei buruz,

iv) 40. eta 41. artikuluetan aipatzen diren arau harmonizatuen edo zehaztapen komun en erabilerari buruz,

v) joerei buruz, hala nola Europak AAre arloan mundu-mailan duen lehiakortasuna, AAre ezarpena Batasunean eta gaitasun digitalen garapena,

vi) AAre balio-kateen tipologia aldakorren joerei buruz, bereziki kontuak ematearen ondoriozko inplikazioei buruz,

vii) III. eranskina 7. artikuluen arabera aldatzeko beharri buruz eta 5. artikulua 112. artikuluen arabera berrikusteko beharri buruz, kontuan hartuta eskura dauden froga egokiak eta azken aurrerapen teknologikoak;

f) Batzordeari laguntza eman AAre arloko alfabetatzea sustatzeko, AA-sistemak erabiltzeari dagokionez abantailak, arriskuak, babesak eta eskubideak eta betebeharrak ulertzeko eta herritarrak sentsibilizatzeko;

g) irizpide komunak garatzeko eta merkatuko operadoreen eta agintaritzaren eskudunen artean erregelamendu honetan aurreikusitako kontzeptu egokiak ulertzeko bidea eman, adibidez, erreferentzia-parametroak garatzen lagunduz;

h) hala badagokio, Batasuneko beste instituzio, organo eta organismo batzuekin lankidetzan aritu, bai eta Batasuneko aditu-talde eta sare egokiekin ere, bereziki arlo hauetan: produktuen segurtasuna, zibersegurtasuna, lehia, zerbitzu digitalak eta komunikabideetakoak, finantza-zerbitzuak, kontsumitzaileen babesa eta datuen eta oinarriko eskubideen babesa;

i) hirugarren herrialdeetako agintaritzaren eskudunekin eta nazioarteko antolakundeekin lankidetzan eraginkorra izaten lagunduz;

j) laguntza eman agintaritzaren nazional eskudunei eta Batzordeari erregelamendu hau aplikatzeko beharrezkoak diren ezagutza teknikoak eta antolakuntzakoak garatzen, adibidez, aplikazio horretan parte hartzen duten estatu kideetako langileen prestakuntza-beharrak ebaluatzen lagunduz;



personal de los Estados miembros que participe en dicha aplicación;

k) asistir a la Oficina de IA en el apoyo a las autoridades nacionales competentes para el establecimiento y el desarrollo de espacios controlados de pruebas para la IA, y facilitar la cooperación y el intercambio de información entre espacios controlados de pruebas para la IA;

l) contribuir a la elaboración de documentos de orientación y proporcionar el asesoramiento pertinente al respecto;

m) proporcionar asesoramiento a la Comisión en relación con asuntos internacionales en materia de IA;

n) emitir dictámenes para la Comisión sobre las alertas cualificadas relativas a modelos de IA de uso general;

o) recibir dictámenes de los Estados miembros sobre alertas cualificadas relativas a modelos de IA de uso general y sobre las experiencias y prácticas nacionales en materia de supervisión y ejecución de los sistemas de IA, en particular los sistemas que integran los modelos de IA de uso general.

Artículo 67.– Foro consultivo

1. Se creará un foro consultivo para proporcionar conocimientos técnicos y asesorar al Consejo de IA y a la Comisión, así como para contribuir a las funciones de estos en virtud del presente Reglamento.

2. La composición del foro consultivo representará una selección equilibrada de partes interesadas, incluidos la industria, las empresas emergentes, las pymes, la sociedad civil y el mundo académico. La composición del foro consultivo estará equilibrada en lo que respecta a los intereses comerciales y los no comerciales y, dentro de la categoría de los intereses comerciales, en lo que respecta a las pymes y otras empresas.

3. La Comisión nombrará a los miembros del foro consultivo, de conformidad con los criterios establecidos en el apartado 2, de entre las partes interesadas con conocimientos especializados reconocidos en el ámbito de la IA.

4. El mandato de los miembros del foro consultivo será de dos años y podrá prorrogarse hasta un máximo de cuatro años.

5. La Agencia de los Derechos Fundamentales de la Unión Europea, la Agencia de la Unión Europea para la Ciberseguridad, el Comité Europeo de Normalización

k) laguntza eman AA-bulegoari agintaritza nazional eskudunei AArako proba-ingurune arautuak ezartzen eta garatzen, eta lankidetzeta eta informazio-trukea erraztu AArako proba-ingurune arautuen artean;

l) orientazio-dokumentuak egiten lagundu eta horri buruzko aholkularitza eman;

m) AAren arloko nazioarteko gaiei buruzko aholkularitza eman Batzordeari;

n) erabilera orokorreko AA-ereduei buruzko alerta kualifikatuen inguruko irizpenak eman Batzordearentzat;

o) Estatu kideen irizpenak jaso erabilera orokorreko AA-ereduei buruzko alerta kualifikatuen inguruan eta AA-sistemak gainbegiratzearen eta gauzatzearen arloko esperientzia eta jardunbide nazionalen inguruan, bereziki erabilera orokorreko AA-ereduak osatzen dituzten sistemei dagokienez.

67. artikulua.– Kontsulta-foroa

1. Kontsulta-foro bat sortuko da, ezagutza teknikoak eta aholkularitza emateko AA-kontseiluari eta Batzordeari, bai eta erregelamendu honen arabera dituzten eginkizunetan laguntzeko ere.

2. Kontsulta-foroaosatzean, alderdi interesdunen hautaketa orekatu bat ordezkatzeko da, industria, enpresa emergenteak, ETEak, gizarte zibila eta mundu akademikoa barne. Kontsulta-foroaren osaketa orekatua izango da, halaber, interes komertzialem eta ez-komertzialem dagokienez, eta, interes komertzialen kategoriaren barruan, ETEei eta beste enpresa batzuei dagokienez.

3. AAren eremuan ezagutza espezializatuak dituzten alderdi interesdunen artetik izendatuko ditu Batzordeak kontsulta-foroko kideak, 2. apartatuan ezarritako irizpideei jarraituz.

4. Kontsulta-foroko kideek bi urteko agintaldia izango dute, eta gehienez lau urtera arte luzatu ahal izango da.

5. Oinarritzko Eskubideen Agentzia (ENISA), Zibersegurtasunerako Europar Batasuneko Agentzia, Europako Normalizazio Komitea (CEN), Normalizazio



(CEN), el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) serán miembros permanentes del foro consultivo.

6. El foro consultivo establecerá su reglamento interno. Elegirá dos copresidentes de entre sus miembros, de conformidad con los criterios establecidos en el apartado 2. El mandato de los copresidentes será de dos años, renovable una sola vez.

7. El foro consultivo celebrará reuniones al menos dos veces al año. Podrá invitar a expertos y otras partes interesadas a sus reuniones.

8. El foro consultivo podrá elaborar dictámenes, recomendaciones y contribuciones por escrito a petición del Consejo de IA o de la Comisión.

9. El foro consultivo podrá crear subgrupos permanentes o temporales, según proceda, para examinar cuestiones específicas relacionadas con los objetivos del presente Reglamento.

10. El foro consultivo redactará un informe anual de sus actividades. Dicho informe se pondrá a disposición del público.

Artículo 68.– Grupo de expertos científicos independientes

1. La Comisión adoptará, mediante un acto de ejecución, disposiciones sobre la creación de un grupo de expertos científicos independientes (en lo sucesivo, «grupo de expertos científicos») destinado a apoyar las actividades de garantía del cumplimiento previstas en el presente Reglamento. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. El grupo de expertos científicos estará compuesto por expertos seleccionados por la Comisión sobre la base de conocimientos científicos o técnicos actualizados en el ámbito de la IA necesarios para las funciones establecidas en el apartado 3, y será capaz de demostrar que cumple todas las condiciones siguientes:

a) conocimientos especializados y competencias particulares, y conocimientos científicos o técnicos en el ámbito de la IA;

b) independencia de cualquier proveedor de sistemas de IA o de modelos de IA de uso general;

c) capacidad para llevar a cabo actividades con diligencia, precisión y objetividad.

Elektroteknikoko Europako Komitea (CENELEC) eta Telekomunikazioen Estandarizaziorako Europako Institutua (ETSI) kontsulta-foroko kide iraunkorrak izango dira.

6. Kontsulta-foroak bere barne-erregelamendua ezarriko du. Bi presidentekide hautatuko ditu bertako kideen artean, 2. apartatuan ezarritako irizpideei jarraituz. Presidentekideek bi urteko agintaldia izango dute, eta behin baino ezin izango da berritu.

7. Kontsulta-foroak urtean bitan egingo ditu bilerak, gutxienez. Adituak eta beste alderdi interesdun batzuk gonbidatu ahal izango ditu bileretara.

8. Kontsulta-foroak irizpenak, gomendioak eta ekarpenak egin ahal izango ditu, idatziz, AA-kontseiluak edo Batzordeak eskatuz gero.

9. Kontsulta-foroak azpitalde iraunkorrak edo aldi baterakoak sortu ahal izango ditu, dagokionaren arabera, erregelamendu honen helburuekin lotutako gai espezifikoak aztertzeko.

10. Kontsulta-foroak bere jardueren inguruko txosten bat idatziko du urtero. Txosten hori herritarren eskura jarriko da.

68. artikulua.– Aditu zientifiko independenteen taldea

1. Batzordeak, betearazpen-egintza baten bidez, aditu zientifiko independenteen talde bat (aurrerantzean, «aditu zientifikoen taldea») sortzeari buruzko xedapenak hartuko ditu, erregelamendu honetan aurreikusitakoa betearazteko jarduerak babesteko. Betearazpen-egintza hori 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko da.

2. Batzordeak hautatuko ditu aditu zientifikoen taldeko adituak, 3. apartatuan ezarrita dauden eginkizunetarako beharrezkoak diren AAren eremuko ezagutza zientifiko edo tekniko eguneratuetan oinarrituta. Bada, baldintza hauek guztiak betetzen dituela ziurtatu beharko du taldeak:

a) ezagutza espezializatuak eta konpetentzia partikularrak, eta ezagutza zientifiko edo teknikoak izatea AAren eremuan;

b) loturarik ez izatea AA-sistemen edo erabilera orokorreko AA-ereduen hornitzailearen batekin;

c) jarduerak arduraz, zehaztasunez eta objektibotasunez egiteko gaitasuna izatea.



La Comisión, en consulta con el Consejo de IA, determinará el número de expertos del grupo de acuerdo con las necesidades requeridas y garantizará una representación geográfica y de género justa.

3. El grupo de expertos científicos asesorará y apoyará a la Oficina de IA, en particular en lo que respecta a las siguientes funciones:

a) apoyar la aplicación y el cumplimiento del presente Reglamento en lo que respecta a los sistemas y modelos de IA de uso general, en particular:

i) alertando a la Oficina de IA de los posibles riesgos sistémicos a escala de la Unión de modelos de IA de uso general, de conformidad con el artículo 90,

ii) contribuyendo al desarrollo de herramientas y metodologías para evaluar las capacidades de los sistemas y modelos de IA de uso general, también a través de parámetros de referencia,

iii) asesorando sobre la clasificación de modelos de IA de uso general con riesgo sistémico,

iv) asesorando sobre la clasificación de diversos sistemas y modelos de IA de uso general,

v) contribuyendo al desarrollo de herramientas y modelos;

b) apoyar la labor de las autoridades de vigilancia del mercado, a petición de estas;

c) apoyar las actividades transfronterizas de vigilancia del mercado a que se refiere el artículo 74, apartado 11, sin perjuicio de los poderes de las autoridades de vigilancia del mercado;

d) apoyar a la Oficina de IA en el ejercicio de sus funciones en el contexto del procedimiento de salvaguardia de la Unión con arreglo al artículo 81.

4. Los expertos del grupo desempeñarán sus funciones con imparcialidad y objetividad y garantizarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades. No solicitarán ni aceptarán instrucciones de nadie en el ejercicio de sus funciones previstas en el apartado 3. Cada experto cumplimentará una declaración de intereses que se hará pública. La Oficina de IA establecerá sistemas y procedimientos para gestionar y prevenir activamente los posibles conflictos de intereses.

Batzordeak, AA-kontseiluari kontsulta eginda, beharizanen arabera erabakiko du zenbat aditu behar dituen taldeak, eta ordezkaritza zuzena bermatuko du geografiari eta generoari dagokienez.

3. Aditu zientifikoen taldeak aholkularitza eta laguntza emango dio AA-bulegoari, bereziki eginkizun hauei dagokienez:

a) erregelamendu hau aplikatzen eta betetzen laguntzea, erabilera orokorreko AA-ereduei eta sistemei dagokienez, bereziki:

i) AA-bulegoari alertak emanez erabilera orokorreko AA-ereduek Batasunaren mailan ekar ditzaketen arrisku sistemikoei buruz, 90. artikuluaaren arabera,

ii) erabilera orokorreko AA-ereduen eta sistemen gaitasunak ebaluatzeko tresnak eta metodologiak garatzen lagunduz, baita erreferentzia-parametroak erabiliz ere,

iii) arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen sailkapenari buruzko aholkularitza emanez,

iv) erabilera orokorreko AA-eredu eta sistema ezberdinen sailkapenari buruzko aholkuak emanez,

v) tresnak eta ereduak garatzen lagunduz;

b) merkatua zaintzeko agintaritzen lana babestea, haiek eskatuz gero;

c) merkatua zaintzeko mugaz gaindiko jarduerak babestea (74.11 artikuluan daude zehaztuta), hargatik eragotzi gabe merkatua zaintzeko agintaritzen ahalak;

d) AA-bulegoari laguntzea Batasunaren babes-prozeduraren testuinguruan dituen eginkizunak betetzen, 81. artikuluaaren arabera.

4. Taldeko adituek inpartzialtasunez eta objektibotasunez beteko dituzte beren eginkizunak, eta bermatu egingo dute konfidentzialki erabiliko dituztela beren eginkizunak eta jarduerak bete bitartean eskuratutako informazioa eta datuak. Ez dute inoren jarraibiderik eskatuko edo onartuko 3. apartatuan aurreikusitako eginkizunak betetzeko. Aditu bakoitzak interesen adierazpen bat beteko du, eta herritarren eskura jarriko da. AA-bulegoak sistemak eta prozedurak ezarriko ditu sor litezkeen interes-gatazkak kudeatzeko eta prebenitzeko.



5. El acto de ejecución a que se refiere el apartado 1 incluirá disposiciones sobre las condiciones, los procedimientos y las disposiciones detalladas para que el grupo de expertos científicos y sus miembros emitan alertas y soliciten la asistencia de la Oficina de IA para el desempeño de las funciones del grupo de expertos científicos.

Artículo 69.— Acceso a expertos por parte de los Estados miembros

1. Los Estados miembros podrán recurrir a expertos del grupo de expertos científicos para que apoyen sus actividades de garantía del cumplimiento previstas en el presente Reglamento.

2. Se podrá exigir a los Estados miembros que paguen tasas por el asesoramiento y el apoyo prestado por los expertos. La estructura y el importe de las tasas, así como la escala y la estructura de los costes recuperables, se establecerán en el acto de ejecución a que se refiere el artículo 68, apartado 1, teniendo en cuenta los objetivos de la correcta aplicación del presente Reglamento, la rentabilidad y la necesidad de garantizar que todos los Estados miembros tengan un acceso efectivo a los expertos.

3. La Comisión facilitará el acceso oportuno de los Estados miembros a los expertos, según sea necesario, y garantizará que la combinación de las actividades de apoyo llevadas a cabo por las estructuras de apoyo a los ensayos de IA de la Unión con arreglo al artículo 84 y por expertos con arreglo al presente artículo se organice de manera eficiente y ofrezca el mayor valor añadido posible.

SECCIÓN 2

Autoridades nacionales competentes

Artículo 70.— Designación de las autoridades nacionales competentes y de los puntos de contacto único

1. Cada Estado miembro establecerá o designará al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes a los efectos del presente Reglamento. Dichas autoridades nacionales competentes ejercerán sus poderes de manera independiente, imparcial y sin sesgos, a fin de preservar la objetividad de sus actividades y funciones y de garantizar la aplicación y ejecución del presente Reglamento. Los miembros de dichas autoridades se abstendrán de todo acto incompatible con sus funciones. Siempre que se respeten esos principios, tales actividades y funciones podrán ser realizadas por

5. Articulo honen 1. apartatuan aipatzen den betearazpen-egintzak xedapenak jasoko ditu baldintza, prozedura eta xedapen zehatzei buruz, aditu zientifikoen taldeak eta haren kideek alertak egin eta AA-bulegoaren laguntza eska dezaten aditu zientifikoen taldearen eginkizunak betetzeko.

69. artikulua.— Estatu kideek adituengana jotzea

1. Estatu kideek aditu zientifikoen taldeko adituengana jo ahal izango dute erregelamendu honetan aurreikusitakoa betearazteko jarduerak babes ditzaten.

2. Adituek emandako aholkularitza eta laguntza ordaintzeko tasak ordain ditzatela eskatu ahal izango zaie estatu kideei. Erregelamendu honen 68.1 artikuluan aipatutako betearazpen-egintzan ezarriko dira tasen egitura eta zenbatekoa, bai eta berreskura daitezkeen kostuen eskala eta egitura ere, kontuan hartuta erregelamendu hau behar bezala aplikatzeko helburuak, errentagarritasuna eta estatu kide guztiek adituengana jotzeko aukera izango dutela bermatzeko beharra.

3. Beharrezkoa denean, Batzordeak erraztu egingo du estatu kideek adituengana jotzea, eta bermatu egingo du modu eraginkorrean antolatzen dela Batasuneko AA-saiakuntzei sostengua emateko egiturek —84. artikuluaaren arabera— eta adituek —artikulu honen arabera— egindako babes-jardueren konbinazioa, eta ahalik eta balio erantsi handiena eskaintzen duela.

2. ATALA

Agintaritza nazional eskudunak

70. artikulua.— Agintaritza nazional eskudunak eta harremanetarako gune bakarrak izendatzea

1. Estatu kide bakoitzak gutxienez agintaritza jakinarazle bat eta merkatua zaintzeko agintaritza bat ezarri edo izendatuko ditu, agintaritza nazional eskudun izateko erregelamendu honen ondorioetarako. Agintaritza nazional eskudun horiek modu independente eta inpartzialean eta alborapenik gabe baliatuko dituzte beren ahalak, beren jardueren eta eginkizunen objektibotasuna babesteko eta erregelamendu honen aplikazioa eta betearazpena bermatzeko. Agintaritza horietako kideek ez dute parte hartuko beren eginkizunekin bateraezina den ezein egintzatan. Printzipio horiek errespetatuz gero, izendatutako agintaritza batek edo batzuek egin ahal izango dituzte



una o varias autoridades designadas, de conformidad con las necesidades organizativas del Estado miembro.

2. Los Estados miembros comunicarán a la Comisión la identidad de las autoridades notificantes y de las autoridades de vigilancia del mercado y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. Los Estados miembros pondrán a disposición del público, por medios de comunicación electrónica, información sobre la forma de contactar con las autoridades competentes y los puntos de contacto únicos a más tardar el 2 de agosto de 2025. Los Estados miembros designarán una autoridad de vigilancia del mercado que actúe como punto de contacto único para el presente Reglamento y notificarán a la Comisión la identidad de dicho punto. La Comisión pondrá a disposición del público la lista de puntos de contacto únicos.

3. Los Estados miembros garantizarán que sus autoridades nacionales competentes dispongan de recursos técnicos, financieros y humanos adecuados, y de infraestructuras para el desempeño de sus funciones de manera efectiva con arreglo al presente Reglamento. En concreto, las autoridades nacionales competentes dispondrán permanentemente de suficiente personal cuyas competencias y conocimientos técnicos incluirán un conocimiento profundo de las tecnologías de IA, datos y computación de datos; la protección de los datos personales, la ciberseguridad, los riesgos para los derechos fundamentales, la salud y la seguridad, y conocimientos acerca de las normas y requisitos legales vigentes. Los Estados miembros evaluarán y, en caso necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado.

4. Las autoridades nacionales competentes adoptarán las medidas adecuadas para garantizar un nivel adecuado de ciberseguridad.

5. En el desempeño de sus funciones, las autoridades nacionales competentes actuarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

6. A más tardar el 2 de agosto de 2025 y cada dos años a partir de entonces, los Estados miembros presentarán a la Comisión un informe acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes, que incluirá una evaluación de su idoneidad. La Comisión remitirá dicha información al Consejo de IA para que mantenga un debate sobre ella y, en su caso, formule recomendaciones.

jarduera eta eginkizun horiek, estatu kidearen antolamendu-beharrei jarraituz.

2. Estatu kideek Batzordeari jakinaraziko diote zein diren agintaritza jakinarazleak eta merkatua zaintzeko agintaritzak, eta zein eginkizun duten; halaber, ondoren aldaketaren bat egonez gero, horren berri emango zaio Batzordeari. Estatu kideek, komunikazio elektronikoen bidez, herritarren eskura jarriko dute agintaritza eskudunekin eta harremanetarako gun e bakarrekin harremanetan jartzeko moduari buruzko informazioa, 2025eko abuztuaren 2a baino lehen. Estatu kideek merkatua zaintzeko agintaritza bat izendatuko dute harremanetarako gun e bakar gisa jardun dezan erregelamendu honen ondoretarako, eta Batzordeari jakinaraziko diote gun e hori zein den. Batzordeak herritarren eskura jarriko du harremanetarako gun e bakarren zerrenda.

3. Estatu kideek bermatu egingo dute beren agintaritza nazional eskudunek badituztela baliabide tekniko, finantza-baliabide eta giza baliabide egokiak, bai eta beren eginkizunak eraginkortasunez betetzeko azpiegiturak ere, erregelamendu honen arabera. Zehazki, agintaritza nazional eskudunek behar adina langile izango dituzte etengabe, eta langile horien konpetentziek eta ezagutza teknikoek hauek barne hartuko dituzte: AA-teknologiak, datuen eta datuen konputazioaren ezagutza sakona; datu pertsonalen babesa, zibersegurtasuna, oinarriko eskubideetarako arriskuak, osasuna eta segurtasuna, eta indarrean dauden legezko arau eta betekizunei buruzko ezagutzak. Estatu kideek urtero ebaluatuko eta, behar izanez gero, eguneratuko dituzte apartatu honetan aipatzen diren konpetentzien eta baliabideen arloko betekizunak.

4. Agintaritza nazional eskudunek neurri egokiak hartuko dituzte zibersegurtasun-maila egokia bermatzeko.

5. Agintaritza nazional eskudunek, beren eginkizunak betetzean, 78. artikuluan ezarritako konfidentzialtasun-betebeharren arabera jardungo dute.

6. Beranduenez 2025eko abuztuaren 2an eta handik aurrera bi urtean behin, agintaritza nazional eskudunen finantza-baliabideen eta giza baliabideen egoerari buruzko txosten bat aurkeztuko diote estatu kideek Batzordeari, eta egokitasunaren inguruko ebaluazioa ere jasoko du txosten horrek. Batzordeak AA-kontseiluari bidaliko dio informazio hori, hari buruzko eztabaida izan dezan eta, hala badagokio, gomendioak egin ditzan.



7. La Comisión facilitará el intercambio de experiencias entre las autoridades nacionales competentes.

8. Las autoridades nacionales competentes podrán proporcionar orientaciones y asesoramiento sobre la aplicación del presente Reglamento, en particular a las pymes —incluidas las empresas emergentes—, teniendo en cuenta las orientaciones y el asesoramiento del Consejo de IA y de la Comisión, según proceda. Siempre que una autoridad nacional competente tenga la intención de proporcionar orientaciones y asesoramiento en relación con un sistema de IA en ámbitos regulados por otros actos del Derecho de la Unión, se consultará a las autoridades nacionales competentes con arreglo a lo dispuesto en dichos actos, según proceda.

9. Cuando las instituciones, órganos y organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como autoridad competente para su supervisión.

CAPÍTULO VIII

BASE DE DATOS DE LA UE PARA SISTEMAS DE IA DE ALTO RIESGO

Artículo 71.— Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el ANEXO III

1. La Comisión, en colaboración con los Estados miembros, creará y mantendrá una base de datos de la UE que contendrá la información mencionada en los apartados 2 y 3 del presente artículo en relación con los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, que estén registrados con arreglo a los artículos 49 y 60 y los sistemas de IA que no se consideren de alto riesgo en virtud del artículo 6, apartado 3, y que estén registrados con arreglo al artículo 6, apartado 4, y al artículo 49. La Comisión consultará a los expertos pertinentes a la hora de fijar las especificaciones funcionales de dicha base de datos y al Consejo de IA a la hora de actualizarlas.

2. Los datos enumerados en el anexo VIII, secciones A y B, serán introducidos en la base de datos de la UE por el proveedor o, en su caso, por el representante autorizado.

3. Los datos enumerados en el anexo VIII, sección C, serán introducidos en la base de datos de la UE por el responsable del despliegue que sea una autoridad pública, órgano u organismo, o actúe en su nombre, de conformidad con el artículo 49, apartados 3 y 4.

7. Batzordeak erraztu egingo du agintaritza nazional eskudunen artean esperientzia trukatzeara.

8. Agintaritza nazional eskudunek erregelamendu honen aplikazioari buruzko orientabideak eta aholkularitza eman ahal izango dituzte, bereziki ETEei —enpresa emergenteak barne—, kontuan hartuta AA-kontseiluaren eta Batzordearen orientabideak eta aholkularitza, dagokionaren arabera. Agintaritza nazional eskudun batek AA-sistema baten inguruko orientabideak eta aholkuak eman nahi baditu Batasuneko zuzenbideko beste egintza batzuek araututako eremuetan, kontsulta egingo zaie agintaritza nazional eskudunei egintza horietan xedatutakoari jarraituz, dagokionaren arabera.

9. Batasuneko instituzio, organo eta organismoak erregelamendu honen aplikazio-eremuan sartzen direnean, Datuak Babesteko Europako Ikuskatzaileak gainbegiratze-lanetarako agintaritza eskudun gisa jardungo du.

VIII. KAPITULUA

EB-REN DATU BASEA, ARRISKU HANDIKO AA-SISTEMETARAKO

71. artikulua.— EBren datu-basea III. ERANSKINEAN zerrendatutako arrisku handiko AA-sistemetarako

1. Batzordeak, estatu kideekin lankidetzan, EBren datu-base bat sortu eta mantenduko du. Datu-base horrek artikulua honetako 2. eta 3. apartatueta aipatutako informazioa bilduko du, 6.2 artikuluan aipatutako arrisku handiko AA-sistemei dagokienez, baldin eta 49. eta 60. artikuluen arabera erregistratuta badaude, eta 6.3 artikuluen arabera arrisku handikotzat jotzen ez diren AA-sistemei dagokienez, baldin eta 6.4 eta 49. artikuluen arabera erregistratuta badaude. Batzordeak, datu-base horren zehaztapen funtzionalak finkatzerakoan, kontsulta egingo die dagokien adituei, eta, zehaztapenok eguneratzerakoan, AA-kontseiluari.

2. VIII. eranskinetako A eta B ataletan zerrendatutako datuak hornitzaileak edo, hala badagokio, ordezkari baimenduak sartuko ditu EBren datu-basean.

3. VIII. eranskinetako C atalean zerrendatutako datuak hedapenaren arduradunak sartuko ditu EBren datu-basean, baldin eta agintaritza publikoa, organoa edo organismoa bada, edo haren izenean jarduten badu, 49. artikuluko 3. eta 4. apartatuen arabera.



4. A excepción de la sección a que se refieren el artículo 49, apartado 4, y el artículo 60, apartado 4, letra c), la información presente en la base de datos de la UE y registrada de conformidad con lo dispuesto en el artículo 49 será accesible y estará a disposición del público de manera sencilla. Debe ser fácil navegar por la información y esta ha de ser legible por máquina. Únicamente podrán acceder a la información registrada de conformidad con el artículo 60 las autoridades de vigilancia de mercado y la Comisión, a menos que el proveedor potencial o el proveedor hayan dado su consentimiento a que la información también esté accesible para el público.

5. La base de datos de la UE únicamente contendrá datos personales en la medida en que sean necesarios para la recogida y el tratamiento de información de conformidad con el presente Reglamento. Dicha información incluirá los nombres y datos de contacto de las personas físicas responsables del registro de sistema y que cuenten con autoridad legal para representar al proveedor o al responsable del despliegue, según proceda.

6. La Comisión será la responsable del tratamiento de la base de datos de la UE, y proporcionará apoyo técnico y administrativo adecuado a los proveedores, proveedores potenciales y responsables del despliegue. La base de datos de la UE cumplirá los requisitos de accesibilidad aplicables.

CAPÍTULO IX

VIGILANCIA POSCOMERCIALIZACIÓN, INTERCAMBIO DE INFORMACIÓN Y VIGILANCIA DEL MERCADO

SECCIÓN 1

Vigilancia poscomercialización

Artículo 72.– Vigilancia poscomercialización por parte de los proveedores y plan de vigilancia poscomercialización para sistemas de IA de alto riesgo

1. Los proveedores establecerán y documentarán un sistema de vigilancia poscomercialización de forma proporcionada a la naturaleza de las tecnologías de IA y a los riesgos de los sistemas de IA de alto riesgo.

2. El sistema de vigilancia poscomercialización recopilará, documentará y analizará de manera activa y sistemática los datos pertinentes que pueden facilitar los responsables del despliegue o que pueden recopilarse a través de otras fuentes sobre el funcionamiento de los sistemas de IA de alto riesgo durante toda su vida útil, y que permiten al proveedor evaluar el cumplimiento

4. Erregelamendu honen 49.4 artikuluan eta 60.4.c) artikuluan aipatzen den atala izan ezik, EBren datu-basean dagoen eta 49. artikuluan xedatutakoaren arabera erregistratuta dagoen informazioa irisgarria izango da, eta herritarrek erraz eskuratzeko moduan egongo da. Erraza izan behar du informazioan zehar nabigatzea, eta makinek irakurtzeko modukoa izan behar du. Merkatua zaintzeko agintaritzek eta Batzordeak soilik eskuratu ahal izango dute 60. artikuluan arabera erregistratutako informazioa, salbu eta hornitzaile potentzialak edo hornitzaileak baimena eman badu informazio hori herritarrentzat ere eskuragarri egon dadin.

5. EBren datu-baseak erregelamendu honen arabera informazioa biltzeko eta tratatzeko beharrezkoak diren heinean soilik izango ditu datu pertsonalak. Informazio horren barruan sartuko dira sistemaren erregistroaz arduratzen diren eta, dagokionaren arabera, hornitzailea edo hedapenaren arduraduna ordezkatzeko legezko aginpidea duten pertsona fisikoen izenak eta harremanetarako datuak.

6. Batzordea izango da EBren datu-basearen tratamenduaren arduraduna, eta laguntza tekniko eta administratibo egokia emango die hornitzaileei, hornitzaile potentzialei eta hedapenaren arduradunei. EBren datu-baseak aplikatu behar diren irisgarritasun-betekizunak beteko ditu.

IX. KAPITULUA

MERKATURATU OSTEKO ZAINZA, INFORMAZIO- TRUKEA ETA MERKATUAREN ZAINZA

1. ATALA

Merkaturatu osteko zaintza

72. artikulua.– Hornitzaileen merkaturatu osteko zaintza eta merkaturatu osteko zaintza-plana arrisku handiko AA-sistemetarako

1. Hornitzaileek merkaturatu osteko zaintza-sistema bat ezarri eta dokumentatuko dute, eta sistema hori proportzionala izango da AA-teknologiaren izaerarekiko eta arrisku handiko AA-sistemen arriskuekiko.

2. Merkaturatu osteko zaintza-sistemak modu aktibo eta sistematikoan bildu, dokumentatu eta aztertuko ditu arrisku handiko AA-sistemen funtzionamenduari buruz, haien balio-bizitza osoan, hedapenaren arduradunek eman ditzaketen edo beste iturri batzuen bidez bildu daitezkeen datu esanguratsuak. Datu horiek aukera ematen diote hornitzaileari AA-sistemek III. kapituluko 2.



permanente de los requisitos establecidos en el capítulo III, sección 2, por parte de los sistemas de IA. Cuando proceda, la vigilancia poscomercialización incluirá un análisis de la interacción con otros sistemas de IA. Esta obligación no comprenderá los datos operativos sensibles de los responsables del despliegue que sean autoridades garantes del cumplimiento del Derecho.

3. El sistema de vigilancia poscomercialización se basará en un plan de vigilancia poscomercialización. El plan de vigilancia poscomercialización formará parte de la documentación técnica a que se refiere el anexo IV. La Comisión adoptará un acto de ejecución en el que se establecerán disposiciones detalladas que constituyan un modelo para el plan de vigilancia poscomercialización y la lista de elementos que deberán incluirse en él a más tardar el 2 de febrero de 2026. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

4. En el caso de los sistemas de IA de alto riesgo regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando ya se hayan establecido un sistema y un plan de vigilancia poscomercialización con arreglo a dichos actos, con el fin de garantizar la coherencia, evitar duplicidades y reducir al mínimo las cargas adicionales, los proveedores podrán optar por integrar, según proceda, los elementos necesarios descritos en los apartados 1, 2 y 3, utilizando el modelo a que se refiere el apartado 3, en los sistemas y planes que ya existan en virtud de dicha legislación, siempre que alcance un nivel de protección equivalente.

El párrafo primero del presente apartado también se aplicará a los sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, introducidos en el mercado o puestos en servicio por entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos en virtud del Derecho de la Unión en materia de servicios financieros.

SECCIÓN 2

Intercambio de información sobre incidentes graves

Artículo 73.— Notificación de incidentes graves

1. Los proveedores de sistemas de IA de alto riesgo introducidos en el mercado de la Unión notificarán cualquier incidente grave a las autoridades de vigilancia del mercado de los Estados miembros en los que se haya producido dicho incidente.

2. La notificación a que se refiere el apartado 1 se efectuará inmediatamente después de que el proveedor

atalean ezarritako betekizunak etengabe betetzen dituzten ebaluatzeko. Hala dagokionean, beste AA-sistema batzuekiko interakzioa ere aztertuko du merkaturatu osteko zaintzak. Betebehar horretan ez dira sartuko zuzenbidea betearazteko agintaritzaren diren hedapenaren arduradunen bereziki babestutako datu operatiboak.

3. Merkaturatu osteko zaintza-sistemak merkaturatu osteko zaintza-plan bat izango du oinarri. Merkaturatu osteko zaintza-plana IV. eranskinean aipatzen den dokumentazio teknikoaren parte izango da. Batzordeak betearazpen-egintza bat hartuko du. Egintza horretan, xedapen zehatzak ezarriko dira merkaturatu osteko zaintza-planerako eredu bat osatzeko eta, gainera, beranduenez 2026ko otsailaren 2an plan horretan sartu beharko diren elementuen zerrenda bat ere egingo da. Beteazpen-egintza hori 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko da.

4. Batasunaren harmonizazioko lege-egintzek —I. eranskineko A atalean daude zerrendatuta— arautzen dituzten arrisku handiko AA-sistemen kasuan —dagoeneko ezarri direnean, egintza horien arabera, merkaturatu osteko zaintza-sistema eta -plana—, koherentzia bermatu, bikoiztasunak saihestu eta karga gehigarriak ahalik eta gehien murrizteko helburuz, hornitzaileek erabaki ahal izango dute, dagokionaren arabera, 1., 2. eta 3. apartatuetan deskribatutako beharrezko elementuak integratzea legeria horren arabera lehendik dauden sistema eta planetan, 3. apartatuan aipatutako ereduak erabiliz, betiere babes-maila baliokidea lortzen badute.

Apartatu honetako lehenengo paragrafoa III. eranskineko 5. puntuan aipatzen diren arrisku handiko AA-sistemei ere aplikatuko zaie, baldin eta Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera ezarritako barne-gobernantza, -sistema edo -prozesuei buruzko betekizunak bete behar dituzten finantza-entitateek jarri badituzte merkaturatutako edo ipini badituzte zerbitzuan.

2. ATALA

Gorabehera larriei buruzko informazio-trukea

73. artikulua.— Gorabehera larriak jakinaraztea

1. Batasuneko merkaturatutako jarri diren arrisku handiko AA-sistemen hornitzaileek gorabehera larri oro jakinaraziko diete gorabehera hori gertatu den estatu kideetako merkaturatutako zaintzeko agintaritzei.

2. Hornitzaileak AA-sistemaren eta gorabehera larriaren artean kausazko erlazio bat dagoela edo egon



haya establecido un vínculo causal entre el sistema de IA y el incidente grave o la probabilidad razonable de que exista dicho vínculo y, en cualquier caso, a más tardar quince días después de que el proveedor o, en su caso, el responsable del despliegue, tengan conocimiento del incidente grave.

El plazo para la notificación a que se refiere el párrafo primero tendrá en cuenta la magnitud del incidente grave.

3. No obstante lo dispuesto en el apartado 2 del presente artículo, en caso de una infracción generalizada o de un incidente grave tal como se define en el artículo 3, punto 49, letra b), la notificación a que se refiere el apartado 1 del presente artículo se realizará de manera inmediata y a más tardar dos días después de que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente.

4. No obstante lo dispuesto en el apartado 2, en caso de fallecimiento de una persona, la notificación se efectuará de manera inmediata después de que el proveedor o el responsable del despliegue haya establecido —o tan pronto como sospeche— una relación causal entre el sistema de IA de alto riesgo y el incidente grave, en un plazo no superior a diez días a contar de la fecha en la que el proveedor o, en su caso, el responsable del despliegue tenga conocimiento del incidente grave.

5. Cuando sea necesario para garantizar la notificación en tiempo oportuno, el proveedor o, en su caso, el responsable del despliegue podrá presentar inicialmente una notificación incompleta, seguida de una notificación completa.

6. Después de notificar un incidente grave con arreglo al apartado 1, el proveedor realizará sin demora las investigaciones necesarias en relación con el incidente grave y el sistema de IA afectado. Esto incluirá una evaluación de riesgos del incidente y las medidas correctoras.

El proveedor cooperará con las autoridades competentes y, en su caso, con el organismo notificado afectado durante las investigaciones a que se refiere el párrafo primero, y no emprenderá acción alguna que suponga la modificación del sistema de IA afectado de un modo que pueda repercutir en cualquier evaluación posterior de las causas del incidente sin haber informado antes de dicha acción a las autoridades competentes.

7. Tras la recepción de una notificación relativa a un incidente grave a que se refiere el artículo 3, punto 49, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos

litekeela ezarri bezain laster egingo da 1. apartatuan aipatzen den jakinarazpena, eta, nolanahi ere, hornitzaileak edo, hala badagokio, hedapenaren arduradunak gorabehera larriaren berri izan eta gehienez ere hamabost eguneko epean.

Lehenengo paragrafoan aipatzen den jakinarazpen-epea gorabehera larriaren garrantziaren araberakoa izango da.

3. Artikulu honen 2. apartatuan xedatutakoa gorabehera, hedadura handiko arau-hauste bat edo gorabehera larri bat gertatzen bada —3.49.b) artikuluan definitutakoaren arabera— berehala egin beharko da artikulu honen 1. apartatuan aipatzen den jakinarazpena, eta, gehienez ere, hornitzaileak edo, hala badagokio, hedapenaren arduradunak gorabeheraren berri izan eta bi eguneko epean.

4. Artikulu honen 2. apartatuan xedatutakoa gorabehera, pertsona bat hiltzen bada, hornitzaileak edo hedapenaren arduradunak arrisku handiko AA-sistemaren eta gorabehera larriaren artean kausazko erlazio bat ezarri —edo horren susmoa izan— bezain laster egingo da jakinarazpena, eta, gehienez hamar eguneko epean, hornitzaileak edo, hala badagokio, hedapenaren arduradunak gorabehera larriaren berri izaten duenetik aurrera.

5. Baldin eta jakinarazpena garaiz egingo dela bermatzeko beharrezkoa bada, hornitzaileak edo, hala badagokio, hedapenaren arduradunak jakinarazpen osatugabe bat aurkeztu ahal izango du hasieran, eta, ondoren, jakinarazpen osoa.

6. Artikulu honen 1. apartatuari jarraikiz gorabehera larri bat jakinarazi ondoren, hornitzaileak atzerapenik gabe egingo ditu gorabehera larriari eta ukitutako AA-sistemari buruzko bidezko ikerketak. Ikerketa horien barruan egongo dira gorabeheraren arriskuen ebaluazioa eta neurri zuzentzaileak.

Hornitzaileak lankidetzan jardungo du agintaritza eskudunekin eta, hala badagokio, ukitutako organismo jakinaraziarekin lehenengo paragrafoan aipatzen diren ikerketak egin bitartean, eta ez du abiaraziko ukitutako AA-sistema aldatzea dakarren inolako ekintzarik baldin eta eragina izan badezake gorabeheraren arrazoiei buruzko ondorengo edozein ebaluaziotan, ekintza horren berri agintaritza eskudunei aldeztu aurretik eman ez badie.

7. Erregelamendu honen 3.49.c) artikuluan aipatzen den gorabehera larri bati buruzko jakinarazpena jaso ondoren, merkatua zaintzeko agintaritza egokiak informazioa emango die 77.1 artikuluan aipatzen diren



nacionales a que se refiere el artículo 77, apartado 1. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo. Dichas orientaciones se publicarán a más tardar el 2 de agosto de 2025 y se evaluarán periódicamente.

8. La autoridad de vigilancia del mercado adoptará medidas adecuadas tal como se establece en el artículo 19 del Reglamento (UE) 2019/1020, en un plazo de siete días a partir de la fecha en que reciba la notificación a que se refiere el apartado 1 del presente artículo, y seguirá los procedimientos de notificación previstos en dicho Reglamento.

9. En el caso de los sistemas de IA de alto riesgo a que se refiere el anexo III, introducidos en el mercado o puestos en servicio por proveedores que estén sujetos a instrumentos legislativos de la Unión por los que se establezcan obligaciones de información equivalentes a las establecidas en el presente Reglamento, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c).

10. En el caso de los sistemas de IA de alto riesgo que sean componentes de seguridad de dispositivos, o que en sí mismos sean dispositivos, regulados por los Reglamento (UE) 2017/745 y (UE) 2017/746, la notificación de incidentes graves se limitará a los mencionados en el artículo 3, punto 49, letra c), del presente Reglamento, y se hará a la autoridad nacional competente elegida para tal fin por los Estados miembros en los que se haya producido el incidente.

11. Las autoridades nacionales competentes informarán de inmediato a la Comisión de todo incidente grave, independientemente de han adoptado medidas al respecto, de conformidad con el artículo 20 del Reglamento (UE) 2019/1020.

SECCIÓN 3

Garantía del cumplimiento

Artículo 74.— Vigilancia del mercado y control de los sistemas de IA en el mercado de la Unión

1. El Reglamento (UE) 2019/1020 se aplicará a los sistemas de IA regulados por el presente Reglamento. A efectos de garantía del cumplimiento efectivo del presente Reglamento:

a) se entenderá que toda referencia a un operador económico con arreglo al Reglamento (UE) 2019/1020 incluye a todos los operadores mencionados en el artículo 2, apartado 1, del presente Reglamento;

agintaritza edo organismo publiko nazionalai. Batzordeak orientabide espezifikoak egingo ditu artikulua honetako 1. apartatuan ezarritako betebeharrak betetzea errazteko. Orientabide horiek 2025eko abuztuaren 2an argitaratuko dira berandueze, eta aldizka ebaluatuko dira.

8. Merkatua zaintzeko agintaritzak neurri egokiak hartuko ditu —(EB) 2019/1020 Erregelamenduaren 19. artikuluan ezartzen den bezala—, artikulua honen 1. apartatuan aipatzen den jakinarazpena jaso eta zazpi eguneko epean, eta erregelamendu horretan aurreikusitako jakinarazpen-prozedurei jarraituko die.

9. III. eranskinean aipatzen diren arrisku handiko AA-sistemen kasuan, erregelamendu honetan ezarritako informazio-betebeharren baliokideak ezartzen dituzten Batasuneko lege-tresnen mende dauden hornitzaileek merkatuan jarri edo zerbitzuan ipinitakoak badira, 3.49.c) artikuluan aipatutakoetara mugatuko da gorabehera larrien jakinarazpena.

10. Gailuen segurtasun-osagaiak edo gailuak eurak diren arrisku handiko AA-sistemen kasuan —(EB) 2017/745 Erregelamenduan eta (EB) 2017/746 Erregelamenduan daude araututa—, erregelamendu honen 3.49.c) artikuluan aipatutakoetara mugatuko da gorabehera larrien jakinarazpena, eta gorabehera hori gertatu den estatu kideek horretarako hautatutako agintaritza nazional eskudunari egingo zaio jakinarazpena.

11. Agintaritza nazional eskudunek berehala jakinaraziko diote Batzordeari gorabehera larri oro, horren inguruko neurriak hartu ala ez, (EB) 2019/1020 Erregelamenduaren 20. artikuluan ezarritakoaren arabera.

3. ATALA

Bermatzea Erregelamendua betearazten dela

74. artikulua.— Merkatuaren zaintza eta AA-sistemen kontrola Batasuneko merkatuan

1. (EB) 2019/1020 Erregelamendua erregelamendu honetan araututako AA-sistemei aplikatuko zaie. Erregelamendu hau modu efektiboan betearazten dela bermatzeko:

a) ulertuko da (EB) 2019/1020 Erregelamenduaren arabera operadore ekonomiko bati egindako erreferentzia orok barne hartzen dituela erregelamendu honen 2.1 artikuluan aipatutako operadore guztiak;



b) se entenderá que toda referencia a un producto con arreglo al Reglamento (UE) 2019/1020 incluye todos los sistemas de IA que estén comprendidos en el ámbito de aplicación del presente Reglamento.

2. Como parte de sus obligaciones de presentación de información en virtud del artículo 34, apartado 4, del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado informarán anualmente a la Comisión y a las autoridades nacionales de competencia pertinentes de cualquier información recabada en el transcurso de las actividades de vigilancia del mercado que pueda ser de interés potencial para la aplicación del Derecho de la Unión en materia de normas de competencia. Asimismo, informarán anualmente a la Comisión sobre el recurso a prácticas prohibidas que se hayan producido durante ese año y sobre las medidas adoptadas.

3. En el caso de los sistemas de IA de alto riesgo asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad responsable de las actividades de vigilancia del mercado designada en virtud de dichos actos legislativos.

Como excepción a lo dispuesto en el párrafo primero, en circunstancias adecuadas, los Estados miembros podrán designar otra autoridad pertinente como autoridad de vigilancia del mercado, siempre que se garantice la coordinación con las autoridades sectoriales de vigilancia del mercado pertinentes responsables de la ejecución de los actos legislativos de armonización de la Unión enumerados en el anexo I.

4. Los procedimientos a que se refieren los artículos 79 a 83 del presente Reglamento no se aplicarán a los sistemas de IA asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo I, sección A, cuando dichos actos legislativos ya prevean procedimientos que garanticen un nivel equivalente de protección que tengan el mismo objetivo. En dichos casos, se aplicarán los procedimientos sectoriales pertinentes.

5. Sin perjuicio de los poderes de las autoridades de vigilancia del mercado en virtud del artículo 14 del Reglamento (UE) 2019/1020, a efectos de garantizar la ejecución efectiva del presente Reglamento, las autoridades de vigilancia del mercado podrán ejercer a distancia los poderes a que se refiere el artículo 14, apartado 4, letras d) y j), de dicho Reglamento, según proceda.

6. En el caso de los sistemas de IA de alto riesgo introducidos en el mercado, puestos en servicio o

b) ulertuko da (EB) 2019/1020 Erregelamenduaren arabera produktu bati egindako erreferentzia orok barne hartzen dituela erregelamendu honen aplikazio-eremuan sartuta dauden AA-sistema guztiak.

2. Merkatua zaintzeko agintaritzek (EB) 2019/1020 Erregelamenduaren 34.4 artikulua arabera informazioa aurkezteko dituzten betebeharren artean, merkatua zaintzeko jardueretan bildutako informazio ororen berri emango diete urtero Batzordeari eta lehiaren agintaritza nazionalari, baldin eta informazio hori interesgarria izan badaiteke lehiari buruzko arauen arloko Batasuneko zuzenbidea aplikatzeko. Era berean, urtero jakinaraziko diote Batzordeari ea urte horretan jardunbide debekatuak erabili diren eta zer neurri hartu diren.

3. Batasunaren harmonizazioko lege-egintzek —I. eranskineko A atalean daude zerrendatuta— arautzen dituzten produktuei lotutako arrisku handiko AA-sistemen kasuan, lege-egintza horien arabera izendatutako merkatua zaintzeko agintaritza izango da, erregelamendu honen ondorioetarako, merkatua zaintzeko jardueren ardura izango duen agintaritza.

Lehenengo paragrafoan xedatutakoaren salbuespen gisa, egoera egokia denean, estatu kideek beste agintaritza bat izendatu ahal izango dute merkatua zaintzeko agintaritza gisa, betiere bermatzen bada behar bezala koordinatuko direla I. eranskinean zerrendatuta dauden Batasunaren harmonizazioko lege-egintzak betearazteaz arduratzen diren merkatua zaintzeko agintaritza sektorial egokiekin.

4. Erregelamendu honetako 79. eta 83. artikuluen artean aipatzen diren prozedurak ez zaizkie aplikatuko Batasunaren harmonizazioko lege-egintzek —I. eranskineko A atalean daude zerrendatuta— arautzen dituzten produktuei lotutako AA-sistemei, baldin eta helburu bera duten eta babes-maila baliokidea bermatzen duten prozedurak aurreikusten badituzte lege-egintza horiek. Kasu horietan, dagozkien prozedura sektorialak aplikatuko dira.

5. Ezertan eragotzi gabe (EB) 2019/1020 Erregelamenduaren 14. artikulua arabera merkatua zaintzeko agintaritzek dituzten ahalak, erregelamendu hau modu efektiboan betetzen dela bermatzeko, merkatua zaintzeko agintaritzek urrunetik baliatu ahal izango dituzte erregelamendu horren 14.4 artikulua d) eta j) letretan aipatzen diren ahalak, dagokionaren arabera.

6. Batasunak finantza-zerbitzuen arloan xedatutako zuzenbidearen arabera araututako finantza-entitateek



utilizados por entidades financieras reguladas por el Derecho de la Unión en materia de servicios financieros, la autoridad de vigilancia del mercado a efectos del presente Reglamento será la autoridad nacional pertinente responsable de la supervisión financiera de dichas entidades con arreglo a la mencionada legislación, en la medida en que la introducción en el mercado, la puesta en servicio o la utilización del sistema de IA esté directamente relacionada con la prestación de dichos servicios financieros.

7. Como excepción a lo dispuesto en el apartado 6, en las circunstancias apropiadas y siempre que se garantice la coordinación, el Estado miembro podrá designar otra autoridad pertinente como autoridad de vigilancia del mercado a efectos del presente Reglamento.

Las autoridades nacionales de vigilancia del mercado que supervisen las entidades de crédito reguladas por la Directiva 2013/36/UE y que participen en el Mecanismo Único de Supervisión establecido por el Reglamento (UE) n.º 1024/2013 deberán comunicar sin demora al Banco Central Europeo toda información obtenida en el transcurso de sus actividades de vigilancia del mercado que pueda ser de interés para las funciones de supervisión prudencial del Banco Central Europeo especificadas en dicho Reglamento.

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

9. Cuando las instituciones, órganos y organismos de la Unión entren en el ámbito de aplicación del presente Reglamento, el Supervisor Europeo de Protección de Datos actuará como su autoridad de vigilancia del mercado, salvo en relación con el Tribunal de Justicia de la Unión Europea cuando actúe en el ejercicio de su función judicial.

merkatuan jarri, zerbitzuan ipini edo erabilitako arrisku handiko AA-sistemen kasuan, hau izango da merkatua zaintzeko agintaritza erregelamendu honen ondorioetarako: aipatutako legeria betez entitate horien finantza gainbegiratzeko ardura duen agintaritza nazional egokia, kontuan hartuta AA-sistema bat merkatuan jarri, zerbitzuan ipini edo erabiltzea zuzenean dagoela lotuta finantza-zerbitzu horiek ematearekin.

7. Artikulu honen 6. apartatuan xedatutakoaren salbuespen gisa, egoera egokia bada eta koordinazioa bermatzen baldin bada, estatu kideak beste agintaritza egoki bat izendatu ahal izango du merkatua zaintzeko agintaritza izateko erregelamendu honen ondorioetarako.

2013/36/EB Zuzentarauak arautzen dituen kreditu-entitateak gainbegiratzen dituzten eta (EB) 1024/2013 Erregelamenduak ezarritako Gainbegiratze Mekanismo Bakarrean parte hartzen duten merkatua zaintzeko agintaritza nazionalak atzerapenik gabe jakinarazi beharko diote Europako Banku Zentralari merkatua zaintzeko jardueretan eskuratutako informazio guztia, baldin eta interesgarria izan badaiteke erregelamendu horretan zehaztutako Europako Banku Zentralaren zuhurtziazko gainbegiratze-eginkizunak egiteko.

8. Erregelamendu honen III. eranskineko 1. puntuan zerrendatuta dauden arrisku handiko AA-sistemen kasuan, sistema horiek zuzenbidea betearazteko, mugak kudeatzeko eta justizia eta demokraziarako erabiltzen diren heinean, eta erregelamendu honen III. eranskineko 6., 7. eta 8. puntuetan zerrendatutako arrisku handiko AA-sistemen kasuan, estatu kideek hauek izendatu ahal izango dituzte merkatua zaintzeko agintaritza izateko erregelamendu honen ondorioetarako: bai (EB) 2016/679 Erregelamenduaren edo (EB) 2016/680 Zuzentarauaren arabera datuak babesteaz arduratzen diren kontrol-agintaritza eskudunak, bai (EB) 2016/680 Zuzentarauaren 41. eta 44. artikuluen artean ezarritako baldintza berberen arabera izendatutako beste edozein agintaritza. Merkatua zaintzeko jarduerak ez diote inola ere eragingo agintaritza judizialen independentziari, eta ez dituzte beste inola ere oztopatuko haien eginkizun judizialek eratorritako jarduerak.

9. Batasuneko instituzio, organo eta organismoak erregelamendu honen aplikazio-eremuan sartzen direnean, Datuak Babesteko Europako Ikuskatzailea izango da merkatua zaintzeko agintaritza, Europar Batasuneko Justizia Auzitegiari dagokionez izan ezik, bere eginkizun judizialean diharduenean.



10. Los Estados miembros facilitarán la coordinación entre las autoridades de vigilancia del mercado designadas con arreglo al presente Reglamento y otras autoridades u organismos nacionales pertinentes responsables de supervisar la aplicación de la legislación de armonización de la Unión indicada en el anexo I o en otras disposiciones de Derecho de la Unión que pudieran resultar pertinente para los sistemas de IA de alto riesgo a que se refiere el anexo III.

11. Las autoridades de vigilancia del mercado y la Comisión podrán proponer actividades conjuntas, incluidas investigaciones conjuntas, que deben llevar a cabo bien las autoridades de vigilancia del mercado, bien las autoridades de vigilancia del mercado junto con la Comisión, con el objetivo de fomentar el cumplimiento, detectar incumplimientos, sensibilizar u ofrecer orientaciones en relación con el presente Reglamento con respecto a las categorías específicas de sistemas de IA de alto riesgo que presentan un riesgo grave en dos o más Estados miembros de conformidad con el artículo 9 del Reglamento (UE) 2019/1020. La Oficina de IA prestará apoyo de coordinación a las investigaciones conjuntas.

12. Sin perjuicio de los poderes previstos en el Reglamento (UE) 2019/1020, y cuando proceda y se limite a lo necesario para el desempeño de sus funciones, los proveedores concederán a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de entrenamiento, validación y prueba utilizados para el desarrollo de los sistemas de IA de alto riesgo, también, cuando proceda y con sujeción a garantías de seguridad, a través de interfaces de programación de aplicaciones (API) o de otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

13. Se concederá a las autoridades de vigilancia del mercado acceso al código fuente del sistema de IA de alto riesgo, previa solicitud motivada y solo si se cumplen las dos siguientes condiciones:

a) el acceso al código fuente es necesario para evaluar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2, y

b) se han agotado todos los procedimientos de prueba o auditoría y todas las comprobaciones basadas en los datos y la documentación facilitados por el proveedor, o han resultado insuficientes.

14. Cualesquiera información o documentación obtenidas por las autoridades de vigilancia del mercado

10. Estatu kideek erraztu egingo dute koordinazioa egotea erregelamendu honen arabera izendatu diren merkatua zaintzeko agintaritzen eta bestelako agintaritza edo organismo nazionalen artean, agintaritza eta organismo horien ardura den heinean I. eranskinean —edo III. eranskinean aipatzen diren arrisku handiko AA-sistemetak egokiak izan litezkeen Batasuneko zuzenbideko beste xedapen batzuetan— adierazi diren Batasunaren harmonizazioko legeria aplikatzen den gainbegiratzea.

11. (EB) 2019/1020 Erregelamenduaren 9. artikulua arabera bi estatu kide edo gehiagotan arrisku larria dakarren arrisku handiko AA-sistemen kategoría espezifikoek dagokienez erregelamendu hau beteko dela sustatzeko, ez-betetzeak detektatzeko eta haren inguruan sentibilizatzeko eta orientabideak emateko, baterako jarduerak proposatu ahal izango dituzte merkatua zaintzeko agintaritzek eta Batzordeak, baita baterako ikerketak ere, merkatua zaintzeko agintaritzek bakarrik edo Batzordearekin batera egin behar badituzte. AA-bulegoak koordinazio-laguntza emango du baterako ikerketak egiteko.

12. (EB) 2019/1020 Erregelamenduan aurreikusitako ahalei kalterik egin gabe, eta hala dagokionean eta bere eginkizunak betetzeko beharrezkoa dena mugatzen denean, hornitzaileek sarbide osoa emango diete merkatua zaintzeko agintaritzei, bai arrisku handiko AA-sistemak garatzeko erabilitako entrenamendu-, balioztatze- eta proba-datuen multzoetara, bai dokumentaziora, eta, hala dagokionean eta segurtasun-bermeei lotuta, aplikazio-programaren interfazeen (API) edo urrutitik sartzeari ahalbidetzen duten beste tresna eta bitarteko tekniko egoki batzuen bidez.

13. Arrisku handiko AA-sistemaren iturburu-koderako sarbidea emango zaie merkatua zaintzeko agintaritzei, arrazoituta eskatuz gero, bi baldintza hauek betetzen badira:

a) iturburu-koderako sarbidea beharrezkoa da arrisku handiko AA-sistema bat III. kapituluko 2. atalean ezarritako betekizunekin bat datorren ebaluatzeko, eta

b) proba- edo auditoretza-prozedura guztiak amaitu dira, baita hornitzaileak emandako datuetan eta dokumentazioan oinarritutako egiaztapen guztiak ere, edo ez dira nahikoak izan.

14. Merkatua zaintzeko agintaritzak lortutako informazio eta dokumentazio guztia 78. artikuluan



se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78.

Artículo 75.– Asistencia mutua, vigilancia del mercado y control de sistemas de IA de uso general

1. Cuando un sistema de IA se base en un modelo de IA de uso general y un mismo proveedor desarrolle tanto el modelo como el sistema, la Oficina de IA estará facultada para vigilar y supervisar el cumplimiento por parte de dicho sistema de IA de las obligaciones en virtud del presente Reglamento. Para llevar a cabo estas tareas de vigilancia y supervisión, la Oficina de IA tendrá todos los poderes de una autoridad prevista en la presente sección y en el Reglamento (UE) 2019/1020.

2. Cuando las autoridades de vigilancia del mercado pertinentes tengan motivos suficientes para considerar que los sistemas de IA de uso general que pueden ser utilizados directamente por los responsables del despliegue al menos para una de las finalidades clasificadas como de alto riesgo con arreglo al presente Reglamento no cumplen los requisitos establecidos en el presente Reglamento, cooperarán con la Oficina de IA para llevar a cabo evaluaciones del cumplimiento e informarán al respecto al Consejo de IA y las demás autoridades de vigilancia del mercado.

3. Cuando una autoridad de vigilancia del mercado no pueda concluir su investigación sobre el sistema de IA de alto riesgo por no poder acceder a determinada información relativa al modelo de IA de uso general, a pesar de haber realizado todos los esfuerzos adecuados para obtener esa información, podrá presentar una solicitud motivada a la Oficina de IA para que se imponga el acceso a dicha información. En tal caso, la Oficina de IA facilitará a la autoridad solicitante sin demora y, en cualquier caso en un plazo de treinta días, toda la información que la Oficina de IA considere pertinente para determinar si un sistema de IA de alto riesgo no es conforme. Las autoridades de vigilancia del mercado preservarán la confidencialidad de la información obtenida de conformidad con lo dispuesto en el artículo 78 del presente Reglamento. Se aplicará *mutatis mutandis* el procedimiento previsto en el capítulo VI del Reglamento (UE) 2019/1020.

Artículo 76.– Supervisión de las pruebas en condiciones reales por las autoridades de vigilancia del mercado

1. Las autoridades de vigilancia del mercado tendrán las competencias y los poderes necesarios para garantizar que las pruebas en condiciones reales se ajusten a lo dispuesto en el presente Reglamento.

ezarritako konfidentziasun-betebeharren arabera tratatuko da.

75. artikulua.– Elkarrekiko laguntza, merkatuaren zaintza eta kontrola erabilera orokorreko AA-sistemetan

1. AA-sistema bat erabilera orokorreko AA-eredu batean oinarritzen denean eta hornitzaile berak garatzen duenean bai eredu, bai sistema, AA-bulegoak zaindu eta gainbegiratuko du ea AA-sistema horrek bete egiten dituen erregelamendu honen arabera betebeharrak. Zaintza- eta gainbegiratze-lan horiek egiteko, atal honetan eta (EB) 2019/1020 Erregelamenduan aurreikusitako agintaritza baten ahal guztiak izango ditu AA-bulegoak.

2. Hedapenaren arduradunek zuzenean erabil ditzakete erabilera orokorreko AA-sistema batzuk erregelamendu honen arabera arrisku handikotzat sailkatutako helburuetako baterako gutxienez. Horrelakoetan, merkatua zaintzeko agintaritza egokiek nahikoa arrazoi dutenean pentsatzeko hedapenaren arduradunek ez dituztela betetzen erregelamendu honetan ezarritako betekizunak, lankidetzan jardungo dute AA-bulegoarekin betetze-mailaren ebaluazioak egiteko, eta horren berri emango diete AA-kontseiluari eta merkatua zaintzeko gainerako agintaritzei.

3. Merkatua zaintzeko agintaritza batek, bidezko ahalegin guztiak eginda ere, ezin izan badu eskuratu erabilera orokorreko AA-ereduari buruzko informazio jakin bat, eta, ondorioz, ezin izan badu amaitu arrisku handiko AA-sistemari buruzko ikerketa, eskaera arrazoitu bat aurkeztu ahal izango dio AA-bulegoari, informazio horretarako sarbidea ezar dadin. Kasu horretan, AA-bulegoak, atzerapenik gabe eta, nolana ere, hogeita hamar eguneko epean, arrisku handiko AA-sistema bat egokia ez den zehazteko esanguratsutzat jotzen duen informazio guztia emango dio agintaritza eskatzaileari. Erregelamendu honen 78. artikuluan xedatutakoaren arabera lortutako informazioaren konfidentziasuna bermatuko dute merkatua zaintzeko agintaritzek. *Mutatis mutandis* aplikatuko da (EB) 2019/1020 Erregelamenduaren VI. kapituluaren aurreikusitako prozedura.

76. artikulua.– Merkatua zaintzeko agintariak baldintza errealeko probak gainbegiratzea

1. Merkatua zaintzeko agintaritzek beharrezko eskumen eta ahalak izango dituzte baldintza errealeko probak erregelamendu honetan xedatutakoari egokitzen zaizkiola bermatzeko.



2. Cuando se realicen pruebas en condiciones reales de sistemas de IA supervisadas dentro de un espacio controlado de pruebas para la IA con arreglo al artículo 58, las autoridades de vigilancia del mercado verificarán el cumplimiento de del artículo 60 como parte de su función supervisora en el espacio controlado de pruebas para la IA. Dichas autoridades podrán permitir, según proceda, que el proveedor o proveedor potencial lleve a cabo pruebas en condiciones reales, como excepción a las condiciones establecidas en el artículo 60, apartado 4, letras f) y g).

3. Cuando una autoridad de vigilancia del mercado haya sido informada por el proveedor potencial, el proveedor o un tercero de un incidente grave o tenga otros motivos para pensar que no se cumplen las condiciones establecidas en los artículos 60 y 61, podrá adoptar una de las decisiones siguientes en su territorio, según proceda:

a) suspender o poner fin a las pruebas en condiciones reales;

b) exigir al proveedor o proveedor potencial y al responsable del despliegue o responsable del despliegue potencial que modifiquen cualquier aspecto de las pruebas en condiciones reales.

4. Cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3 del presente artículo o haya formulado una objeción en el sentido del artículo 60, apartado 4, letra b), la decisión o la objeción deberá estar motivada e indicar las vías de que dispone el proveedor o proveedor potencial para poder impugnar la decisión o la objeción.

5. En su caso, cuando una autoridad de vigilancia del mercado haya adoptado una decisión mencionada en el apartado 3, comunicará los motivos de dicha decisión a las autoridades de vigilancia del mercado de los demás Estados miembros en que se haya probado el sistema de IA de conformidad con el plan de la prueba.

Artículo 77.— Poderes de las autoridades encargadas de proteger los derechos fundamentales

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

2. AArako proba-ingurune arautu baten barruan gainbegiraturako AA-sistemen baldintza errealeko probak egiten direnean —58. artikulua arabera—, 60. artikulua betetzen den egiaztatuko dute merkatua zaintzeko agintaritzek, AArako proba-ingurune arautuan duten gainbegiratze-eginkizunaren barruan. Agintaritza horiek aukera eman ahal izango dute, dagokionaren arabera, hornitzaileak edo hornitzaile potentzialak baldintza errealeko probak egin ditzan, 60.4 artikuluko f) eta g) letretan ezarritako baldintzen salbuespen gisa.

3. Hornitzaileak, hornitzaile potentzialak edo hirugarren batek gorabehera larri baten berri ematen dionean merkatua zaintzeko agintaritzari, edo agintaritza horrek beste arrazoi batzuk baditu 60. eta 61. artikuluetan ezarritako baldintzak betetzen ez direla pentsatzeko, erabaki hauetako bat hartu ahal izango du bere lurraldean, dagokionaren arabera:

a) baldintza errealeko probak etetea edo amaitzea;

b) baldintza errealeko proben edozein alderdi aldatzeko eskatzea hornitzaileari edo hornitzaile potentzialari eta hedapenaren arduradunari edo hedapenaren arduradun potentzialari.

4. Merkatua zaintzeko agintaritza batek artikulua honen 3. apartatuan aipatutako erabaki bat hartu duenean edo eragozpenen bat jarri duenean 60.4.b) artikuluari dagokionez, erabakia edo eragozpena arrazoituta egon beharko da, eta adierazi beharko du zein bide erabili ahal izango duen hornitzaileak edo hornitzaile potentzialak erabakia edo eragozpena aurkaratzeko.

5. Hala badagokio, merkatua zaintzeko agintaritza batek 3. apartatuan aipatutako erabaki bat hartzen duenean, erabaki horren arrazoiak azalduko dizkie probaren planaren arabera AA-sistema probatu den gainerako estatu kideetako merkatua zaintzeko agintaritzei.

77. artikulua.— Oinarrizko eskubideak babesteaz arduratzen diren agintaritzen ahalak

1. III. eranskinean aipatutako arrisku handiko AA-sistemak erabiltzeari dagokionez, oinarrizko eskubideen babesaren arloan —diskriminaziorik ezaren eskubidea barne— Batasuneko zuzenbidean jasota dauden betebeharrak gainbegiratzeko edo errespetarazteko ardura duten agintaritza edo organismo publiko nazionalak ahalmena izango dute erregelamendu honen arabera sortutako edo gordetako edozein dokumentazio eskatzeko eta eskuratzeko, hizkera eta formatu irisgarri batean, baldin eta dokumentazio hori eskuratzeko beharrezkoa bada beren ahalak modu efektiboan betetzeko, beren jurisdikzioaren mugen barruan.



de los límites de su jurisdicción. La autoridad u organismo público pertinente informará sobre cualquier solicitud de este tipo a la autoridad de vigilancia del mercado del Estado miembro que corresponda.

2. A más tardar el 2 de noviembre de 2024, cada Estado miembro designará las autoridades u organismos públicos a que se refiere el apartado 1 y los incluirá en una lista que pondrá a disposición del público. Los Estados miembros notificarán dicha lista a la Comisión y a los demás Estados miembros y la mantendrán actualizada.

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

4. Cualquier información o documentación obtenidas por las autoridades u organismos públicos nacionales a que se refiere el apartado 1 del presente artículo con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad dispuestas en el artículo 78.

Artículo 78.– Confidencialidad

1. La Comisión, las autoridades de vigilancia del mercado, los organismos notificados y cualquier otra persona física o jurídica que participe en la aplicación del presente Reglamento, de conformidad con el Derecho de la Unión o nacional, respetarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades de modo que se protejan, en particular:

a) los derechos de propiedad intelectual e industrial y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos mencionados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo [\(57\)](#);

b) la aplicación eficaz del presente Reglamento, en particular a efectos de investigaciones, inspecciones o auditorías;

c) los intereses de seguridad pública y nacional;

Dagokion agintaritzak edo organismo publikoak horrelako eskaera guztien berri emango dio dagokion estatu kideko merkatua zaintzeko agintaritzari.

2. 2024ko azaroaren 2rako, 1. apartatuan aipatzen diren agintariak edo organismo publikoak izendatuko ditu estatu kide bakoitzak; zerrenda batean sartuko ditu eta herritarren eskura ipiniko du zerrenda hori. Estatu kideek zerrenda horren berri emango diete Batzordeari eta gainerako estatu kideei, eta eguneratuta mantenduko dute.

3. Baldin eta 1. apartatuan aipatutako dokumentazioa ez bada nahikoa zehazteko oinarritzko eskubideen babesaren arloan Batasuneko zuzenbidean aurreikusita dauden betebeharrak urratu diren ala ez, 1. apartatuan aipatzen den agintaritzak edo organismo publikoak eskaera arrazoitu bat aurkeztu ahal izango dio merkatua zaintzeko agintaritzari, arrisku handiko AA-sistemaren probak antolatzeako bitarteko teknikoaren bidez. Merkatua zaintzeko agintaritzak agintaritzak edo organismo publiko eskatzailearen lankidetzak estuarekin antolatuko ditu probak, eskaera aurkeztu eta arrazoizko epe batean.

4. Artikulu honen 1. apartatuan aipatzen diren agintaritzak edo organismo publiko nazionalak artikulu honen arabera lortzen duten edozein informazio edo dokumentazio 78. artikuluan xedatutako konfidentzialtasun-betebeharren arabera tratatuko da.

78. artikulua.– Konfidentzialtasuna

1. Batzordeak, merkatua zaintzeko agintaritzek, organismo jakinaraziek eta erregelamendu honen aplikazioan parte hartzen duen beste edozein pertsona fisikok edo juridikok, Batasuneko zuzenbidearekin edo zuzenbide nazionalarekin bat etorritik, beren eginkizunak eta jarduerak betetzean lortutako informazioaren eta datuen konfidentzialtasuna errespetatuko dute, eta, bereziki, alderdi hauek babestuko dituzte:

a) jabetza intelektual eta industrialaren eskubideak eta enpresa-informazio konfidentziala edo pertsona fisiko edo juridiko baten merkataritza-sekretuak, iturburu-kodea barne, Europako Parlamentuaren eta Kontseiluaren (EB) 2016/943 Zuzentarauaren 5. artikuluan aipatutako kasuetan izan ezik [\(57\)](#);

b) erregelamendu hau modu eraginkorrean aplikatzea, bereziki ikerketa, ikuskapen edo auditoretzei dagokienez;

c) segurtasun publikoaren eta nazionalaren interesak;



d) el desarrollo de las causas penales o los procedimientos administrativos;

e) la información clasificada con arreglo al Derecho de la Unión o nacional.

2. Las autoridades involucradas en la aplicación del presente Reglamento de conformidad con el apartado 1 solo solicitarán los datos que sean estrictamente necesarios para la evaluación del riesgo que presentan los sistemas de IA y para el ejercicio de sus competencias de conformidad con el presente Reglamento y con el Reglamento (UE) 2019/1020. Establecerán medidas adecuadas y eficaces en materia de ciberseguridad a fin de proteger la seguridad y la confidencialidad de la información y los datos obtenidos, y suprimirán los datos recopilados tan pronto como dejen de ser necesarios para los fines para los que se obtuvieron, de conformidad con el Derecho de la Unión y nacional aplicable.

3. Sin perjuicio de lo dispuesto en los apartados 1 y 2, la información intercambiada de forma confidencial entre las autoridades nacionales competentes o entre estas y la Comisión no se revelará sin consultar previamente a la autoridad nacional competente de origen y al responsable del despliegue cuando las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo utilicen los sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, y dicha divulgación comprometería los intereses de seguridad pública y nacional. Este intercambio de información no comprenderá los datos operativos sensibles relativos a las actividades de las autoridades garantes del cumplimiento del Derecho, del control de fronteras, de la inmigración o del asilo.

Cuando las autoridades garantes del cumplimiento del Derecho, de la inmigración o del asilo sean proveedores de sistemas de IA de alto riesgo a que se refiere el anexo III, puntos 1, 6 o 7, la documentación técnica mencionada en el anexo IV permanecerá dentro de las instalaciones de dichas autoridades. Dichas autoridades velarán por que las autoridades de vigilancia del mercado a que se refiere el artículo 74, apartados 8 y 9, según proceda, puedan, previa solicitud, acceder inmediatamente a la documentación u obtener una copia de esta. Tan solo se permitirá acceder a dicha documentación o a cualquier copia de esta al personal de la autoridad de vigilancia del mercado que disponga de una habilitación de seguridad del nivel adecuado.

4. Los apartados 1, 2 y 3 no afectarán a los derechos u obligaciones de la Comisión, los Estados miembros y sus autoridades pertinentes, ni a los derechos u obligaciones de los organismos notificados en lo que se refiere al intercambio de información y la difusión de

d) auzi penalen edo administrazio-prozeduren garapena;

e) Batasuneko zuzenbidearen edo zuzenbide nazionalaren arabera informazio sailkatua.

2. AA-sistemek dakarten arriskua ebaluatzeko eta erregelamendu honen eta (EB) 2019/1020 Erregelamenduaren arabera beren eskumenak baliatzeko behar-beharrezkoak diren datuak baino ez dituzte eskatuko 1. apartatuaren arabera erregelamendu honen aplikazioan parte hartzen duten agintaritzek. Neurri egoki eta eraginkorrak ezarriko dituzte zibersegurtasunaren arloan, lortutako informazioaren eta datuen segurtasuna eta konfidentzialtasuna babesteko, eta bildutako datuak ezabatu egingo dituzte lortu ziren helburuetarako beharrezkoak izateari utzi bezain laster, aplikatu behar diren Batasuneko zuzenbidearekin eta zuzenbide nazionalarekin bat etorritik.

3. Artikulu honen 1. eta 2. apartatuetan xedatutakoa alde batera utzi gabe, agintaritza nazional eskudunen artean edo agintaritza horien eta Batzordearen artean modu konfidentzialean trukaturako informazioa ez da ezagutaraziko jatorrizko agintaritza nazional eskudunari eta hedapenaren arduradunari aldez aurretik kontsulta egin gabe, baldin eta zuzenbidea betearazteaz, muga-kontrolaz, immigrazioaz edo asiloaz arduratzen diren agintaritzek III. eranskineko 1., 6. edo 7. puntuetan aipatzen diren arrisku handiko AA-sistemak erabiltzen badituzte eta zabaltze horrek arriskuan jartzen baditu segurtasun publikoaren eta nazionalaren interesak. Informazio-truke horretan ez dira sartuko bereziki babestutako datu operatiboak, baldin eta zuzenbidea betearazteaz, muga-kontrolaz, immigrazioaz edo asiloaz arduratzen diren agintaritzen jardueri buruzkoak badira.

Zuzenbidea betearazteaz, immigrazioaz edo asiloaz arduratzen diren agintaritzak III. eranskineko 1., 6. edo 7. puntuetan aipatzen diren arrisku handiko AA-sistemen hornitzaileak direnean, agintaritza horien instalazioen barruan egon beharko da IV. eranskinean aipatutako dokumentazio teknikoa. Agintaritza horiek zainduko dute 74. artikularen 8. eta 9. apartatuetan aipatzen diren merkatua zaintzeko agintaritzek, dagokionaren arabera, dokumentazioa berehala eskuratu edo haren kopia bat lortu ahal izatea, aldez aurretik eskatuz gero. Merkatua zaintzeko agintaritzako langileek bakarrik eskuratu ahal izango dute dokumentazio hori edo haren edozein kopia, baldin eta maila egokiko segurtasun-gaikuntza badute.

4. Artikulu honen 1., 2. eta 3. apartatuek ez dute eraginik izango Batzordearen, estatu kideen eta dagozkien agintaritzen eskubide edo betebeharretan, ez eta organismo jakinarazien eskubide edo betebeharretan ere, informazio-trukeari eta



advertencias, también en el contexto de la cooperación transfronteriza, ni a las obligaciones de facilitar información en virtud del Derecho penal de los Estados miembros que incumban a las partes interesadas.

5. Cuando sea necesario y con arreglo a las disposiciones pertinentes de los acuerdos internacionales y comerciales, la Comisión y los Estados miembros podrán intercambiar información confidencial con autoridades reguladoras de terceros países con las que hayan celebrado acuerdos de confidencialidad bilaterales o multilaterales que garanticen un nivel de confidencialidad adecuado.

Artículo 79.– Procedimiento aplicable a escala nacional a los sistemas de IA que presenten un riesgo

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

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

Cuando, en el transcurso de tal evaluación, la autoridad de vigilancia del mercado o, cuando proceda, la autoridad de vigilancia del mercado en cooperación con la autoridad nacional pública a que se refiere el artículo 77, apartado 1, constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad podrá determinar y, en cualquier caso, en un plazo de

ohartarazpenak zabaltzeari dagokionez, ezta mugaz gaindiko lankidetzaren testuinguruan ezta alderdi interesdunei dagozkien estatu kideen zigor-zuzenbidearen arabera informazioa emateko betebeharretan ere.

5. Beharrezkoa denean, eta nazioarteko eta merkataritzako akordioetako dagozkion xedapenen arabera, Batzordeak eta estatu kideek informazio konfidentziala trukatu ahal izango dute beste herrialde batzuetako agintaritza arautzaileekin, baldin eta konfidentzialtasun-akordio bilateral edo multilateralak sinatu badituzte haiekin, konfidentzialtasun-maila egokia bermatzeko.

79. artikulua.– Arriskua dakarten AA-sistemei nazio-mailan aplikatzekoa den prozedura

1. Arriskua dakarten AA-sistemak «arriskua dakarten produktutzat» hartuko dira, (EB) 2019/1020 Erregelamenduaren 3.19 artikuluan definitzen diren bezala, baldin eta pertsonen osasunari, segurtasunari edo oinarrizko eskubideei eragiten dieten arriskuak badakartzate.

2. Estatu kide bateko merkatua zaintzeko agintaritzak nahikoa arrazoi duenean pentsatzeko AA-sistema batek artikulua honetako 1. apartatuan aipatutako arrisku bat dakarrela, dagokion AA-sistemaren ebaluazioa egingo du, erregelamendu honetan ezarritako betekizun eta betebehar guztiak betetzen dituen egiaztatzeko. Arreta berezia jarri behar zaie kolektibo kalteberentzako arriskua dakarten AA-sistemei. Oinarrizko eskubideetarako arriskuak detektatzen direnean, 77.1 artikuluan aipatzen diren agintaritza edo organismo publiko nazionalak ere jakinaraziko die merkatua zaintzeko agintaritzak, eta erabateko lankidetzan jardungo du haiekin. Behar den guztian, operadoreak lankidetzan arituko dira merkatua zaintzeko agintaritzarekin eta 77.1 artikuluan aipatzen diren gainerako agintaritza edo organismo publiko nazionalekin.

Ebaluazioa egin bitartean, merkatua zaintzeko agintaritzak edo, hala dagokionean, merkatua zaintzeko agintaritzak eta 77.1 artikuluan aipatzen diren agintaritza nazional publikoak lankidetzan, egiaztatzen badu AA-sistemak ez dituela betetzen erregelamendu honetan ezarritako betekizunak eta betebeharrak, bidegabeko atzerapenik gabe eskatuko dio dagokion operadoreari neurri zuzentzaile egoki guztiak har ditzala AA-sistema aipatutako betekizun eta betebeharretara egokitzeko, sistema hori merkatutik erretiratzeko edo berreskuratzeko, agintaritza horrek erabaki ahal izango duen epe baten barruan, eta, nolahi ere, hamabost



quince días hábiles a más tardar o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes según corresponda.

La autoridad de vigilancia del mercado informará al organismo notificado correspondiente en consecuencia. El artículo 18 del Reglamento (UE) 2019/1020 será de aplicación a las medidas mencionadas en el párrafo segundo del presente apartado.

3. Cuando la autoridad de vigilancia del mercado considere que el incumplimiento no se limita a su territorio nacional, informará a la Comisión y a los demás Estados miembros sin demora indebida de los resultados de la evaluación y de las medidas que haya instado al operador a adoptar.
4. El operador se asegurará de que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en la Unión.
5. Si el operador de un sistema de IA no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 2, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del sistema de IA en su mercado nacional o su puesta en servicio, para retirar el producto o el sistema de IA independiente de dicho mercado o recuperarlo. Dicha autoridad notificará estas medidas sin demora indebida a la Comisión y a los demás Estados miembros.
6. La notificación a que se refiere el apartado 5 incluirá todos los detalles disponibles, en particular la información necesaria para la identificación del sistema de IA no conforme, el origen del sistema de IA y la cadena de suministro, la naturaleza de la presunta no conformidad y el riesgo planteado, la naturaleza y duración de las medidas nacionales adoptadas y los argumentos expresados por el operador correspondiente. En concreto, las autoridades de vigilancia del mercado indicarán si la no conformidad se debe a uno o varios de los motivos siguientes:
 - a) el no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5;
 - b) el incumplimiento de los requisitos establecidos en el capítulo III, sección 2, por parte de un sistema de IA de alto riesgo;
 - c) deficiencias en las normas armonizadas o especificaciones comunes mencionadas en los artículos 40 y 41 que confieren la presunción de conformidad;

egun balioduneko epean gehienez, edo, dagokionaren arabera, Batasunaren harmonizazioko lege-egintzek aurreikusten duten epean.

Merkatua zaintzeko agintaritzak horren berri emango dio organismo jakinarazari. (EB) 2019/1020 Erregelamenduaren 18. artikuluan ezarritakoa aplikatuko zaie apartatu honen bigarren paragrafoan aipatutako neurriei.

3. Merkatua zaintzeko agintaritzak uste badu ez-betetzea ez dela bere lurralde nazionalera mugatzen, Batzordeari eta gainerako estatu kideei jakinaraziko dizkie, bidegabeko atzerapenik gabe, ebaluazioaren emaitzak eta operadoreari ezarritako neurriak.
4. Operadoreak ziurtatu egingo du Batasunean merkaturatu dituen ukitutako AA-sistema guztiei aplikatzen zaizkiela neurri zuzentzaile egoki guztiak.
5. AA-sistema baten operadoreak ez baditu neurri zuzentzaile egokiak hartzen 2. apartatuan aipatzen den epean, merkaturatutako agintaritzak behin-behineko neurri egoki guztiak hartuko ditu AA-sistema bere merkatu nazionalen merkaturatzea edo zerbitzuan ipintzea debekatzeko edo murrizteko, eta produktua edo AA-sistema independentea merkatu horretatik erretiratzeko edo berreskuratzeko. Agintaritza horrek bidegabeko atzerapenik gabe jakinaraziko dizkie neurri horiek Batzordeari eta gainerako estatu kideei.
6. Artikulu honen 5. apartatuan aipatzen den jakinarazpenak eskura dauden xehetasun guztiak jasoko ditu, bereziki adostasuna betetzen ez duen AA-sistema identifikatzeko behar den informazioa, AA-sistemaren jatorria eta hornidura-katea, ustezko ez-adostasunaren izaera eta arriskua, hartutako neurri nazionalen izaera eta iraupena, eta dagokion operadoreak adierazi dituen argudioak. Zehazki, merkaturatutako agintaritzek adieraziko dute ea adostasun-eza arrazoi hauetakoren batengatik edo batzuegatik gertatu den:
 - a) ez errespetatzea 5. artikuluan aipatutako AA-jardunbideen debekua;
 - b) arrisku handiko AA-sistema batek ez betetzea III. kapituluko 2. atalean ezarritako betekizunak;
 - c) hutsuneak egotea adostasun-presuntzioa ematen duten eta 40. eta 41. artikuluetan aipatuta dauden arau harmonizatueta edo zehaztapen komunetan;



d) el incumplimiento del artículo 50.

d) ez betetzea 50. artikulua.

7. Las autoridades de vigilancia del mercado distintas de la autoridad de vigilancia del mercado del Estado miembro que inició el procedimiento comunicarán sin demora indebida a la Comisión y a los demás Estados miembros toda medida que adopten y cualquier información adicional de que dispongan en relación con la no conformidad del sistema de IA de que se trate y, en caso de desacuerdo con la medida nacional notificada, sus objeciones al respecto.

7. Prozedura hasi zuen estatu kideko merkatua zaintzeko agintaritzaz bestelakoak diren merkatua zaintzeko agintaritzek, bidegabeko atzerapenik gabe jakinaraziko dizkiete Batzordeari eta gainerako estatu kideei kasuan kasuko AA-sistemaren ez-adostasunaren inguruan hartzen dituzten neurri guztiak eta daukaten edozein informazio gehigarri, eta, jakinarazitako neurri nazionalarekin ados ez badaude, horren inguruko eragozpenak azalduko dituzte.

8. Si, en el plazo de tres meses desde la recepción de la notificación mencionada en el apartado 5 del presente artículo, ninguna autoridad de vigilancia del mercado de un Estado miembro ni la Comisión presentan objeción alguna sobre una medida provisional adoptada por una autoridad de vigilancia del mercado de otro Estado miembro, la medida se considerará justificada. Esto se entiende sin perjuicio de los derechos procedimentales del operador correspondiente con arreglo al artículo 18 del Reglamento (UE) 2019/1020. El plazo de tres meses a que se refiere el presente apartado se reducirá a treinta días en caso de no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 del presente Reglamento.

8. Artikulu honen 5. apartatuan aipatutako jakinarazpena jaso eta hiru hilabeteko epean, ez Batzordeak, ez beste estatu kide bateko merkatua zaintzeko agintaritza bakar batek ere ez badu eragozpenik jartzen beste estatu kide bateko merkatua zaintzeko autoritate batek hartutako behin-behineko neurri baten gainean, justifikatutzat joko da neurria. Horrek ez ditu eragotziko dagokion operadoreak (EB) 2019/1020 Erregelamenduaren 18. artikuluaaren arabera dituen prozedura-eskubideak. Apartatu honetan aipatzen den hiru hilabeteko epea hogeita hamar egunera murriztuko da baldin eta ez bada errespetatzen erregelamendu honen 5. artikuluan aipatzen den AA-jardunbideen debekua.

9. Las autoridades de vigilancia del mercado velarán por que se adopten sin demora indebida las medidas restrictivas adecuadas respecto del producto o del sistema de IA de que se trate, tales como la retirada del producto o del sistema de IA de su mercado.

9. Merkatua zaintzeko agintaritzek zaindu egingo dute bidegabeko atzerapenik gabe hartzen direla AA-sistemari edo produktuari buruzko neurri murriztaile egokiak, hala nola AA-sistema edo produktua merkatutik erretiratzea.

Artículo 80.– Procedimiento aplicable a los sistemas de IA clasificados por el proveedor como no de alto riesgo en aplicación del anexo III

80. artikulua.– III. eranskina aplikatuz hornitzaileak arrisku handikotzat jotzen ez dituen AA-sistemei aplikatzekoa den prozedura

1. Cuando una autoridad de vigilancia del mercado tenga motivos suficientes para considerar que un sistema de IA que el proveedor haya clasificado como no de alto riesgo con arreglo al artículo 6, apartado 3, sí lo es, dicha autoridad realizará una evaluación del sistema de IA de que se trate por cuanto se refiere a su clasificación como sistema de IA de alto riesgo en función de las condiciones establecidas en el artículo 6, apartado 3, y las directrices de la Comisión.

1. Merkatua zaintzeko agintaritza batek nahikoa arrazoi duenean pentsatzeko hornitzaileak 6.3 artikuluaaren arabera arrisku handikotzat sailkatu ez duen AA-sistema bat badela arrisku handikoa, kasuan kasuko AA-sistemaren ebaluazioa egingo du agintaritza horrek, arrisku handiko AA-sistema gisa sailkatzeari dagokionez, 6.3 artikuluan eta Batzordearen gidalerroetan ezarritako baldintzak kontuan hartuta.

2. Cuando, al realizar dicha evaluación, la autoridad de vigilancia del mercado constate que el sistema de IA afectado es de alto riesgo, pedirá sin demora indebida al proveedor correspondiente que adopte todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones establecidos en el presente Reglamento, así como que adopte las medidas correctoras adecuadas en el plazo que la autoridad de vigilancia del mercado podrá determinar.

2. Ebaluazio hori egitean, merkatua zaintzeko agintaritzak egiaztatzen badu ukitutako AA-sistema arrisku handikoa dela, bidegabeko atzerapenik gabe eskatuko dio hornitzaileari beharrezkoak diren neurri guztiak har ditzala AA-sistemak erregelamendu honetan ezarritako betekizunak eta betebeharrak bete ditzan, eta neurri zuzentzaile egokiak har ditzala merkatua zaintzeko agintaritzak zehaztu ahal izango duen epean.



3. Cuando la autoridad de vigilancia del mercado considere que la utilización del sistema de IA afectado no se circunscribe a su territorio nacional, informará a la Comisión y a los demás Estados miembros sin demora indebida de los resultados de la evaluación y de las medidas que haya exigido al proveedor que adopte.

4. El proveedor se asegurará de que se adopten todas las medidas necesarias para que el sistema de IA cumpla los requisitos y obligaciones que se establecen en el presente Reglamento. Cuando el proveedor de un sistema de IA afectado no haga lo necesario para que cumpla dichos requisitos y obligaciones en el plazo a que se refiere el apartado 2 del presente artículo, se le impondrán multas de conformidad con el artículo 99.

5. El proveedor se asegurará de que se adopten todas las medidas correctoras adecuadas para todos los sistemas de IA afectados que haya comercializado en toda la Unión.

6. Cuando el proveedor del sistema de IA afectado no adopte las medidas correctoras adecuadas en el plazo a que se refiere el apartado 2 del presente artículo, se aplicará el artículo 79, apartados 5 a 9.

7. Cuando, al realizar la evaluación con arreglo al apartado 1 del presente artículo, la autoridad de vigilancia del mercado determine que el proveedor había clasificado erróneamente el sistema de IA como de no alto riesgo con el fin de eludir la aplicación de los requisitos establecidos en el capítulo III, sección 2, se impondrán multas al proveedor de conformidad con el artículo 99.

8. En el ejercicio de su facultad de supervisión de la aplicación del presente artículo, y de conformidad con el artículo 11 del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado podrán realizar los controles pertinentes, teniendo en cuenta, en particular, la información almacenada en la base de datos de la UE a que se refiere el artículo 71 del presente Reglamento.

Artículo 81.– Procedimiento de salvaguardia de la Unión

1. Cuando, en el plazo de tres meses desde la recepción de la notificación a que se refiere el artículo 79, apartado 5, o en el plazo de treinta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, la autoridad de vigilancia del mercado de un Estado miembro formule objeciones sobre una medida adoptada por otra autoridad de vigilancia del mercado, o cuando la Comisión considere que la medida es contraria al Derecho de la Unión, la Comisión entablará consultas sin demora indebida con la autoridad de vigilancia del mercado del Estado

3. Merkatua zaintzeko agintaritzak uste badu ukitutako AA-sistemaren erabilera ez dela haren lurralde nazionalera mugatzen, Batzordeari eta gainerako estatu kideei jakinaraziko dizkie, bidegabeko atzerapenik gabe, ebaluazioaren emaitzak eta hornitzaileari ezarri dizkion neurriak.

4. Hornitzaileak ziurtatuko du behar diren neurri guztiak hartzen direla erregelamendu honetan ezarritako betekizunak eta betebeharrak bete ditzan AA-sistemak. Ukitutako AA-sistema baten hornitzaileak ez badu behar dena egiten betekizun eta betebeharrak horiek artikuluko honen 2. apartatuan aipatutako epean bete ditzan, isunak ezarriko zaizkio 99. artikuluaekin bat etorritik.

5. Hornitzaileak ziurtatu egingo du Batasun osoan merkaturatu dituen ukitutako AA-sistema guztiei aplikatzen zaizkiela neurri zuzentzaile egoki guztiak.

6. Ukitutako AA-sistemaren hornitzaileak ez baditu neurri zuzentzaile egokiak hartzen artikuluko honen 2. apartatuan aipatzen den epean, 79. artikulua 5.etik 9.era bitarteko apartatuak aplikatuko dira.

7. Artikulu honen 1. apartatuaren arabera ebaluazioa egitean merkatua zaintzeko agintaritzak ondorioztatzen badu hornitzaileak ez zuela behar bezala sailkatu AA-sistema —arisku handikoa ez zela sailkatuta—, eta hala sailkatu izanaren helburua zela III. kapituluko 2. atalean ezarritako betekizunak aplikatu behar ez izatea, isunak ezarriko zaizkio hornitzaileari, 99. artikuluaekin bat etorritik.

8. Artikulu hau aplikatzen den gainbegiratzeko ahalmena baliatuz, eta bat etorritik (EB) 2019/1020 Erregelamenduaren 11. artikuluaekin, merkatua zaintzeko agintaritzek kontrol egokiak egin ahal izango dituzte, kontuan hartuta, bereziki, erregelamendu honen 71. artikuluan aipatzen den EBren datu-basean biltegiatutako informazioa.

81. artikulua.– Batasunaren babes-prozedura

1. Erregelamendu honen 79.5 artikuluan aipatzen den jakinarazpena jaso eta hiru hilabeteko epean, edo hogeita hamar eguneko epean 5. artikuluan aipatutako AA-jardunbideen debekua errespetatzen ez bada, estatu kide bateko merkatua zaintzeko agintaritzak eragozpenak jartzen baditu merkatua zaintzeko beste agintaritza batek hartutako neurri bati buruz, edo Batzordeak uste badu neurria Batasuneko zuzenbidearen aurkakoa dela, Batzordeak bidegabeko atzerapenik gabe egingo dizkie kontsultak dagokion estatu kideko merkatua zaintzeko agintaritzari eta



miembro pertinente y el operador u operadores, y evaluará la medida nacional. Basándose en los resultados de la mencionada evaluación, la Comisión decidirá, en un plazo de seis meses a partir de la notificación a que se refiere el artículo 79, apartado 5, o de sesenta días en caso de que no se respete la prohibición de las prácticas de IA a que se refiere el artículo 5, si la medida nacional está justificada y notificará su decisión a la autoridad de vigilancia del mercado del Estado miembro interesado. La Comisión informará también a las demás autoridades de vigilancia del mercado de su decisión.

2. Cuando la Comisión considere que la medida adoptada por el Estado miembro correspondiente está justificada, todos los Estados miembros se asegurarán de adoptar las medidas restrictivas adecuadas con respecto al sistema de IA de que se trate, como exigir la retirada del sistema de IA de su mercado sin demora indebida, e informarán de ello a la Comisión. Cuando la Comisión considere que la medida nacional no está justificada, el Estado miembro correspondiente retirará la medida e informará de ello a la Comisión.

3. Cuando se considere que la medida nacional está justificada y la no conformidad del sistema de IA se atribuya a deficiencias de las normas armonizadas o especificaciones comunes a las que se refieren los artículos 40 y 41 del presente Reglamento, la Comisión aplicará el procedimiento previsto en el artículo 11 del Reglamento (UE) n.º 1025/2012.

Artículo 82.– Sistemas de IA conformes que presenten un riesgo

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

2. El proveedor u otro operador pertinente se asegurará de que se adoptan medidas correctoras con respecto a todos los sistemas de IA afectados que haya comercializado en el mercado de la Unión en el plazo determinado por la autoridad de vigilancia del mercado del Estado miembro a que se refiere el apartado 1.

operadoreari edo operadoreei, eta neurri nazionala ebaluatuko du. Ebaluazio horren emaitzetan oinarrituta, Batzordeak sei hilabeteko epean erabakiko du, 79.5 artikuluan aipatzen den jakinarazpena egiten denetik zenbatzen hasita, edo hirurogei eguneko epean 5. artikuluan aipatutako AA-jardunbideen debekua errespetatzen ez bada, neurri nazionala justifikatuta dagoen, eta erabakiaren berri emango dio estatu kide interesduneko merkatua zaintzeko agintaritzari. Batzordeak merkatua zaintzeko gainerako agintariei ere emango die bere erabakiaren berri.

2. Batzordeak uste badu dagokion estatu kideak hartutako neurria justifikatuta dagoela, estatu kide guztiek ziurtatuko dute neurri murriztaile egokiak hartuko dituztela kasuan kasuko AA-sistemari dagokionez, hala nola AA-sistema bere merkatutik bidegabeko atzerapenik gabe erretiratzeko eskatzea, eta horren berri emango diote Batzordeari. Batzordeak uste badu neurri nazionala ez dagoela justifikatuta, dagokion estatu kideak neurria erretiratuko du, eta horren berri emango dio Batzordeari.

3. Uste denean neurri nazionala justifikatuta dagoela eta erregelamendu honen 40. eta 41. artikuluetan aipatzen diren arau harmonizatuen edo zehaztapen komunengatik inguruko hutsuneei egozten zaizkion AA-sistemaren adostasun-eza, (EB) 1025/2012 Erregelamenduaren 11. artikuluan aurreikusitako prozedura aplikatuko du Batzordeak.

82. artikulua.– Erregelamenduarekin ados etorri arren arriskua dakarten AA-sistemak

1. Baldin eta, 79. artikuluan xedatutakoaren arabera ebaluazioa egin eta 77.1 artikuluan aipatzen den agintaritzaren nazional publikoari kontsulta egin ondoren, estatu kide bateko merkatua zaintzeko agintaritzak ondorioztatzen badu arrisku handiko AA-sistema batek, erregelamendu hau bete arren, arriskua dakarrela pertsonen osasun edo segurtasunerako, oinarritzko eskubideetarako edo interes publikoa babesteko beste alderdi batzuetarako, operadore interesdunari eskatuko dio neurri guztiak har ditzala bermatzeko dena delako AA-sistemak ez duela arrisku hori izango merkatuan jartzen edo zerbitzuan ipintzen denean, bidegabeko atzerapenik gabe, agintaritzaren horrek zehaztu ahal izango duen epe baten barruan.

2. Hornitzaileak edo operadoreak ziurtatu egingo du neurri zuzentzaileak hartzen direla Batasuneko merkatuan merkaturatu dituen ukitutako AA-sistema guztiei dagokienez, 1. apartatuan aipatutako estatu kideko merkatua zaintzeko agintaritzak zehaztutako epean.



3. Los Estados miembros informarán inmediatamente a la Comisión y a los demás Estados miembros cuando se llegue a una conclusión en virtud del apartado 1. La información facilitada incluirá todos los detalles disponibles, en particular los datos necesarios para detectar el sistema de IA afectado y para determinar su origen y cadena de suministro, la naturaleza del riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

4. La Comisión entablará sin demora indebida consultas con los Estados miembros afectados y los operadores pertinentes y evaluará las medidas nacionales adoptadas. Basándose en los resultados de esta evaluación, la Comisión decidirá si la medida está justificada y, en su caso, propondrá otras medidas adecuadas.

5. La Comisión comunicará inmediatamente su decisión a los Estados miembros afectados y a los operadores pertinentes. Informará asimismo a los demás Estados miembros.

Artículo 83.– Incumplimiento formal

1. Cuando la autoridad de vigilancia del mercado de un Estado miembro constata una de las situaciones indicadas a continuación, exigirá al proveedor correspondiente que subsane el incumplimiento de que se trate, dentro de un plazo que dicha autoridad podrá determinar:

a) se ha colocado el marcado CE contraviniendo el artículo 48;

b) no se ha colocado el marcado CE;

c) no se ha elaborado la declaración UE de conformidad con el artículo 47;

d) no se ha elaborado correctamente la declaración UE de conformidad con el artículo 47;

e) no se ha efectuado el registro en la base de datos de la UE de conformidad con el artículo 71;

f) cuando proceda, no se ha designado a un representante autorizado;

g) no se dispone de documentación técnica.

2. Si el incumplimiento a que se refiere el apartado 1 persiste, la autoridad de vigilancia del mercado del Estado miembro de que se trate adoptará medidas adecuadas y proporcionadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o para

3. Estatu kideek berehala emango diete horren berri Batzordeari eta gainerako estatu kideei, ondorioen bat lortzen dutenean 1. apartatuari jarraikiz. Emandako informazioak eskura dauden xehetasun guztiak jasoko ditu, bereziki ukitutako AA-sistema detektatzeko beharrezkoak diren datuak, baita haren jatorria eta hornidura-katea, planteatutako arriskuaren izaera eta hartu diren neurri nazionalen izaera eta iraupena zehazteko beharrezkoak diren datuak ere.

4. Batzordeak, bidegabeko atzerapenik gabe, kontsultak egingo dizkie ukitutako estatu kideei eta kasuan kasuko operadoreei, eta hartu diren neurri nazionalak ebaluatuko ditu. Ebaluazio horren emaitzetan oinarrituta, neurria justifikatuta dagoen ala ez erabakiko du Batzordeak, eta, hala badagokio, beste neurri egoki batzuk proposatuko ditu.

5. Batzordeak berehala jakinaraziko die bere erabakia ukitutako estatu kideei eta kasuan kasuko operadoreei. Gainerako estatu kideei ere jakinaraziko die.

83. artikulua.– Formazko ez-betetzeak

1. Baldin eta estatu kide bateko merkatua zaintzeko agintaritzak jarraian adierazitako egoeretako bat egiaztatzen badu, dagokion hornitzaileari eskatuko dio ez-betetzea zuzen dezala, agintaritza horrek zehaztu ahal izango duen epean. Hauek izan daitezke ez-betetzea eragin dezaketen egoerak:

a) 48. artikuluan ezarritakoa urratuz jarri da CE marka;

b) ez da jarri CE marka;

c) ez da egin 47. artikuluen arabera EB adostasun-adierazpena;

d) EB adostasun-adierazpena ez da behar bezala egin 47. artikuluen arabera;

e) ez da erregistratu EBren datu-basean, 71. artikuluen arabera;

f) hala dagokiola, ez da izendatu ordezkari baimendu bat;

g) ez dago dokumentazio teknikorik.

2. Artikulu honen 1. apartatuan aipatzen den ez-betetzeak bere horretan jarraitzen badu, dagokion estatu kideko merkatua zaintzeko agintaritzak neurri egokiak eta proportzionatuak hartuko ditu arrisku handiko AA-sistemaren merkaturatzea murrizteko edo debekatze



asegurarse de que se recupera o retira del mercado sin demora.

Artículo 84.– Estructuras de apoyo a los ensayos de IA de la Unión

1. La Comisión designará una o varias estructuras de apoyo a los ensayos de IA de la Unión para realizar las actividades enumeradas en el artículo 21, apartado 6, del Reglamento (UE) 2019/1020 en el ámbito de la IA.
2. Sin perjuicio de las actividades a que se refiere el apartado 1, las estructuras de apoyo a los ensayos de IA de la Unión también proporcionarán asesoramiento técnico o científico independiente a petición del Consejo de IA, la Comisión o de las autoridades de vigilancia del mercado.

SECCIÓN 4

Vías de recurso

Artículo 85.– Derecho a presentar una reclamación ante una autoridad de vigilancia del mercado

Sin perjuicio de otras vías administrativas o judiciales de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el presente Reglamento podrá presentar reclamaciones ante la autoridad de vigilancia del mercado pertinente.

De conformidad con el Reglamento (UE) 2019/1020, tales reclamaciones se tendrán en cuenta a la hora de llevar a cabo actividades de vigilancia del mercado y se tramitarán de conformidad con los procedimientos específicos establecidos con este fin por las autoridades de vigilancia del mercado.

Artículo 86.– Derecho a explicación de decisiones tomadas individualmente

1. Toda persona que se vea afectada por una decisión que el responsable del despliegue adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada.

edo atzerapenik gabe berreskuratzen edo merkatutik erretiratzen dela ziurtatzeko.

84. artikulua.– Batasuneko AA-saiakuntzei sostengua emateko egiturak

1. Batzordeak egitura bat edo batzuk izendatuko ditu Batasuneko AA-saiakuntzei sostengua emateko (EB) 2019/1020 Erregelamenduaren 21.6 artikuluan zerrendatutako jarduerak egiteko AAren eremuan.
2. Artikulu honen 1. apartatuan aipatutako jardueren kalterik egin gabe, Batasuneko AA-saiakuntzei sostengua emateko egiturek aholkularitza tekniko edo zientifiko independentea ere emango dute, AA-kontseiluak, Batzordeak edo merkatua zaintzeko agintaritzek hala eskatuz gero.

4. ATALA

Errekurtso-bideak

85. artikulua.– Merkatua zaintzeko agintaritza bati erreklamazio bat aurkezteko eskubidea

Ezertan eragotzi gabe beste errekurtsobide administratibo edo judizial batzuei jarraitzeko aukera, erregelamendu honetan xedatutakoa urratu dela pentsatzeko arrazoiak dituen pertsona fisiko edo juridiko orok erreklamazioak aurkeztu ahal izango dizkio merkatua zaintzeko dagokion agintaritzari.

(EB) 2019/1020 Erregelamenduekin bat etorriz, erreklamazio horiek kontuan hartuko dira merkatua zaintzeko jarduerak egitean, eta merkatua zaintzeko agintaritzek horretarako ezarritako prozedura espezifikoen arabera izapidetuko dira.

86. artikulua.– Banaka hartutako erabakien inguruko azalpenak jasotzeko eskubidea

1. Erregelamendu honen III. eranskinean agertzen den arrisku handiko AA-sistema baten irteera-emaitzetan oinarrituta —alde batera utzita 2. puntuaren zerrendatutako sistemak— hedapenaren arduradunak hartzen duen erabaki batek ukitutako pertsona orok, baldin eta erabakiak ondorio juridikoak baditu edo haren eragin nabarmena jaso badu, eta uste badu kaltegarria dela bere osasunerako, segurtasunerako edo oinarritzko eskubideetarako, azalpen argi eta esanguratsuak eskatu ahal izango dizkio hedapenaren arduradunari, eta azken honek azaldu beharko dio ea zer zeregin izan duen AA-sistemak erabakiak hartzeko prozesuan eta zein izan diren hartutako erabakiaren elementu nagusiak.



2. No se aplicará el apartado 1 a la utilización de sistemas de IA para los que existan excepciones o restricciones a la obligación prevista en dicho apartado derivadas del Derecho de la Unión o nacional de conformidad con el Derecho de la Unión.

3. El presente artículo se aplicará únicamente en la medida en que el derecho a que se refiere el apartado 1 no esté previsto de otro modo en el Derecho de la Unión.

Artículo 87.— Denuncia de infracciones y protección de los denunciantes

La Directiva (UE) 2019/1937 se aplicará a la denuncia de infracciones del presente Reglamento y a la protección de las personas que denuncien tales infracciones.

SECCIÓN 5

Supervisión, investigación, cumplimiento y seguimiento respecto de proveedores de modelos de IA de uso general

Artículo 88.— Cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general

1. La Comisión tendrá competencias exclusivas para supervisar y hacer cumplir el capítulo V, teniendo en cuenta las garantías procedimentales previstas en el artículo 94. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de las competencias de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión en virtud de los Tratados.

2. Sin perjuicio de lo dispuesto en el artículo 75, apartado 3, las autoridades de vigilancia del mercado podrán solicitar a la Comisión que ejerza las facultades previstas en la presente sección, cuando resulte necesario y proporcionado para ayudar a que se lleven a cabo las actividades de su competencia en virtud del presente Reglamento.

Artículo 89.— Medidas de seguimiento

1. Con el fin de llevar a cabo los cometidos que se le atribuyen en la presente sección, la Oficina de IA podrá tomar las medidas necesarias para supervisar la aplicación y cumplimiento efectivos del presente Reglamento por parte de los proveedores de modelos de IA de uso general, incluida su observancia de los códigos de buenas prácticas aprobados.

2. AA-sistemen erabilerari ez zaio aplikatuko 1. apartatuan ezarritakoa baldin eta apartatu horretan aurreikusitako betebeharrerako salbuespenak edo murrizketak badaude Batasuneko zuzenbidetik edo zuzenbide nazionaletik eratorrita, Batasuneko zuzenbidearekin bat etorritz.

3. Artikulu hau soilik aplikatuko da baldin eta 1. apartatuan aipatzen den eskubidea beste modu batean aurreikusita ez badago Batasuneko zuzenbidean.

87. artikulua.— Arau-hausteen salaketa eta salatzaileen babes

(EB) 2019/1937 Zuzentaraua aplikatuko zaie erregelamendu honetako arau-hausteen salaketari eta arau-hauste horiek salatzen dituzten pertsonen babesari.

5. ATALA

Erabilera orokorreko AA-ereduen hornitzaileek betebeharrak betetzen dituzten gainbegiratzea, ikertzea eta horren jarraipena egitea

88. artikulua.— Erabilera orokorreko AA-ereduen hornitzaileek betebeharrak betetzen dituzten gainbegiratzea

1. Batzordeak eskumen eskusiboak izango ditu V. kapitulua gainbegiratzeko eta betearazteko, 94. artikuluan aurreikusitako prozedura-bermeak kontuan hartuta. Batzordeak AA-bulegoaren esku utzi behar ditu zeregin horiek, hargatik eragotzi gabe Batzordearen antolamendu-eskumenak eta estatu kideen eta Batasunaren arteko eskumen-banaketa, tratatuen arabera.

2. Erregelamendu honen 75.3 artikuluan xedatutakoari kalterik egin gabe, merkatua zaintzeko agintaritzek atal honetan aurreikusitako ahalmenak baliatzeko eskatu ahal izango diote Batzordeari, beharrezkoa eta neurrikoa denean erregelamendu honen arabera dituen bere eskumeneko jarduerak gauzatzen laguntzeko.

89. artikulua.— Jarraipen-neurriak

1. Atal honetan esleitzen zaizkion zereginak betetzeko, AA-bulegoak beharrezko neurriak hartu ahal izango ditu erabilera orokorreko AA-ereduen hornitzaileek erregelamendu hau —onartu diren jardunbide egokien kodeak barne— aplikatzen eta behar bezala betetzen duten gainbegiratzeko.



2. Los proveedores posteriores tendrán derecho a presentar reclamaciones alegando infracciones del presente Reglamento. Las reclamaciones deberán motivarse debidamente e indicar, como mínimo:

a) el punto de contacto del proveedor del modelo de IA de uso general de que se trate;

b) una descripción de los hechos, las disposiciones del presente Reglamento afectadas y los motivos por los que el proveedor posterior considera que el proveedor del modelo de IA de uso general de que se trate ha infringido el presente Reglamento;

c) cualquier otra información que el proveedor posterior que presente la reclamación considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

Artículo 90.– Alertas del grupo de expertos científicos sobre riesgos sistémicos

1. El grupo de expertos científicos podrá proporcionar alertas cualificadas a la Oficina de IA cuando tenga motivos para sospechar que:

a) un modelo de IA de uso general plantea un riesgo concreto reconocible a escala de la Unión, o

b) un modelo de IA de uso general reúne las condiciones a que se refiere el artículo 51.

2. Tras recibir dicha alerta cualificada, la Comisión podrá ejercer, a través de la Oficina de IA y tras haber informado al Consejo de IA, las facultades previstas en la presente sección con el fin de evaluar la cuestión. La Oficina de IA informará al Consejo de IA de cualquier medida que se adopte de conformidad con los artículos 91 a 94.

3. Las alertas cualificadas deberán motivarse debidamente e indicar, como mínimo:

a) el punto de contacto del proveedor del modelo de IA de uso general con riesgo sistémico de que se trate;

b) una descripción de los hechos y los motivos por los que el grupo de expertos científicos proporciona la alerta;

c) cualquier otra información que el grupo de expertos científicos considere pertinente, como, por ejemplo, en su caso, información que haya recopilado por iniciativa propia.

2. Ondorengo hornitzaileek erreklamazioak aurkezteko eskubidea izango dute, erregelamendu honen arau-hausteak alegatuz. Erreklamazioak behar bezala arrazoitu beharko dira, eta, gutxienez, datu hauek adierazi beharko dituzte:

a) kasuan kasuko erabilera orokorreko AA-ereduaren hornitzailearen harremanetarako gunea;

b) zer gertatu den, erregelamendu honetako zer xedapeni eragiten dion eta zergatik uste duen ondorengo hornitzaileak kasuan kasuko erabilera orokorreko AA-ereduaren hornitzaileak erregelamendu hau urratu duela;

c) erreklamazioa aurkezten duen ondorengo hornitzaileak egokitzen jotzen duen beste edozein informazio, hala nola, hala badagokio, bere ekimenez bildu duen informazioa.

90. artikulua.– Aditu zientifikoek taldeak arrisku sistemikoei buruz emandako alertak

1. Aditu zientifikoek taldeak alerta kualifikatuak eman ahal izango dizkio AA-bulegoari, egoera hauek susmatzeko arrazoiak dituenean:

a) erabilera orokorreko AA-eredu batek arrisku zehatz bat dakarrela, Batasunaren mailan ikusteko modukoa, edo

b) erabilera orokorreko AA-eredu batek 51. artikuluan aipatzen diren baldintzak betetzen dituela.

2. Alerta kualifikatu hori jaso ostean, Batzordeak, AA-bulegoaren bidez eta AA-kontseiluari jakinarazi ondoren, atal honetan aurreikusitako ahalmenak baliatu ahal izango ditu gaia ebaluatzeko. AA-bulegoak 91.etik 94.era bitarteko artikuluekin bat etorritik hartzen den edozein neurriren berri emango dio AA-kontseiluari.

3. Alerta kualifikatuak behar bezala arrazoitu beharko dira, eta, gutxienez, datu hauek adierazi beharko dituzte:

a) arrisku sistemikoa dakarren kasuan kasuko erabilera orokorreko AA-ereduaren hornitzailearen harremanetarako gunea;

b) zer gertatu den eta zergatik eman duen alerta aditu zientifikoek taldeak;

c) aditu zientifikoek taldeak egokitzen jotzen duen beste edozein informazio, hala nola, hala badagokio, bere ekimenez bildu duen informazioa.



Artículo 91.– Poderes para solicitar documentación e información

1. La Comisión podrá solicitar al proveedor del modelo de IA de uso general interesado que facilite la documentación preparada por el proveedor de conformidad con los artículos 53 y 55, o cualquier otra información que sea necesaria para evaluar el cumplimiento del presente Reglamento por parte del proveedor.
2. Antes de enviar la solicitud de información, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.
3. Cuando el grupo de expertos científicos presente la correspondiente solicitud debidamente motivada, la Comisión podrá dirigir al proveedor de un modelo de IA de uso general una solicitud de información si el acceso a dicha información resulta necesario y proporcionado para que el grupo de expertos científicos pueda llevar a cabo sus cometidos en virtud del artículo 68, apartado 2.
4. La solicitud de información indicará la base jurídica y la finalidad de la solicitud, precisará qué información se requiere, fijará el plazo en el que deberá facilitarse la información e indicará las multas que se establecen en el artículo 101 por facilitar información incorrecta, incompleta o engañosa.
5. El proveedor del modelo de IA de uso general interesado, o su representante, facilitará la información solicitada. De tratarse de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas facilitarán la información solicitada en nombre del proveedor del modelo de IA de uso general interesado. Los abogados debidamente habilitados podrán facilitar la información en nombre de sus representados. Los representados seguirán siendo, no obstante, plenamente responsables, si la información facilitada es incompleta, incorrecta o engañosa.

Artículo 92.– Poderes para realizar evaluaciones

1. La Oficina de IA, previa consulta al Consejo de IA, podrá realizar evaluaciones del modelo de IA de uso general de que se trate con el fin de:
 - a) evaluar si el proveedor cumple sus obligaciones en virtud del presente Reglamento, cuando la información recabada con arreglo al artículo 91 resulte insuficiente, o
 - b) investigar riesgos sistémicos a escala de la Unión de modelos de IA de uso general con riesgo

91. artikulua.– Dokumentazioa eta informazioa eskatzeko ahalak

1. Hornitzaileak 53. eta 55. artikuluen arabera prestatutako dokumentazioa emateko eskatu ahal izango dio Batzordeak erabilera orokorreko AA-ereduaren hornitzaile interesdunari; era berean, hornitzaileak erregelamendu hau betetzen duen ebaluatzeko beharrezkoa den beste edozein informazio ere eskatu ahal izango dio.
2. Informazio-eskaera bidali aurretik, AA-bulegoak elkarriketa egituratu bat hasi ahal izango du erabilera orokorreko AA-ereduaren hornitzailearekin.
3. Aditu zientifikoen taldeak behar bezala arrazoiutako eskaera aurkezten duenean, Batzordeak informazio-eskaera bat bidali ahal izango dio erabilera orokorreko AA-eredu baten hornitzaileari, baldin eta informazio hori eskuratzea beharrezkoa eta neurrikoa bada aditu zientifikoen taldeak bere eginkizunak bete ahal izan ditzan 68.2 artikuluan ezarritakoaren arabera.
4. Informazio-eskaeran, datu hauek adieraziko dira: zein diren eskaeraren oinarri juridikoa eta helburua, zer informazio eskatzen den, zer epe dagoen informazioa emateko eta zer isun ezar litezkeen, 101. artikuluari jarraikiz, informazio okerra, osatugabea edo engainagarria ematen bada.
5. Erabilera orokorreko AA-ereduaren hornitzaile interesdunak edo haren ordezkariak emango du eskatutako informazioa. Pertsona juridikoak, sozietateak edo enpresak badira, edo hornitzaileak nortasun juridikorik ez badu, legez edo estatutuen arabera haiek ordezkatzeko gaituta dauden pertsonak emango dute eskatutako informazioa erabilera orokorreko AA-ereduaren hornitzaile interesdunaren izenean. Behar bezala gaitutako abokatuek ere eman ahal izango dute informazioa beren ordezkatuaren izenean. Hala ere, ordezkatuak erantzukizun osoa izaten jarraituko dute, baldin eta emandako informazioa osatugabea, okerra edo engainagarria bada.

92. artikulua.– Ebaluazioak egiteko ahalak

1. AA-bulegoak, AA-kontseiluari kontsulta egin ondoren, kasuan kasuko erabilera orokorreko AA-ereduaren ebaluazioak egin ahal izango ditu, helburu hauekin:
 - a) ebaluatzea ea hornitzaileak erregelamendu honen arabera dituen betebeharrak betetzen dituen, 91. artikuluaen arabera bildutako informazioa nahikoa ez denean, edo
 - b) arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen Batasunaren mailako arrisku sistemikoak



sistémico, en particular a raíz de una alerta cualificada del grupo de expertos científicos de conformidad con el artículo 90, apartado 1, letra a).

2. La Comisión podrá decidir nombrar a expertos independientes para que realicen las evaluaciones en su nombre, también expertos científicos del grupo establecido de conformidad con el artículo 68. Los expertos independientes que se nombren para realizar estas tareas cumplirán los criterios establecidos en el artículo 68, apartado 2.

3. A los efectos del apartado 1, la Comisión podrá solicitar el acceso al modelo de IA de uso general de que se trate a través de API o de otros medios y herramientas técnicas adecuados, como, por ejemplo, el código fuente.

4. La solicitud de acceso indicará la base jurídica, la finalidad y los motivos de la solicitud, y fijará el plazo durante el que deberá facilitarse el acceso y las multas que se establecen en el artículo 101 por no facilitarlo.

5. Los proveedores del modelo de IA de uso general interesados o su representante facilitarán la información solicitada. En caso de que se trate de personas jurídicas, sociedades o empresas, o cuando el proveedor carezca de personalidad jurídica, las personas habilitadas por ley o por sus estatutos para representarlas, facilitarán el acceso solicitado en nombre del proveedor del modelo de IA de uso general interesado.

6. La Comisión adoptará actos de ejecución en los que se establezcan las modalidades detalladas y las condiciones de las evaluaciones, incluidas las disposiciones detalladas para la participación de expertos independientes y el procedimiento para su selección. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

7. Antes de solicitar el acceso al modelo de IA de uso general de que se trate, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general para recabar más información sobre los ensayos internos del modelo, las salvaguardias internas para prevenir los riesgos sistémicos y otros procedimientos y medidas internos que el proveedor haya adoptado para mitigar tales riesgos.

Artículo 93.— Poderes para solicitar la adopción de medidas

ikertzea, bereziki aditu zientifikoaren taldearen alerta kualifikatu baten ondorioz —90.1.a) artikulua arabera—.

2. Batzordeak aditu independenteak izendatu ahal izango ditu haren izenean egin ditzaten ebaluazioak; 68. artikulua arabera ezarritako taldeko aditu zientifikoak ere izendatu ahal izango ditu. Zeregin horiek egiteko izendatzen diren aditu independenteek 68.2 artikuluan ezarritako irizpideak bete beharko dituzte.

3. Artikulu honen 1. apartatuan ezarritakoaren ondorioetarako, erabilera orokorreko AA-eredurako sarbidea eskatu ahal izango du Batzordeak, API bidez edo beste bitarteko eta tresna tekniko egoki batzuen bidez —hala nola iturburu-kodearen bidez— sartu ahal izateko.

4. Sarbide-eskaeran, datu hauek adieraziko dira: zein diren eskaeraren oinarri juridikoa, helburua eta arrazoiak; zer epetan eman beharko den sarbidea, eta zer isun ezar litezkeen, 101. artikuluari jarraikiz, sarbiderik ematen ez bada.

5. Erabilera orokorreko AA-ereduaren hornitzaile interesdunek edo haien ordezkariak emango dute eskatutako informazioa. Pertsona juridikoak, sozietateak edo enpresak badira, edo hornitzaileak nortasun juridikorik ez badu, legez edo estatutuen arabera haiek ordezkatzeko gaituta dauden pertsonak emango dute eskatutako sarbidea erabilera orokorreko AA-ereduaren hornitzaile interesdunaren izenean.

6. Batzordeak betearazpen-egintzak hartuko ditu. Horietan, ebaluazioen modalitateak eta baldintzak zehaztuko dira, aditu independenteek parte hartzeko xedapen zehatzak eta horiek hautatzeko prozedura barne. Betearazpen-egintza horiek 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko dira.

7. Kasuan kasuko erabilera orokorreko AA-eredurako sarbidea eskatu aurretik, AA-bulegoak elkarrizketa egituratu bat hasi ahal izango du erabilera orokorreko AA-ereduaren hornitzailearekin, informazio gehiago biltzeko ereduaren barne-saiakuntzei buruz, arrisku sistemikoak prebenitzeko barne-babesei buruz eta hornitzaileak arrisku horiek arintzeko hartu dituen beste barne-prozedura eta -neurri batzuei buruz.

93. artikulua.— Neurriak hartzeko eskatzeko ahalak



1. Cuando resulte necesario y conveniente, la Comisión podrá solicitar a los proveedores que:

a) adopten las medidas oportunas para cumplir las obligaciones establecidas en los artículos 53 y 54;

b) apliquen medidas de reducción de riesgos cuando la evaluación realizada de conformidad con el artículo 92 apunte a que existen motivos serios y fundados de preocupación por la existencia de un riesgo sistémico a escala de la Unión;

c) restrinjan la comercialización del modelo, lo retiren o lo recuperen.

2. Antes de solicitar que se adopten medidas, la Oficina de IA podrá entablar un diálogo estructurado con el proveedor del modelo de IA de uso general.

3. Si, durante el diálogo estructurado a que se refiere el apartado 2, el proveedor del modelo de IA de uso general con riesgo sistémico se compromete a adoptar medidas de reducción para hacer frente a un riesgo sistémico a escala de la Unión, la Comisión podrá, mediante una decisión, hacer dichos compromisos vinculantes y declarar que no hay ya motivos para actuar.

Artículo 94.– Garantías procesales de los operadores económicos del modelo de IA de uso general

El artículo 18 del Reglamento (UE) 2019/1020 se aplicará *mutatis mutandis* a los proveedores del modelo de IA de uso general, sin perjuicio de las garantías procesales más específicas previstas en el presente Reglamento.

CAPÍTULO X

CÓDIGOS DE CONDUCTA Y DIRECTRICES

Artículo 95.– Códigos de conducta para la aplicación voluntaria de requisitos específicos

1. La Oficina de IA y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta, con los correspondientes mecanismos de gobernanza, destinados a fomentar la aplicación voluntaria de alguno o de todos los requisitos establecidos en el capítulo III, sección 2, a los sistemas de IA que no sean de alto riesgo, teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector que permitan la aplicación de dichos requisitos.

1. Beharrezkoa eta komenigarria denean, Batzordeak lan hauek egin ditzatela eskatu ahal izango die hornitzaileei:

a) neurri egokiak har ditzatela 53. eta 54. artikuluetan ezarritako betebeharrak betetzeko;

b) arriskuak murrizteko neurriak aplika ditzatela 92. artikulua arabera egindako ebaluazioak adierazten duenean kezkatzeko moduko arrazoi handi eta sendoak daudela arrisku sistemiko bat dagoelako Batasunaren mailan;

c) ereduaren merkaturatzea murriztu, erretiratu edo berreskura dezatela.

2. Neurriak hartzeko eskatu aurretik, AA-bulegoak elkarriketa egituratu bat hasi ahal izango du erabilera orokorreko AA-ereduaren hornitzailearekin.

3. Baldin eta, 2. apartatuan aipatzen den elkarriketa egituratuan, arrisku sistemikoa dakarren erabilera orokorreko AA-ereduaren hornitzaileak konpromisoa hartzen badu murrizketa-neurriak hartzeko Batasunaren mailako arrisku sistemiko bati aurre egiteko, Batzordeak, erabaki baten bidez, lotesle egin ahal izango ditu konpromiso horiek, eta jadanik jarduteko arrazoirik ez dagoela adierazi.

94. artikulua.– Erabilera orokorreko AA-ereduaren operadore ekonomikoen berme prozesalak

(EB) 2019/1020 Erregelamenduaren 18. artikulua *mutatis mutandis* aplikatuko zaie erabilera orokorreko AA-ereduaren hornitzaileei, hargatik eragotzi gabe erregelamendu honetan aurreikusitako berme prozesal espezifikagoak.

X. KAPITULUA

JOKABIDE-KODEAK ETA GIDALERROAK

95. artikulua.– Betekizun espezifikoak borondatez aplikatzeko jokabide-kodeak

1. AA-bulegoak eta estatu kideek jokabide-kodeak egitea sustatu eta erraztuko dute, dagozkien gobernantza-mekanismoak erabilita, arrisku handikoak ez diren AA-sistemei III. kapituluko 2. atalean ezarritako betekizunen bat edo guztiak borondatez aplikatzea sustatzeko, kontuan hartuta eskura dauden soluzio teknikoak eta betekizun horiek aplikatzea ahalbidetzen duten sektoreko jardunbide egokienak.



2. La Oficina de IA y los Estados miembros facilitarán la elaboración de códigos de conducta relativos a la aplicación voluntaria, también por parte de los responsables del despliegue, de requisitos específicos para todos los sistemas de IA, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos, incluidos, entre otros pero no exclusivamente, elementos como:

a) los elementos aplicables establecidos en las Directrices éticas de la Unión para una IA fiable;

b) la evaluación y reducción al mínimo de las repercusiones de los sistemas de IA en la sostenibilidad medioambiental, también por cuanto se refiere a la programación eficiente desde el punto de vista energético y las técnicas para diseñar, entrenar y utilizar la IA de manera eficiente;

c) la promoción de la alfabetización en materia de IA, en particular en el caso de las personas que se ocupan del desarrollo, funcionamiento y utilización de la IA;

d) la facilitación de un diseño inclusivo y diverso de los sistemas de IA, por ejemplo mediante la creación de equipos de desarrollo inclusivos y diversos y la promoción de la participación de las partes interesadas en dicho proceso;

e) la evaluación y prevención de los perjuicios de los sistemas de IA para las personas vulnerables o los colectivos de personas vulnerables, también por cuanto se refiere a accesibilidad para las personas con discapacidad, así como para la igualdad de género.

3. Los códigos de conducta podrán ser elaborados por proveedores o responsables del despliegue de sistemas de IA particulares, por las organizaciones que los representen o por ambos, también con la participación de cualquier parte interesada y sus organizaciones representativas, como, por ejemplo, las organizaciones de la sociedad civil y el mundo académico. Los códigos de conducta podrán comprender uno o varios sistemas de IA en función de la similitud de la finalidad prevista de los distintos sistemas.

4. La Oficina de IA y los Estados miembros tendrán en cuenta los intereses y necesidades específicos de las pymes, incluidas las empresas emergentes, a la hora de fomentar y facilitar la elaboración de códigos de conducta.

Artículo 96.– Directrices de la Comisión sobre la aplicación del presente Reglamento

2. AA-bulegoak eta estatu kideek erraztu egingo dute jokabide-kodeak egitea AA-sistema guztietarako betekizun espezifikoak borondatez aplikatzeari buruz —baita hedapenaren arduradunaren eskutik ere—, oinarri hartuta helburu argiak eta helburu horiek lortu diren neurtzeko emaitzen funtsezko adierazleak, besteak beste, baina ez soilik, elementu hauek barne:

a) AA fidagarri bat izateko Batasunaren gidalerro etikoetan ezarri diren aplikatzeko moduko elementuak;

b) AA-sistemek ingurumen-jasangarritasunean dituzten ondorioak ebaluatzea eta ahalik eta gehien murriztea, baita energiaren ikuspegitik eraginkorra den programazioari eta AA eraginkortasunez diseinatu, entrenatu eta erabiltzeko teknikei dagokienez ere;

c) AAren arloko alfabetatzea sustatzea, bereziki AAren garapen, funtzionamendu eta erabileraz arduratzen diren pertsonen kasuan;

d) AA-sistemen diseinu inklusibo eta askotarikoa erraztea, adibidez garapen-talde inklusibo eta askotarikoak sortuz eta prozesu horretan interesa duten alderdien parte-hartzea sustatuz;

e) AA-sistemek pertsona kalteberei edo pertsona kalteberen kolektiboek eragin diezaieketen kaltea ebaluatzea eta prebenitzea, baita desgaitasuna duten pertsonentzako irisgarritasunari eta genero-berdintasunari dagokienez ere.

3. Jokabide-kodeak egin ditzakete AA-sistemen hornitzaile edo hedapenaren arduradun partikularrek, haiek ordezkatzan dituzten antolakundeek edo biek; halaber, edozein alderdi interesdunek eta haiek ordezkatzan dituzten antolakundeek ere parte hartu ahal izango dute, hala nola gizarte zibileko eta mundu akademikoko antolakundeek. Jokabide-kodeak AA-sistema bat edo gehiago hartu ahal izango dituzte, kontuan hartuta zer-nolako antzekotasuna dagoen sistema horien helburu aurreikusien artean.

4. Jokabide-kodeak egitea sustatzeko eta errazteko orduan, AA-bulegoak eta estatu kideek kontuan hartuko dituzte ETEen interes eta beharrian espezifikoak —enpresa emergenteenak barne—.

96. artikulua.– Batzordeak erregelamendu hau aplikatzeko zehaztutako gidalerroak



1. La Comisión elaborará directrices sobre la aplicación práctica del presente Reglamento y, en particular, sobre:

a) la aplicación de los requisitos y obligaciones a que se refieren los artículos 8 a 15 y el artículo 25;

b) las prácticas prohibidas a que se refiere el artículo 5;

c) la aplicación práctica de las disposiciones relacionadas con modificaciones sustanciales;

d) la aplicación práctica de las obligaciones de transparencia establecidas en el artículo 50;

e) información detallada sobre la relación entre el presente Reglamento y la lista de actos legislativos de armonización de la Unión enumerados en el anexo I, así como otras disposiciones de Derecho de la Unión pertinentes, también por cuanto se refiere a la coherencia en su aplicación;

f) la aplicación de la definición de sistema de IA que figura en el artículo 3, punto 1.

Al publicar estas directrices, la Comisión prestará especial atención a las necesidades de las pymes, incluidas las empresas emergentes, de las autoridades públicas locales y de los sectores que tengan más probabilidades de verse afectados por el presente Reglamento.

Las directrices a que se refiere el párrafo primero del presente apartado tendrán debidamente en cuenta el estado de la técnica generalmente reconocido en materia de IA, así como las normas armonizadas y especificaciones comunes pertinentes a que se refieren los artículos 40 y 41, o las normas armonizadas o especificaciones técnicas que se establezcan con arreglo al Derecho de armonización de la Unión.

2. A petición de los Estados miembros o de la Oficina de IA, o por propia iniciativa, la Comisión actualizará las directrices anteriormente adoptadas cuando se considere necesario.

CAPÍTULO XI

DELEGACIÓN DE PODERES Y PROCEDIMIENTO DE COMITÉ

Artículo 97.— Ejercicio de la delegación

1. Batzordeak erregelamendu honen aplikazio praktikoari buruzko gidalerroak prestatuko ditu, eta, bereziki, alderdi hauek azalduko ditu:

a) 8.etik 15.era bitarteko artikuluetan eta 25. artikuluan aipatzen diren betekizunen eta betebeharren aplikazioa;

b) 5. artikuluan aipatzen diren jardunbide debekatuak;

c) funtsezko aldaketekin zerikusia duten xedapenen aplikazio praktikoa;

d) 50. artikuluan ezarritako gardentasun-betebeharren aplikazio praktikoa;

e) informazio zehatza erregelamendu honen eta I. eranskinean zerrendatuta dauden Batasunaren harmonizazioko lege-egintzen zerrendaren arteko harremanari buruz, bai eta Batasuneko zuzenbideko beste xedapen egoki batzuk ere, aplikazioaren koherentziari dagokionez;

f) 3.1 artikuluan ageri den AA-sistemaren definizioaren aplikazioa.

Gidalerro horiek argitaratzeko orduan, Batzordeak arreta berezia jarriko die ETEen —enpresa emergenteak barne—, tokiko agintaritzak publikoen eta erregelamendu honen eraginpean egoteko aukera handiena duten sektoreen beharrezan.

Apartatu honen lehenengo paragrafoan aipatzen diren gidalerroetan behar bezala hartuko dira kontuan AAren arloan oro har onartzen den teknikaren egoera, bai eta 40. eta 41. artikuluetan aipatzen diren arau harmonizatuak eta zehaztapen komunak ere, edo Batasuneko harmonizazio-zuzenbidearen arabera ezartzen diren arau harmonizatuak edo zehaztapen teknikoak.

2. Beharrezkotzat jotzen denean eguneratuko ditu Batzordeak aurretik hartutako jarraibideak, bere ekimenez edo Estatu kideek edo AA-bulegoak hala eskatuz gero.

XI. KAPITULUA

AHALAK ESKUORDETZEA ETA KOMITEAREN PROZEDURA

97. artikulua.— Eskuordetza egikaritzea



1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.
2. Los poderes para adoptar actos delegados mencionados en el artículo 6, apartado 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, se otorgan a la Comisión por un período de cinco años a partir del 1 de agosto de 2024. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.
3. La delegación de poderes mencionada en el artículo 6, apartados 6 y 7, el artículo 7, apartados 1 y 3, el artículo 11, apartado 3, el artículo 43, apartados 5 y 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, y el artículo 53, apartados 5 y 6, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada ella. No afectará a la validez de los actos delegados que ya estén en vigor.
4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.
5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.
6. Los actos delegados adoptados en virtud del artículo 6, apartados 6 o 7, el artículo 7, apartados 1 o 3, el artículo 11, apartado 3, el artículo 43, apartados 5 o 6, el artículo 47, apartado 5, el artículo 51, apartado 3, el artículo 52, apartado 4, o el artículo 53, apartados 5 o 6, entrarán en vigor únicamente si, en un plazo de tres meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 98.— Procedimiento de comité

1. Batzordeari ahalak ematen zaizkio egintza eskuordetuak hartzeko, artikulua honetan ezarritako baldintzetan.
2. Bost urterako ematen zaizkio Batzordeari, 2024ko abuztuaren 1etik aurrera, 6.6, 6.7, 7.1, 7.3, 11.3, 43.5, 43.6, 47.5, 51.3, 52.4, 53.5 eta 53.6 artikuluetan aipatutako egintza eskuordetuak hartzeko ahalak. Bost urteko aldia amaitu baino bederatzir hilabete lehenago, beranduenez, Batzordeak txosten bat egingo du ahalak eskuordetzeari buruz. Ahalen eskuordetzea isilbidez luzatuko da iraupen bereko aldietan, salbu eta Europako Parlamentuak edo Kontseiluak luzapen horren aurka egiten badute, aldi bakoitza amaitu baino hiru hilabete lehenago, beranduenez.
3. Europako Parlamentuak edo Kontseiluak edozein unetan errebokatu ahal izango ditu 6.6, 6.7, 7.1, 7.3, 11.3, 43.5, 43.6, 47.5, 51.3, 52.4, 53.5 eta 53.6 artikuluetan aipatzen diren ahalen eskuordetzeak. Errebokatzeko erabakiak amaiera emango dio bertan zehazten diren ahalak eskuordetzeari. Erabakia Europar Batasunaren Aldizkari Ofizialean argitaratu eta hurrengo egunean jarriko da indarrean, edo bertan adierazten den geroagoko data batean. Ez du eraginik izango jada indarrean dauden egintza eskuordetuen balioan.
4. Egintza eskuordetu bat onartu aurretik, Batzordeak kontsulta egingo die estatu kide bakoitzak izendatutako adituei, legeria hobetzeari buruzko 2016ko apirilaren 13ko erakundearteko akordioan ezarritako printzipioen arabera.
5. Batzordeak egintza eskuordetu bat hartu bezain laster, Europako Parlamentuari eta Kontseiluari jakinaraziko die, biei batera.
6. Erregelamendu honen 6.6, 6.7, 7.1, 7.3, 11.3, 43.5, 43.6, 47.5, 51.3, 52.4, 53.5 edo 53.6 artikuluen arabera hartutako egintza eskuordetuak indarrean jarriko dira, baldin eta, Europako Parlamentuari eta Kontseiluari jakinarazi eta hiru hilabeteko epean, instituzio horietako batek ere eragozpenik jartzen ez badu, edo epe hori amaitu baino lehen jakinarazten badiote bi instituzioek Batzordeari ez dutela eragozpenik jarriko. Epea hiru hilabetez luzatuko da, Europako Parlamentuak edo Kontseiluak hala eskatuz gero.

98. artikulua.— Komitearen prozedura



1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.
2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

CAPÍTULO XII

SANCIONES

Artículo 99.— Sanciones

1. De conformidad con las condiciones previstas en el presente Reglamento, los Estados miembros establecerán el régimen de sanciones y otras medidas de ejecución, como advertencias o medidas no pecuniarias, aplicable a las infracciones del presente Reglamento que cometan los operadores y adoptarán todas las medidas necesarias para garantizar que se aplican de forma adecuada y efectiva y teniendo así en cuenta las directrices emitidas por la Comisión con arreglo al artículo 96. Tales sanciones serán efectivas, proporcionadas y disuasorias. Tendrán en cuenta los intereses de las pymes, incluidas las empresas emergentes, así como su viabilidad económica.
2. Los Estados miembros comunicarán a la Comisión, sin demora y, como muy tarde, en la fecha de aplicación las normas referentes a las sanciones y otras medidas de ejecución mencionadas en el apartado 1 y la informarán, sin demora, de toda modificación de dichas normas.
3. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 35 000 000 EUR o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.
4. El incumplimiento de cualquiera de las disposiciones que figuran a continuación en relación con los operadores o los organismos notificados, distintas de los mencionados en el artículo 5, estará sujeto a multas administrativas de hasta 15 000 000 EUR o, si el infractor es una empresa, de hasta el 3 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior:

a) las obligaciones de los proveedores con arreglo al artículo 16;

1. Batzordeak Komite baten laguntza izango du. Komite horren adiera (EB) 182/2011 Erregelamenduak biltzen duena da.
2. Apartatu hau aipatzen denean, (EB) 182/2011 Erregelamenduaren 5. artikulua aplikatuko da.

XII. KAPITULUA

ZEHAPENAK

99. artikulua.— Zehapenak

1. Erregelamendu honetan aurreikusitako baldintzen arabera, estatu kideek zehapen-araubidea eta beste betearazpen-neurri batzuk ezarriko dituzte, hala nola ohartarazpenak edo diruzkoak ez diren neurriak, operadoreek erregelamendu hau hausten dutenean aplikatzeko, eta behar diren neurri guztiak hartuko dituzte behar bezala eta eraginkortasunez aplikatzen direla bermatzeko, Batzordeak emandako gidalerroak kontuan hartuta —96. artikulua—. Zehapenak eraginkorrak, proportzionatuak eta disuasiozkoak izango dira. Kontuan izango dituzte ETEen interesak —enpresa emergenteenak barne—, bai eta haien bideragarritasun ekonomikoa ere.
2. Estatu kideek Batzordeari jakinaraziko dizkiote, atzerapenik gabe eta beranduez aplikazio-datan, 1. apartatuan aipatutako zehapenei eta beste betearazpen-neurri batzuei buruzko arauak, eta atzerapenik gabe emango diote arau horien aldaketa guztien berri.
3. Erregelamendu honen 5. artikuluan aipatutako AA-jardunbideen debekua ez errespetatzeak 35 000 000 eurora arteko administrazio-isunak izango ditu, edo, arau-hauslea enpresa bat bada, aurreko finantza-ekitaldiari dagokion urteko mundu-mailako guztizko negozio-bolumenaren % 7ra artekoak, zenbateko hori handiagoa bada.
4. Albo batera utzita 5. artikuluan aipatutako xedapenak, operadore edo organismo jakinaraziren batek ez badu betetzen jarraian adierazi den beste edozein xedapen, 15 000 000 eurora arteko administrazio-isunak ezarriko zaizkio, edo, arau-hauslea enpresa bat bada, aurreko finantza-ekitaldiari dagokion urteko mundu-mailako guztizko negozio-bolumenaren % 3ra artekoak, zenbateko hori handiagoa bada. Hona hemen:

a) 16. artikulua arabera hornitzaileek dituzten betebeharrak;



b) las obligaciones de los representantes autorizados con arreglo al artículo 22;

c) las obligaciones de los importadores con arreglo al artículo 23;

d) las obligaciones de los distribuidores con arreglo al artículo 24;

e) las obligaciones de los responsables del despliegue con arreglo al artículo 26;

f) los requisitos y obligaciones de los organismos notificados con arreglo al artículo 31, al artículo 33, apartados 1, 3 y 4, o al artículo 34;

g) las obligaciones de transparencia de los proveedores y responsables del despliegue con arreglo al artículo 50.

5. La presentación de información inexacta, incompleta o engañosa a organismos notificados o a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 7 500 000 EUR o, si el infractor es una empresa, de hasta el 1 % del volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior.

6. En el caso de las pymes, incluidas las empresas emergentes, cada una de las multas a que se refiere el presente artículo podrá ser por el porcentaje o el importe a que se refieren los apartados 3, 4 y 5, según cuál de ellos sea menor.

7. Al decidir la imposición de una multa administrativa y su cuantía en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación de que se trate y, en su caso, se tendrá en cuenta lo siguiente:

a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA y, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;

b) si otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por la misma infracción;

c) si otras autoridades han impuesto ya multas administrativas al mismo operador por infracciones de otros actos legislativos nacionales o de la Unión, cuando dichas infracciones se deriven de la misma actividad u omisión que constituya una infracción pertinente del presente Reglamento;

b) 22. artikuluaaren arabera ordezkari baimenduek dituzten betebeharrak;

c) 23. artikuluaaren arabera inportatzaileek dituzten betebeharrak;

d) 24. artikuluaaren arabera banatzaileek dituzten betebeharrak;

e) 26. artikuluaaren arabera hedapenaren arduradunek dituzten betebeharrak;

f) 31., 33.1, 33.3, 33.4 eta 34. artikuluen arabera organismo jakinaraziek dituzten betekizunak eta betebeharrak;

g) 50. artikuluaaren arabera hornitzaileek eta hedapenaren arduradunek dituzten gardentasun-betebeharrak.

5. Eskaera bati erantzunez organismo jakinaraziei edo agintaritza nazional eskudunei emandako informazioa zehaztasunik gabea, osatugabea edo engainagarria bada, 7 500 000 eurora arteko administrazio-isunak ezarriko dira, edo, arau-hauslea enpresa bat bada, aurreko finantza-ekitaldiari dagokion urteko mundu-mailako guztizko negozio-bolumenaren % 1era artekoak, zenbateko hori handiagoa bada.

6. ETEen kasuan —enpresa emergenteak barne—, artikulua honetan aipatzen diren isunak ezartzean, 3., 4. eta 5. apartatueta aipatzen diren zenbatekoak edo ehunekoak hartu ahal izango dira kontuan, txikiena zein den.

7. Administrazio-isun bat ezarri eta haren zenbatekoa erabakitzeke, kasu zehatz bakoitzeko egoeraren inguruabar guztiak aztertuko dira, eta, hala badagokio, alderdi hauek hartuko dira kontuan:

a) zein diren arau-haustearen eta haren ondorioen izaera, larritasuna eta iraupena, AA-sistemaren helburua kontuan hartuta, eta, hala dagokionean, zenbat pertsonak izan duen eragina eta zein izan den kalteen maila;

b) ea merkatua zaintzeko beste agintaritza batzuek administrazio-isunak jarri dizkioten operadore berari arau-hauste beraren ondorioz;

c) ea beste agintaritza batzuek administrazio-isunak jarri dizkioten operadore berari beste lege-egintza batzuk urratzeagatik —Batasunekoak edo nazionalak—, baldin eta arau-hauste horiek erregelamendu honen arau-hauste den jardura edo ez-egite beretik badatoz;



d) el tamaño, el volumen de negocios anual y la cuota de mercado del operador que comete la infracción;

e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción;

f) el grado de cooperación con las autoridades nacionales competentes con el fin de subsanar la infracción y mitigar sus posibles efectos adversos;

g) el grado de responsabilidad del operador, teniendo en cuenta las medidas técnicas y organizativas aplicadas por este;

h) la forma en que las autoridades nacionales competentes tuvieron conocimiento de la infracción, en particular si el operador notificó la infracción y, en tal caso, en qué medida;

i) la intencionalidad o negligencia en la infracción;

j) las acciones emprendidas por el operador para mitigar los perjuicios sufridos por las personas afectadas.

8. Cada Estado miembro establecerá normas que determinen en qué medida es posible imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

9. En función del ordenamiento jurídico de los Estados miembros, las normas relativas a las multas administrativas podrán aplicarse de tal modo que las multas las impongan órganos jurisdiccionales nacionales competentes u otros organismos, según proceda en dichos Estados miembros. La aplicación de dichas normas en estos Estados miembros tendrá un efecto equivalente.

10. El ejercicio de poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y nacional, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

11. Los Estados miembros informarán anualmente a la Comisión de las multas administrativas que hayan impuesto durante ese año de conformidad con el presente artículo y de cualquier litigio o proceso judicial relacionados.

Artículo 100.– Multas administrativas a instituciones, órganos y organismos de la Unión

d) zein diren arau-haustea egin duen operadorearen tamaina, urteko negozio-bolumena eta merkatu-kuota;

e) kasuaren inguruabarrei aplikatzekoa zaien beste edozein faktore astungarri edo leungarri, hala nola arau-haustearen bitartez —zuzenean edo zeharka— lortu diren finantza-onurak edo saihestu diren galerak;

f) zenbateko lankidetza ematen dieten agintaritza nazional eskudunei arau-haustea zuzentzeko eta izan ditzakeen ondorio kaltegarriak arintzeko;

g) operadorearen erantzukizun-maila, aplikatu dituen neurri teknikoak eta antolakuntzakoak kontuan hartuta;

h) agintaritza nazional eskudunek nola jakin duten arau-haustearen berri, batez ere operadoreak arau-haustea jakinarazi duen ala ez, eta, hala bada, zer neurritan;

i) arau-haustean intentzionalitaterik edo zabarkeriarik egon den;

j) operadoreak zer ekintza jarri duen abian ukitutako pertsonen jasandako kalteak arintzeko.

8. Estatu kide bakoitzak bere arauak ezarriko ditu estatu kide horretan kokatutako agintaritza eta organismo publikoei administrazio-isunak zein neurritan jarriko zaizkien zehazteko.

9. Estatu kideen ordenamendu juridikoaren arabera, administrazio-isunei buruzko arauak aplikatzean, jurisdikzio-organo eskudunek edo beste organismo batzuek ezarri ahal izango dituzte isunak, estatu kide bakoitzean egoki denaren arabera. Arau horiek estatu kide horietan aplikatzeak ondorio baliokidea izango du.

10. Artikulu honi jarraituz ahalak egikaritu ahal izateko, nahitaez bete beharko dira Batasuneko zuzenbidearekin eta zuzenbide nazionalarekin bat etorritz ezarritako berme prozesal egokiak, barne hartuta benetako babes judiziala eta berme prozesalen errespetua.

11. Estatu kideek urtero jakinaraziko dizkiote Batzordeari zenbat administrazio-isun ezarri dituzten urte horretan artikulu honen ondorioz eta zenbat auzi edo prozesu judizial dauden horrekin lotuta.

100. artikulua.– Administrazio-isunak jartzea Batasuneko instituzio, organo eta organismoiei



1. El Supervisor Europeo de Protección de Datos podrá imponer multas administrativas a las instituciones, órganos y organismos de la Unión comprendidos en el ámbito de aplicación del presente Reglamento. Al decidir la imposición de una multa administrativa y su cuantía en cada caso concreto se tomarán en consideración todas las circunstancias pertinentes de la situación de que se trate y se tendrá debidamente en cuenta lo siguiente:

a) la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias, teniendo en cuenta la finalidad del sistema de IA de que se trate, así como, cuando proceda, el número de personas afectadas y el nivel de los daños que hayan sufrido;

b) el grado de responsabilidad de la institución, órgano u organismo de la Unión, teniendo en cuenta las medidas técnicas y organizativas aplicadas;

c) las acciones emprendidas por la institución, órgano u organismo de la Unión para mitigar los perjuicios sufridos por las personas afectadas;

d) el grado de cooperación con el Supervisor Europeo de Protección de Datos con el fin de subsanar la infracción y mitigar sus posibles efectos adversos, incluido el cumplimiento de cualquiera de las medidas que el propio Supervisor Europeo de Protección de Datos haya ordenado previamente contra la institución, órgano u organismo de la Unión de que se trate en relación con el mismo asunto;

e) toda infracción anterior similar cometida por la institución, órgano u organismo de la Unión;

f) la forma en que el Supervisor Europeo de Protección de Datos tuvo conocimiento de la infracción, en particular si la institución, órgano u organismo de la Unión notificó la infracción y, en tal caso, en qué medida;

g) el presupuesto anual de la institución, órgano u organismo de la Unión.

2. El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 1 500 000 EUR.

3. El incumplimiento por parte del sistema de IA de cualquiera de los requisitos u obligaciones establecidos en el presente Reglamento, distintos de los previstos en el artículo 5, estará sujeto a multas administrativas de hasta 750 000 EUR.

4. Antes de tomar ninguna decisión en virtud del presente artículo, el Supervisor Europeo de Protección de Datos ofrecerá a la institución, órgano u organismo

1. Datuak Babesteko Europako Ikuskatzaileak administrazio-isunak ezarri ahal izango dizkie erregelamendu honen aplikazio-eremuan sartzen diren Batasuneko instituzio, organo eta organismoei. Administrazio-isun bat ezarri eta haren zenbatekoa erabakitzeak, kasu zehatz bakoitzeko egoeraren inguruabar guztiak aztertuko dira, eta alderdi hauek hartuko dira kontuan:

a) zein diren arau-haustearen eta haren ondorioen izaera, larritasuna eta iraupena, AA-sistemaren helburua kontuan hartuta, eta, hala dagokionean, zenbat pertsonak izan duen eragina eta zein izan den kalteen maila;

b) Batasuneko instituzio, organo edo organismoaren erantzukizun-maila, aplikatu dituen neurri teknikoak eta antolakuntzakoak kontuan hartuta;

c) Batasuneko instituzio, organo edo organismoak zer ekintza jarri duen abian ukitutako pertsonen jasandako kalteak arintzeko;

d) zenbateko lankidetzak ematen dieten Datuak Babesteko Europako Ikuskatzaileari arau-haustea zuzentzeko eta izan ditzakeen ondorio kaltegarriak arintzeko, barne hartuta Datuak Babesteko Europako Ikuskatzaileak berak Batasuneko instituzio, organo edo organismo horren aurka gai beraren inguruan aldeztu aurretik agindutako edozein neurri betetzea;

e) Batasuneko instituzio, organo edo organismoak aurretik egindako antzeko arau-hauste oro;

f) Datuak Babesteko Europako Ikuskatzaileak nola jakin duen arau-haustearen berri, batez ere Batasuneko instituzio, organo edo organismoak arau-haustea jakinarazi duen ala ez, eta, hala bada, zer neurritan;

g) Batasuneko instituzio, organo edo organismoaren urteko aurrekontua.

2. Erregelamendu honen 5. artikuluan aipatutako AA-jardunbideen debekua ez errespetatzeak 1 500 000 eurora arteko administrazio-isunak izango ditu.

3. Albo batera utzita 5. artikuluan aurreikusitakoak, AA-sistema batek ez badu betetzen erregelamendu honetan ezarritako beste edozein betekizun edo betebeharrak, 750 000 eurora arteko administrazio-isunak ezarriko zaizkio.

4. Datuak Babesteko Europako Ikuskatzaileak, artikulua honen arabera erabakirik hartu aurretik, balizko arau-hausteari buruz entzuna izateko aukera



de la Unión sometida al procedimiento instruido por el Supervisor Europeo de Protección de Datos la oportunidad de ser oída en lo que respecta a la posible infracción. El Supervisor Europeo de Protección de Datos basará sus decisiones únicamente en los elementos y las circunstancias sobre los que las partes afectadas hayan podido manifestarse. Los denunciantes, si los hay, participarán estrechamente en el procedimiento.

5. Los derechos de defensa de las partes estarán garantizados plenamente en el curso del procedimiento. Tendrán derecho a acceder al expediente del Supervisor Europeo de Protección de Datos, sin perjuicio del interés legítimo de las personas físicas y las empresas en la protección de sus datos personales o secretos comerciales.

6. La recaudación proveniente de la imposición de multas con arreglo al presente artículo contribuirá al presupuesto general de la Unión. Las multas no afectarán al funcionamiento efectivo de la institución, órgano u organismo de la Unión sancionado.

7. El Supervisor Europeo de Protección de Datos informará anualmente a la Comisión de las multas administrativas que haya impuesto en virtud del presente artículo y de cualquier litigio o proceso judicial que haya iniciado.

Artículo 101.– Multas a proveedores de modelos de IA de uso general

1. La Comisión podrá imponer multas a los proveedores de modelos de IA de uso general que no superen el 3 % de su volumen de negocios mundial total anual correspondiente al ejercicio financiero anterior o de 15 000 000 EUR, si esta cifra es superior, cuando la Comisión considere que, de forma deliberada o por negligencia:

- a) infringieron las disposiciones pertinentes del presente Reglamento;
- b) no atendieron una solicitud de información o documentos con arreglo al artículo 91, o han facilitado información inexacta, incompleta o engañosa;
- c) incumplieron una medida solicitada en virtud del artículo 93;
- d) no dieron acceso a la Comisión al modelo de IA de uso general o al modelo de IA de uso general con riesgo sistémico para que se lleve a cabo una evaluación con arreglo al artículo 92.

emango dio Datuak Babesteko Europako Ikuskatzaileak bideratutako prozeduraren mende dagoen Batasuneko instituzio, organo edo organismoari. Ukitutako aldeek adierazi ahal izan dituzten elementuetan eta inguruabarretan soilik oinarrituko ditu erabakiak Datuak Babesteko Europako Ikuskatzaileak. Salatzaileek, halakorik balego, parte-hartze estua izango dute prozeduran.

5. Prozeduran zehar, erabat bermatuta egongo dira aldean defentsa-eskubideak. Datuak Babesteko Europako Ikuskatzailearen espedienteak eskuratzeko eskubidea izango dute, ezertan galarazi gabe pertsona fisikoek eta enpresek beren datu pertsonalak edo merkataritza-sekretuak babesteko duten interes legítimoak.

6. Artikulu honen arabera ezarritako isunen ondorioz bildutako dirua Batasunaren aurrekontu orokorrean sartuko da. Isunek ez dute eraginik izango zehapena izan duen Batasuneko instituzio, organo edo organismoaren benetako funtzionamenduan.

7. Datuak Babesteko Europako Ikuskatzaileak urtero jakinaraziko dizkio Batzordeari zenbat administrazio-isun ezarri dituen urte horretan artikulu honen ondorioz eta zenbat auzi edo prozesu judicial hasi diren.

101. artikulua.– Isunak ezartzea erabilera orokorreko AA-ereduen hornitzaileei

1. Batzordeak isunak ezarri ahal izango dizkie erabilera orokorreko AA-ereduen hornitzaileei, baldin eta aurreko finantza-ekitaldiari dagokion urteko mundu-mailako guztizko negozio-bolumenaren % 3 gainditzen ez badute, edo 15 000 000 euro gainditzen ez badituzte, zenbateko hori handiagoa bada, Batzordeak uste duenean hemen aipatutakoren bat egin dutela, nahita edo zabarkeriaren ondorioz:

- a) erregelamendu honetako xedapenak urratu zituzten;
- b) ez zioten erantzun 91. artikuluaaren arabera egindako informazio- edo dokumentu-eskaeraren bati, edo informazio zehaztugabea, osatugabea edo egainagarria eman zuten;
- c) ez zuten bete 93. artikuluaaren arabera eskatutako neurriren bat;
- d) Batzordeari ez zioten sarbiderik eman erabilera orokorreko AA-eredura edo arrisku sistemikoa dakarren erabilera orokorreko AA-eredura sartzeko, 92. artikuluaaren arabera ebaluazioa egiteko.



Al fijar el importe de la multa o de la multa coercitiva, se tomarán en consideración la naturaleza, gravedad y duración de la infracción, teniendo debidamente en cuenta los principios de proporcionalidad y adecuación. La Comisión también tendrá en cuenta los compromisos contraídos de conformidad con el artículo 93, apartado 3, y en los códigos de buenas prácticas pertinentes previstos en el artículo 56.

2. Antes de adoptar una decisión con arreglo al apartado 1, la Comisión comunicará sus conclusiones preliminares al proveedor del modelo de IA de uso general o del modelo de IA y le dará la oportunidad de ser oído.

3. Las multas impuestas de conformidad con el presente artículo serán efectivas, proporcionadas y disuasorias.

4. La información sobre las multas impuestas en virtud del presente artículo también se comunicará al Consejo de IA, según proceda.

5. El Tribunal de Justicia de la Unión Europea tendrá plena competencia jurisdiccional para examinar las decisiones de imposición de una multa adoptadas por la Comisión en virtud del presente artículo. Podrá anular, reducir o incrementar la cuantía de la multa impuesta.

6. La Comisión adoptará actos de ejecución que contengan disposiciones detalladas y garantías procesales para los procedimientos con vistas a la posible adopción de decisiones con arreglo al apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO XIII

DISPOSICIONES FINALES

Artículo 102.– Modificación del Reglamento (CE) n.o 300/2008

En el artículo 4, apartado 3, del Reglamento (CE) n.o 300/2008, se añade el párrafo siguiente:

«Al adoptar medidas detalladas relativas a las especificaciones técnicas y los procedimientos de aprobación y utilización del equipo de seguridad en relación con sistemas de inteligencia artificial en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Isunaren edo hertsatzeko isunaren zenbatekoa finkatzean, aztertu egingo dira arau-haustearen izaera, larritasuna eta iraupena, proportzionaltasun- eta egokitasun-printzipioak behar bezala kontuan hartuta. Batzordeak kontuan hartuko ditu, halaber, 93.3 artikuluekin bat etorritik hartutako konpromisoak, bai eta 56. artikuluan aurreikusitako jardunbide egokien kodeetan hartutakoak ere.

2. Artikulu honen 1. apartatuari jarraikiz erabaki bat hartu aurretik, Batzordeak aurretiazko ondorioak jakinaraziko dizkio erabilera orokorreko AA-ereduaren edo AA-ereduaren hornitzaileari, eta entzuna izateko aukera emango dio.

3. Artikulu honen arabera ezarritako isunak eraginkorrak, proportzionatuak eta disuasiozkoak izango dira.

4. Artikulu honen arabera ezarritako isunei buruzko informazioa AA-kontseiluari ere jakinaraziko zaio, dagokionaren arabera.

5. Europar Batasuneko Justizia Auzitegiak jurisdikzio-eskumen osoa izango du Batzordeak artikuluan honen arabera isunak ezartzeko hartutako erabakiak aztertzeko. Isuna baliogabetzeko edo zenbatekoa txikitu zein handitzeko eskumena izango du.

6. Batzordeak xedapen zehatzak eta berme prozesalak jasoko dituzten betearazpen-egintzak hartuko ditu, erabakiak hartu ahal izan daitezen artikuluan honetako 1. apartatuan ezarritakoa betez. Betearazpen-egintza horiek 98.2 artikuluan aipatzen den azterketa-prozedurari jarraituz hartuko dira.

XIII. KAPITULUA

AZKEN XEDAPENAK

102. artikulua.– (EB) 300/2008 Erregelamendua aldatzea

(EE) 300/2008 Erregelamenduaren 4.3 artikuluan, paragrafo hau eranstean da:

«Adimen artifizialeko sistemei dagokienez, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1689 Erregelamenduaren zentzuan (*), segurtasun-ekipoaren zehaztapen teknikoei eta onespen- eta erabilera-prozedurei buruzko neurri zehatzak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».



Artículo 103.– Modificación del Reglamento (UE) n.o 167/2013

En el artículo 17, apartado 5, del Reglamento (UE) n.o 167/2013, se añade el párrafo siguiente:

«Al adoptar actos delegados en virtud del párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 104.– Modificación del Reglamento (UE) n.o 168/2013

En el artículo 22, apartado 5, del Reglamento (UE) n.o 168/2013, se añade el párrafo siguiente:

«Al adoptar actos delegados en virtud del párrafo primero relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 105.– Modificación de la Directiva 2014/90/UE

En el artículo 8 de la Directiva 2014/90/UE, se añade el apartado siguiente:

«5. En el caso de los sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), la Comisión tendrá en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento al desempeñar sus actividades con arreglo al apartado 1 y al adoptar especificaciones técnicas y normas de ensayo de conformidad con los apartados 2 y 3.

Artículo 106.– Modificación de la Directiva (UE) 2016/797

En el artículo 5 de la Directiva (UE) 2016/797, se añade el apartado siguiente:

«12. Al adoptar actos delegados en virtud del apartado 1 y actos de ejecución en virtud del apartado 11 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos

103. artikulua.– (EB) 167/2013 Erregelamendua aldatzea

(EB) 167/2013 Erregelamenduaren 17.5 artikuluan, paragrafo hau eranstean da:

«Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1689 Erregelamenduaren zentzuan (*), lehenengo paragrafoari jarraikiz egintza eskuordetuak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

104. artikulua.– (EB) 168/2013 Erregelamendua aldatzea

(EB) 168/2013 Erregelamenduaren 22.5 artikuluan, paragrafo hau eranstean da:

«Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1689 Erregelamenduaren zentzuan (*), lehenengo paragrafoari jarraikiz egintza eskuordetuak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

105. artikulua.– 2014/90/EB Zuzentaraua aldatzea

2014/90/EB Zuzentarauaren 8. artikuluan, apartatu hau eranstean da:

«5. Segurtasun-osagaiak diren adimen artifizialeko sistemen kasuan, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1689 Erregelamenduaren zentzuan (*), Batzordeak, 1. apartatuaren arabera jarduerak gauzatzean eta 2. eta 3. apartatuen arabera zehaztuen teknikoak eta saiakuntza-arauak hartzean, kontuan hartuko ditu erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

106. artikulua.– (EB) 2016/797 Zuzentaraua aldatzea

(EB) 2016/797 Zuzentarauaren 5. artikuluan, apartatu hau eranstean da:

«12. Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1689 Erregelamenduaren zentzuan (*), 1. apartatuari jarraikiz egintza eskuordetuak hartzean eta 11. apartatuari jarraikiz betearazpen-egintzak hartzean, kontuan hartuko dira



establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 107.– Modificación del Reglamento (UE) 2018/858

En el artículo 5 del Reglamento (UE) 2018/858, se añade el apartado siguiente:

«4. Al adoptar actos delegados en virtud del apartado 3 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/... del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 108.– Modificación del Reglamento (UE) 2018/1139

El Reglamento (UE) 2018/1139 se modifica como sigue:

1) En el artículo 17, se añade el apartado siguiente:

«3. Sin perjuicio de lo dispuesto en el apartado 2, al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

(*) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) ([DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj](https://data.europa.eu/eli/reg/2024/1689/oj)).».

2) En el artículo 19, se añade el apartado siguiente:

«4. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

3) En el artículo 43, se añade el apartado siguiente:

«4. Al adoptar actos de ejecución en virtud del apartado 1 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del

erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

107. artikulua.– (EB) 2018/858 Erregelamendua aldatzea

(EB) 2018/858 Erregelamenduaren 5. artikuluan, apartatu hau eransten da:

«4. Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/... Erregelamenduaren zentzuan (*), 3. apartatuari jarraikiz egintza eskuordetuak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

108. artikulua.– (EB) 2018/1139 Erregelamendua aldatzea

(EB) 2018/1139 Erregelamendua honela aldatzen da:

1) 17. artikuluan, apartatu hau eransten da:

«3. Artikulu honen 2. apartatuan xedatutakoa alde batera utzi gabe, segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1689 Erregelamenduaren zentzuan (*), 1. apartatuari jarraikiz betearazpen-egintzak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak.

(*) (EB) 2024/1689 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2024ko ekainaren 13koa, adimen artifizialaren arloan arau harmonizatuak ezartzen dituen eta (EE) 300/2008, (EB) 167/2013, (EB) 168/2013, (EB) 2018/858, (EB) 2018/1139 eta (EB) 2019/2144 erregelamenduak eta 2014/90/EB, (EB) 2016/797 eta (EB) 2020/1828 zuzentarauak aldatzen dituen (Adimen Artifizialari buruzko Erregelamendua) ([2024/07/12ko EBAO, L, 2024/1689, ELI: http://data.europa.eu/eli/reg/2024/1689/oj](https://data.europa.eu/eli/reg/2024/1689/oj)).».

2) 19. artikuluan, apartatu hau eransten da:

«4. Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, (EB) 2024/1689 Erregelamenduaren zentzuan, 1. eta 2. apartatuei jarraikiz egintza eskuordetuak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

3) 43. artikuluan, apartatu hau eransten da:

«4. Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, (EB) 2024/1689 Erregelamenduaren zentzuan, 1. apartatuari jarraikiz



Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

4) En el artículo 47, se añade el apartado siguiente:

«3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

5) En el artículo 57, se añade el párrafo siguiente:

«Al adoptar dichos actos de ejecución relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

6) En el artículo 58, se añade el apartado siguiente:

«3. Al adoptar actos delegados en virtud de los apartados 1 y 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689, se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.».

Artículo 109.– Modificación del Reglamento (UE) 2019/2144

En el artículo 11 del Reglamento (UE) 2019/2144, se añade el párrafo siguiente:

«3. Al adoptar actos de ejecución en virtud del apartado 2 relativos a sistemas de inteligencia artificial que sean componentes de seguridad en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo ^(*), se tendrán en cuenta los requisitos establecidos en el capítulo III, sección 2, de dicho Reglamento.

Artículo 110.– Modificación de la Directiva (UE) 2020/1828

En el anexo I de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo ⁽⁵⁸⁾ se añade el punto siguiente:

«68) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 1689, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y

betearazpen-egintzak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

4) 47. artikuluan, apartatu hau eransten da:

«3. Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, (EB) 2024/1689 Erregelamenduaren zentzuan, 1. eta 2. apartatuei jarraikiz egintza eskuordetuak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

5) 57. artikuluan, paragrafo hau eransten da:

«Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, (EB) 2024/1689 Erregelamenduaren zentzuan, betearazpen-egintza horiek hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

6) 58. artikuluan, apartatu hau eransten da:

«3. Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, (EB) 2024/1689 Erregelamenduaren zentzuan, 1. eta 2. apartatuei jarraikiz egintza eskuordetuak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

109. artikulua.– (EB) 2019/2144 Erregelamendua aldatzea

(EB) 2019/2144 Erregelamenduaren 11. artikuluan, paragrafo hau eransten da:

«3. Segurtasun-osagaiak diren adimen artifizialeko sistemei dagokienez, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1689 Erregelamenduaren zentzuan ^(*), 2. apartatuari jarraikiz betearazpen-egintzak hartzean, kontuan hartuko dira erregelamendu horren III. kapituluko 2. atalean ezarritako betekizunak».

110. artikulua.– (EB) 2020/1828 Zuzentaraua aldatzea

Europako Parlamentuaren eta Kontseiluaren (EB) 2020/1828 Zuzentarauaren ⁽⁵⁸⁾ I. eranskinean, puntu hau eransten da:

«68) (EB) 2024/1689 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2024ko ekainaren 13koa, adimen artifizialaren arloan arau harmonizatuak ezartzen dituen eta (EE) 300/2008, (EB) 167/2013, (EB) 168/2013, (EB) 2018/858, (EB) 2018/1139 eta (EB) 2019/2144 erregelamenduak eta 2014/90/EB, (EB)



(UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) ([DO L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>](https://doi.org/10.1007/978-3-319-22263-0_12))).».

Artículo 111.– Sistemas de IA ya introducidos en el mercado o puestos en servicio y modelos de IA de uso general ya introducidos en el mercado

1. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, apartado 3, letra a), los sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud establecidos en virtud de los actos legislativos enumerados en el anexo X que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2027 deberán estar en conformidad con el presente Reglamento a más tardar el 31 de diciembre de 2030.

Los requisitos establecidos en el presente Reglamento se tendrán en cuenta en la evaluación de cada sistema informático de gran magnitud establecido en virtud de los actos jurídicos enumerados en el anexo X que se efectúe de conformidad con lo dispuesto en dichos actos jurídicos y cuando dichos actos jurídicos hayan sido sustituidos o modificados.

2. Sin perjuicio de que se aplique el artículo 5 con arreglo a lo dispuesto en el artículo 113, apartado 3, letra a), el presente Reglamento se aplicará a los operadores de sistemas de IA de alto riesgo, distintos de los mencionados en el apartado 1 del presente artículo, que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2026 únicamente si, a partir de esa fecha, dichos sistemas se ven sometidos a cambios significativos en su diseño. En cualquier caso, los proveedores y los responsables del despliegue de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas adoptarán las medidas necesarias para cumplir los requisitos y obligaciones del presente Reglamento a más tardar el 2 de agosto de 2030.

3. Los proveedores de modelos de IA de uso general que se hayan introducido en el mercado antes del 2 de agosto de 2025 adoptarán las medidas necesarias para cumplir las obligaciones establecidas en el presente Reglamento a más tardar el 2 de agosto de 2027.

Artículo 112.– Evaluación y revisión

1. La Comisión evaluará la necesidad de modificar la lista del anexo III y la lista de prácticas de IA prohibidas previstas en el artículo 5 una vez al año a partir de la entrada en vigor del presente Reglamento y hasta el final del período de delegación de poderes previsto en el

2016/797 eta (EB) 2020/1828 zuzentarauak aldatzen dituen (Adimen Artifizialari buruzko Erregelamendua) ([2024/07/12ko EBAO, L, 2024/1689, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>](https://doi.org/10.1007/978-3-319-22263-0_12))).».

111. artikulua.– Dagoeneko merkatuan jarri edo zerbitzuan ipini diren AA-sistemak eta dagoeneko merkatuan jarri diren erabilera orokorreko AA-ereduak

1. Ezertan eragotzi gabe 5. artikulua aplikatzea 113.3.a) artikuluan xedatutakoaren arabera, X. eranskinean zerrendatuta dauden lege-egintzen arabera ezarritako magnitude handiko sistema informatikoen osagai diren AA-sistemek, 2027ko abuztuaren 2a baino lehen jarri baziren merkatuan edo ipini baziren zerbitzuan, beranduenez 2030eko abenduaren 31n etorri beharko dute bat erregelamendu honekin.

Erregelamendu honetan ezarritako betekizunak kontuan hartuko dira X. eranskinean zerrendatuta dauden egintza juridikoen arabera ezarritako magnitude handiko sistema informatiko bakoitza ebaluatzean, egintza juridiko horietan xedatutakoaren arabera egiten denean eta egintza juridiko horiek ordeztu edo aldatu direnean.

2. Ezertan eragotzi gabe 5. artikulua aplikatzea 113.3.a) artikuluan xedatutakoaren arabera, erregelamendu hau aplikatuko zaie 1. apartatuan aipatutakoez bestelako arrisku handiko AA-sistemen operadoreei, baldin eta 2026ko abuztuaren 2a baino lehen jarri baziren merkatuan edo ipini baziren zerbitzuan, eta soilik data horretatik aurrera aldaketa esanguratsurik egin bada sistema horien diseinuan. Nolanahi ere, agintaritza publikoek erabiliko dituzten arrisku handiko AA-sistemen hornitzaileek eta hedapenaren arduradunek behar diren neurriak hartuko dituzte beranduenez 2030eko abuztuaren 2rako betetzeko erregelamendu honetan ezarritako betekizun eta betebeharrak.

3. Merkatuan 2025eko abuztuaren 2a baino lehen jarri diren erabilera orokorreko AA-ereduen hornitzaileek behar diren neurriak hartuko dituzte beranduenez 2027ko abuztuaren 2rako betetzeko erregelamendu honetan ezarritako betebeharrak.

112. artikulua.– Ebaluazioa eta berrikuspena

1. Batzordeak urtean behin ebaluatuko du ea aldatu behar diren III. eranskineko zerrenda eta 5. artikuluan aurreikusi diren AA-jardunbide debekatuen zerrenda, erregelamendu hau indarrean sartzen denetik eta 97. artikuluan aurreikusitako ahalak eskuordetzeko aldia amaitu arte. Batzordeak Europako Parlamentuari eta



artículo 97. La Comisión presentará las conclusiones de dicha evaluación al Parlamento Europeo y al Consejo.

2. A más tardar el 2 de agosto de 2028, y posteriormente cada cuatro años, la Comisión evaluará los puntos siguientes e informará de ello al Parlamento Europeo y al Consejo:

a) la necesidad de ampliar los ámbitos enumerados en el anexo III o de añadir nuevos ámbitos;

b) la necesidad de modificar la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50;

c) la necesidad de mejorar la eficacia del sistema de supervisión y gobernanza.

3. A más tardar el 2 de agosto de 2029, y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. El informe incluirá una evaluación de la estructura de control del cumplimiento y de la posible necesidad de que una agencia de la Unión resuelva las deficiencias detectadas. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento. Los informes se harán públicos.

4. En los informes mencionados en el apartado 2 se prestará una atención especial a lo siguiente:

a) el estado de los recursos financieros, técnicos y humanos de las autoridades nacionales competentes para desempeñar de forma eficaz las funciones que les hayan sido asignadas en virtud del presente Reglamento;

b) el estado de las sanciones, en particular, de las multas administrativas a que se refiere el artículo 99, apartado 1, aplicadas por los Estados miembros a las infracciones de las disposiciones del presente Reglamento;

c) las normas armonizadas adoptadas y las especificaciones comunes desarrolladas en apoyo del presente Reglamento;

d) el número de empresas que entran en el mercado después de que se empiece a aplicar el presente Reglamento y, de entre ellas, el número de pymes.

5. A más tardar el 2 de agosto de 2028, la Comisión evaluará el funcionamiento de la Oficina de IA, si se le han otorgado poderes y competencias suficientes para

Kontseiluari aurkeztuko dizkie ebaluazio horren ondorioak.

2. Beranduenez 2028ko abuztuaren 2an, eta hortik aurrera lau urtean behin, Batzordeak puntu hauek ebaluatuko ditu, eta horren berri emango die Europako Parlamentuari eta Kontseiluari:

a) ea zabaldu behar diren III. eranskinean zerrendatutako eremuak edo beste eremuren bat gehitu behar den;

b) ea aldatu behar den 50. artikulua arabera gardentasun-neurri gehigarriak behar dituzten AA-sistemen zerrenda;

c) ea hobetu behar den gainbegiratze- eta gobernantza-sistemaren eraginkortasuna.

3. Beranduenez 2029ko abuztuaren 2an, eta hortik aurrera lau urtean behin, Batzordeak erregelamendu honen ebaluazioari eta berrikuspenari buruzko txosten bat bidaliko die Europako Parlamentuari eta Kontseiluari. Txostenean, betetze-maila kontrolatzeko egituraren ebaluazioa jasoko da, eta hautemandako akatsak Batasuneko agentzia batek konpondu behar dituen ere adieraziko da. Ondorioen arabera, txosten horrekin batera, hala badagokio, erregelamendu hau aldatzeko proposamen bat aurkeztuko da. Txostenok herritarren eskura jarriko dira.

4. 2. apartatuan aipatutako txostenetan, arreta berezia eskainiko zaie alderdi hauei:

a) zer egoeratan dauden agintaritza nazional eskudunen finantza-baliabideak, baliabide teknikoak eta giza baliabideak, eraginkortasunez betetzeko erregelamendu honen arabera esleitu zaizkien eginkizunak;

b) zer egoeratan dauden estatu kideek erregelamendu honetako xedapenak hausteagatik aplikatzen dituzten zehapenak eta, bereziki, 99.1 artikuluan aipatzen diren administrazio-isunak;

c) zer arau harmonizatu hartzen diren eta zer zehaztaperen komun garatzen diren erregelamendu honen babespean;

d) zenbat enpresa eta, horien artean, zenbat ETE, jartzen diren merkatuan erregelamendu hau aplikatzen hasi ondoren.

5. Beranduenez 2028ko abuztuaren 2an, Batzordeak AA-bulegoaren funtzionamendua ebaluatuko du: ea behar adina ahal eta eskumen eman zaizkion bere



desempeñar sus funciones, y si sería pertinente y necesario para la correcta aplicación y ejecución del presente Reglamento mejorar la Oficina de IA y sus competencias de ejecución, así como aumentar sus recursos. La Comisión presentará un informe sobre su evaluación al Parlamento Europeo y al Consejo.

6. A más tardar el 2 de agosto de 2028 y posteriormente cada cuatro años, la Comisión presentará un informe sobre la revisión de los avances en la elaboración de documentos de normalización sobre el desarrollo eficiente desde el punto de vista energético de modelos de IA de uso general y evaluará la necesidad de medidas o acciones adicionales, incluidas medidas o acciones vinculantes. Este informe se remitirá al Parlamento Europeo y al Consejo y se hará público.

7. A más tardar el 2 de agosto de 2028 y posteriormente cada tres años, la Comisión evaluará la incidencia y la eficacia de los códigos de conducta voluntarios por lo que respecta a promover la aplicación de los requisitos establecidos en el capítulo III, sección 2, a sistemas de IA que no sean de alto riesgo y, en su caso, de otros requisitos adicionales aplicables a los sistemas de IA que no sean sistemas de IA de alto riesgo, como, por ejemplo, requisitos relativos a la sostenibilidad medioambiental.

8. A efectos de lo dispuesto en los apartados 1 a 7, el Consejo de IA, los Estados miembros y las autoridades nacionales competentes facilitarán información a la Comisión, cuando así lo solicite, y sin demora indebida.

9. Al llevar a cabo las evaluaciones y revisiones mencionadas en los apartados 1 a 7, la Comisión tendrá en cuenta las posiciones y conclusiones del Consejo de IA, el Parlamento Europeo, el Consejo y los demás organismos o fuentes pertinentes.

10. La Comisión presentará, en caso necesario, las propuestas oportunas de modificación del presente Reglamento, en particular teniendo en cuenta la evolución de la tecnología y el efecto de los sistemas de IA en la salud y la seguridad y en los derechos fundamentales, y a la vista de los avances en la sociedad de la información.

11. Para orientar las evaluaciones y revisiones a que se refieren los apartados 1 a 7 del presente artículo, la Oficina de IA se encargará de desarrollar una metodología objetiva y participativa para la evaluación de los niveles de riesgo a partir de los criterios

eginkizunak betetzeko eta, erregelamendu hau behar bezala aplikatzeko eta betearazteko, ea egokia eta beharrezkoa izango litzatekeen AA-bulegoa eta haren betearazpen-eskumenak hobetzea, eta haren baliabideak handitzea. Batzordeak ebaluazioari buruzko txostena aurkeztuko die Europako Parlamentuari eta Kontseiluari.

6. Beranduenaz 2028ko abuztuaren 2an, eta hortik aurrera lau urtean behin, Batzordeak txosten batean jasoko du erabilera orokorreko AA-ereduek energia-efizientziaren ikuspegitik izan duten garapenari buruzko normalizazio-dokumentuak egiteko aurrerapenen berrikuspena, eta neurri edo ekintza gehigarriren bat egin behar den ebaluatuko du, neurri edo ekintza lotesleak barne. Txosten hori Europako Parlamentuari eta Kontseiluri bidaliko zaie, eta herritarren eskura jarriko da.

7. Beranduenaz 2028ko abuztuaren 2an, eta hortik aurrera hiru urtean behin, Batzordeak ebaluatuko du ea borondatezko jokabide-kodeek zer-nolako eragina eta eraginkortasuna duten arrisku handikoak ez diren AA-sistemei III. kapituluko 2. atalean ezarritako betekizunak aplikatzea sustatzeari dagokionez eta, hala badagokio, arrisku handiko AA-sistemak ez diren AA-sistemei aplikatzekoak diren beste betekizun gehigarri batzuk (adibidez, ingurumen-jasangarritasunari buruzko betekizunak) aplikatzea sustatzeari dagokionez.

8. Artikulu honen 1.tik 7.era bitarteko apartatuetan xedatutakoaren ondorioetarako, AA-kontseiluak, estatu kideek eta agintaritza nazional eskudunek informazioa emango diote Batzordeari, hala eskatzen duenean, eta bidegabeko atzerapenik gabe.

9. Artikulu honen 1.tik 7.era bitarteko apartatuetan adierazitako ebaluazioa eta ikuskapena egiten duenean, Batzordeak kontuan hartuko ditu AA-kontseiluaren, Europako Parlamentuaren, Kontseiluaren eta gainerako organismo edo beharrezko iturrien ikuspuntuak eta ondorioak.

10. Hala behar izanez gero, erregelamendu hau aldatzeko proposamen egokiak aurkeztuko ditu Batzordeak, bereziki aintzat hartuta teknologiek duten bilakaera eta AA-sistemen osasunean, segurtasunean eta oinarritzko eskubideetan duen eragina, eta informazioaren gizartean gertatzen diren aurrerapenak ikusita.

11. Artikulu honen 1.tik 7.era bitarteko apartatuetan aipatzen diren ebaluazioak eta berrikuspenak bideratzeko, arrisku-mailak ebaluatzeko metodologia objektibo eta parte-hartzailea garatuko du AA-bulegoak, dagozkion artikuluetan azaldutako irizpideak oinarri



expuestos en los artículos pertinentes y la inclusión de nuevos sistemas en:

- a) la lista establecida en el anexo III, incluida la ampliación de los ámbitos existentes o la inclusión de nuevos ámbitos en dicho anexo;
- b) la lista de prácticas prohibidas establecida en el artículo 5, y
- c) la lista de sistemas de IA que requieren medidas de transparencia adicionales con arreglo al artículo 50.

12. Las modificaciones del presente Reglamento con arreglo al apartado 10, o los actos delegados o de ejecución pertinentes, que afecten a los actos legislativos de armonización de la Unión sectoriales que se enumeran en el anexo I, sección B, tendrán en cuenta las particularidades normativas de cada sector y los mecanismos de gobernanza, evaluación de la conformidad y ejecución vigentes, así como las autoridades establecidas en ellos.

13. A más tardar el 2 de agosto de 2031, la Comisión evaluará la ejecución del presente Reglamento e informará al respecto al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo, teniendo en cuenta los primeros años de aplicación del presente Reglamento. En función de sus conclusiones, dicho informe irá acompañado, en su caso, de una propuesta de modificación del presente Reglamento en lo que respecta a la estructura de ejecución y a la necesidad de que una agencia de la Unión resuelva las deficiencias detectadas.

Artículo 113.– Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.

Será aplicable a partir del 2 de agosto de 2026.

No obstante:

- a) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025;
- b) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101;
- c) el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.

hartuta, eta sistema berriak sartuko ditu zerrenda hauetan:

- a) III. eranskinean ezarritako zerrendan, lehendik dauden eremuak zabalduz edo eremu berriak sartuz eranskin horretan;
- b) 5. artikuluan ezarritako jardunbide debekatuen zerrendan, eta
- c) 50. artikulua arabera gardentasun-neurri gehigarriak behar dituzten AA-sistemen zerrendan.

12. Erregelamendu honi 10. apartatuaren arabera egingo zaizkien aldaketek edo egintza eskuordetu edo betearazpen-egintzek, baldin eta I. eranskineko B atalean zerrendatzen diren Batasunaren harmonizazioko lege-egintza sektorialeiei eragiten badiete, kontuan hartuko dituzte sektore bakoitzaren arau-bereizitasunak eta gobernantzarako, adostasuna ebaluatzeko eta betearazteko indarrean dauden mekanismoak, bai eta horietan ezarritako agintaritzak ere.

13. Beranduenez 2031ko abuztuaren 2an, erregelamendu honen betearazpena ebaluatuko du Batzordeak, erregelamendu hau aplikatu den lehenengo urteak oinarri hartuta, eta horren inguruko txosten bat aurkeztu beharko die Europako Parlamentuari, Kontseiluari eta Europako Ekonomia eta Gizarte Komiteari. Ateratzen diren ondorioen arabera, txosten horrekin batera, hala badagokio, erregelamendu hau aldatzeko proposamen bat aurkeztuko da, egikaritze-egiturari dagokionez eta Batasuneko agentzia batek hautemandako akatsak konpontzeko beharrari dagokienez.

113. artikulua.– Indarrean jartzea eta aplikatzea

Erregelamendu hau Europar Batasunaren Aldizkari Ofizialean argitaratu eta hogeiei egunera jarriko da indarrean.

2026ko abuztuaren 2tik aurrera aplikatu beharko da.

Hala ere:

- a) I. eta II. kapituluak 2025eko otsailaren 2tik aurrera aplikatuko dira;
- b) III. kapituluko 4. atala, V. kapitulua, VII. kapitulua, XII. kapitulua eta 78. artikulua 2025eko abuztuaren 2tik aurrera aplikatuko dira, 101. artikulua izan ezik;
- c) 6.1 artikulua eta erregelamendu honetako betebeharrak 2027ko abuztuaren 2tik aurrera aplikatuko dira.



El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 13 de junio de 2024.

Por el Parlamento Europeo
La Presidenta
R. METSOLA

Por el Consejo
El Presidente
M. MICHEL

Erregelamendu hau oso-osoan bete beharko da, eta zuzenean aplikatu estatu kide bakoitzean.

Bruselan egin, 2024ko ekainaren 13an.

Europako Parlamentuaren izenean
Presidentea
R. METSOLA

Kontseiluaren izenean
Presidentea
M. MICHEL

(1) [DO C 517 de 22.12.2021, p. 56.](#)

(2) [DO C 115 de 11.3.2022, p. 5.](#)

(3) [DO C 97 de 28.2.2022, p. 60.](#)

(4) Posición del Parlamento Europeo de 13 de marzo de 2024 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 21 de mayo de 2024.

(5) Consejo Europeo, Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) – Conclusiones, EUCO 13/20, 2020, p. 6.

(6) Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas [2020/2012(INL)].

(7) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y por el que se deroga el Reglamento (CEE) n.º 339/93 ([DO L 218 de 13.8.2008, p. 30](#)).

(8) Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo ([DO L 218 de 13.8.2008, p. 82](#)).

(9) Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011 ([DO L 169 de 25.6.2019, p. 1](#)).

(10) Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones

(1) [2021/12/22ko EBAO, C 517, 56. or.](#)

(2) [2022/03/11ko EBAO, C 115, 5. or.](#)

(3) [2022/02/28ko EBAO, C 97, 60. or.](#)

(4) Jarrera, Europako Parlamentuarena, 2024ko martxoaren 13koa (oraindik ez da argitaratu Aldizkari Ofizialean), eta Erabakia, Kontseiluarena, 2024ko maiatzaren 21ekoa.

(5) Kontseilu Europarra, Kontseilu Europarraren bilera berezia (2020ko urriaren 1a eta 2a) – Ondorioak, EUCO 13/20, 2020, 6. or.

(6) Ebazpena, Europako Parlamentuarena, 2020ko urriaren 20koa, Batzordeari zuzendutako gomendioekin, adimen artifizialaren, robotikaren eta teknologia lotuen alderdi etikoen esparru bati buruz [2020/2012 (INL)].

(7) (EE) 765/2008 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2008ko uztailaren 9koa, egiaztatzeko betekizunak ezartzen dituen eta (EEE) 339/93 Erregelamendua indargabetzen duena ([2008/08/13ko EBAO, L 218, 30. or.](#)).

(8) 768/2008/EE Erabakia, Europako Parlamentuarena eta Kontseiluarena, 2008ko uztailaren 9koa, produktuak merkaturatzeko esparru komunari buruzkoa eta Kontseiluaren 93/465/EEE Erabakia indargabetzen duena ([2008/08/13ko EBAO, L 218, 82. or.](#)).

(9) (EB) 2019/1020 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko ekainaren 20koa, merkaturatze zaintzeari eta produktuen adostasunari buruzkoa, eta 2004/42/EE Zuzentaraua eta (EE) 765/2008 eta (EB) 305/2011 erregelamenduak aldatzen dituen ([2019/06/25eko EBAO, L 169, 1. or.](#)).

(10) 85/374/EEE Zuzentaraua, Kontseiluarena, 1985eko uztailaren 25ekoa, produktu akastunek



legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos ([DO L 210 de 7.8.1985, p. 29](#)).

(11) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) ([DO L 119 de 4.5.2016, p. 1](#)).

(12) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE ([DO L 295 de 21.11.2018, p. 39](#)).

(13) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo ([DO L 119 de 4.5.2016, p. 89](#)).

(14) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) ([DO L 201 de 31.7.2002, p. 37](#)).

(15) Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) ([DO L 277 de 27.10.2022, p. 1](#)).

(16) Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios ([DO L 151 de 7.6.2019, p. 70](#)).

(17) Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior,

eragindako kalteen erantzukizunaren arloan estatu kideek dituzten lege-, erregelamendu- eta administrazio-xedapenen hurbilketari buruzkoa ([1985/08/07ko EBAO, L 210, 29. or.](#)).

(11) (EB) 2016/679 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoak babesteari eta datu horien zirkulazio askeari buruzkoa eta 95/46/EE Zuzentaraua (Datuak Babesteko Erregelamendu Orokorra) indargabetzen duena ([2016/05/04ko EBAO, L 119, 1. or.](#)).

(12) (EB) 2018/1725 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko urriaren 23koa, Batasuneko instituzio, organo eta organismoek egiten duten datu pertsonalen tratamenduari dagokionez pertsona fisikoak babesteari eta datu horien zirkulazio askeari buruzkoa eta (EE) 45/2001 Erregelamendua eta 1247/2002/EE Erabakia indargabetzen dituen ([2018/11/21eko EBAO, L 295, 39. or.](#)).

(13) (EB) 2016/680 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, agintaritza eskudunek arau-hauste penalak prebenitu, ikertu, detektatu edo epaitzeko edo zehapen penalak betearazteko egiten duten datu pertsonalen tratamenduari dagokionez pertsona fisikoak babesteari eta datu horien zirkulazio askeari buruzkoa eta Kontseiluaren 2008/977/JAI Esparru Erabakia indargabetzen duena ([2016/05/04ko EBAO, L 119, 89. or.](#)).

(14) 2002/58/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2002ko uztailaren 12koa, komunikazio elektronikoen sektorean datu pertsonalak tratatzeko moduari eta intimitatea babesteari buruzkoa (pribatutasunari eta komunikazio elektronikoei buruzko zuzentaraua) ([2002/07/31ko EBAO, L 201, 37. or.](#)).

(15) (EB) 2022/2065 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2022ko urriaren 19koa, zerbitzu digitalen merkatu bakarrari buruzkoa eta 2000/31/EE Zuzentaraua (zerbitzu digitalen erregelamendua) aldatzen duena ([2022/10/27ko EBAO, L 277, 1. or.](#)).

(16) (EB) 2019/882 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2019ko apirilaren 17koa, produktuen eta zerbitzuen irisgarritasun-betekizunei buruzkoa ([2019/06/07ko EBAO, L 151, 70. or.](#)).

(17) 2005/29/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2005eko maiatzaren 11koa, enpresek barne-merkatuan kontsumitzaileekiko harremanetan dituzten jardunbide



que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre las prácticas comerciales desleales») ([DO L 149 de 11.6.2005, p. 22](#)).

[\(18\)](#) Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros ([DO L 190 de 18.7.2002, p. 1](#)).

[\(19\)](#) Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo ([DO L 333 de 27.12.2022, p. 164](#)).

[\(20\)](#) [DO C 247 de 29.6.2022, p. 1](#).

[\(21\)](#) Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo ([DO L 117 de 5.5.2017, p. 1](#)).

[\(22\)](#) Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión ([DO L 117 de 5.5.2017, p. 176](#)).

[\(23\)](#) Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE ([DO L 157 de 9.6.2006, p. 24](#)).

[\(24\)](#) Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n.º 2320/2002 ([DO L 97 de 9.4.2008, p. 72](#)).

[\(25\)](#) Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, relativo a la homologación de los vehículos agrícolas o forestales, y a la vigilancia del mercado de dichos vehículos ([DO L 60 de 2.3.2013, p. 1](#)).

komertzial desleialei buruzkoa, Kontseiluaren 84/450/EEE Zuzentaraua, Europako Parlamentuaren eta Kontseiluaren 97/7/EE, 98/27/EE eta 2002/65/EE zuzentarauak eta Europako Parlamentuaren eta Kontseiluaren (EE) 2006/2004 Erregelamendua aldatzen dituen («jardunbide komertzial desleialei buruzko zuzentaraua») ([2005/06/11ko EBAO, L 149, 22. or.](#)).

[\(18\)](#) 2002/584/JAI Esparru Erabakia, Kontseiluarena, 2002ko ekainaren 13koa, atxilotzeko Europako aginduari eta estatuen arteko entrega-prozedurei buruzkoa ([2002/07/18ko EBAO, L 190, 1. or.](#)).

[\(19\)](#) (EB) 2022/2557 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2022ko abenduaren 14koa, entitate kritikoen erresilientziari buruzkoa eta Kontseiluaren 2008/114/EE Zuzentaraua indargabetzen duena ([2022/12/27ko EBAO, L 333, 164. or.](#)).

[\(20\)](#) [2022/06/29ko EBAO, C 247, 1. or.](#)

[\(21\)](#) (EB) 2017/745 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2017ko apirilaren 5koa, osasun-produktuei buruzkoa, 2001/83/EE Zuzentaraua, (EE) 178/2002 Erregelamendua eta (EE) 1223/2009 Erregelamendua aldatzen dituen eta Kontseiluaren 90/385/EEE eta 93/42/EEE zuzentarauak indargabetzen dituen ([2017/05/05eko EBAO, L 117, 1. or.](#)).

[\(22\)](#) (EB) 2017/746 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2017ko apirilaren 5koa, in vitro diagnostikorako osasun-produktuei buruzkoa eta 98/79/EE Zuzentaraua eta Batzordearen 2010/227/EB Erabakia indargabetzen dituen ([2017/05/05eko EBAO, L 117, 176. or.](#)).

[\(23\)](#) 2006/42/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2006ko maiatzaren 17koa, makinei buruzkoa eta 95/16/EE Zuzentaraua aldatzen duena ([2006/06/09ko EBAO, L 157, 24. or.](#)).

[\(24\)](#) (EB) 300/2008 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2008ko martxoaren 11koa, abiazio zibilaren segurtasunerako arau orokorreari buruzkoa eta (EE) 2320/2002 Erregelamendua indargabetzen duena ([2008/04/09ko EBAO, L 97, 72. or.](#)).

[\(25\)](#) (EB) 167/2013 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2013ko otsailaren 5koa, nekazaritzako edo basogintzako ibilgailuak homologatzeari eta ibilgailu horien merkaturako zaintzeari buruzkoa ([2013/03/02ko EBAO, L 60, 1. or.](#)).



(26) Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, relativo a la homologación de los vehículos de dos o tres ruedas y los cuatriciclos, y a la vigilancia del mercado de dichos vehículos ([DO L 60 de 2.3.2013, p. 52](#)).

(27) Directiva 2014/90/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre equipos marinos, y por la que se deroga la Directiva 96/98/CE del Consejo ([DO L 257 de 28.8.2014, p. 146](#)).

(28) Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la interoperabilidad del sistema ferroviario dentro de la Unión Europea ([DO L 138 de 26.5.2016, p. 44](#)).

(29) Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y por el que se deroga la Directiva 2007/46/CE ([DO L 151 de 14.6.2018, p. 1](#)).

(30) Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 y (UE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 552/2004 y (CE) n.º 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.º 3922/91 del Consejo ([DO L 212 de 22.8.2018, p. 1](#)).

(31) Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 78/2009, (CE) n.º 79/2009 y (CE) n.º 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º

(26) (EB) 168/2013 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2013ko urtarrilaren 15ekoa, bi edo hiru gurpileko ibilgailuak eta kuatrizikloak homologatzeari eta ibilgailu horien merkatua zaintzeari buruzkoa ([2013/03/02ko EBAO, L 60, 52. or.](#)).

(27) 2014/90/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko uztailaren 23koa, itsas ekipamenduei buruzkoa eta Kontseiluaren 96/98/EE Zuzentaraua indargabetzen duena ([2014/08/28ko EBAO, L 257, 146. or.](#)).

(28) (EB) 2016/797 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko maiatzaren 11koa, Europar Batasuneko trenbide-sistemen elkarrengarritasunari buruzkoa ([2016/05/26ko EBAO, L 138, 44. or.](#)).

(29) (EB) 2018/858 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko maiatzaren 30ekoa, ibilgailu motordunen eta haien atoiari eta ibilgailu horietarako sistemen, osagaien eta unitate tekniko independenteen merkatuaren homologazioari eta zaintzari buruzkoa, (EE) 715/2007 eta (EE) 595/2009 erregelamenduak aldatzen dituen eta 2007/46/EE Zuzentaraua indargabetzen duena ([2018/06/14ko EBAO, L 151, 1. or.](#)).

(30) (EB) 2018/1139 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko uztailaren 4koa, abiazio zibilaren arloko arau erkideei buruzkoa eta Aire Segurtasuneko Europar Batasuneko Agentzia bat sortzen duena, eta (EE) 2111/2005, (EE) 1008/2008, (EB) 996/2010 eta (EB) 376/2014 erregelamenduak eta 2014/30/EB eta 2014/53/EB zuzentzarauak aldatzen dituen eta Europako Parlamentuaren eta Kontseiluaren (EE) 552/2004 eta (EE) 216/2008 erregelamenduak eta Kontseiluaren (EEE) 3922/91 Erregelamendua indargabetzen dituen ([2018/08/22ko EBAO, L 212, 1. or.](#)).

(31) (EB) 2019/2144 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko azaroaren 27koa, ibilgailu motordunak eta haien atoiak, eta ibilgailu horietarako sistemak, osagaiak eta unitate tekniko independenteak homologatzeko betekizunei buruzkoa, haien segurtasun orokorrari eta ibilgailuko bidaiarien eta bide publikoko erabiltzaile kalteberen babesari dagokionez, eta Europako Parlamentuaren eta Kontseiluaren (EB) 2018/858 Erregelamendua aldatzen duena eta Europako Parlamentuaren eta Kontseiluaren (EE) 78/2009, (EE) 79/2009 eta (EE) 661/2009 erregelamenduak eta Batzordearen (EE) 631/2009, (EB) 406/2010, (EB) 672/2010, (EB) 1003/2010, (EB) 1005/2010, (EB) 1008/2010, (EB) 1009/2010, (EB) 19/2011, (EB) 109/2011, (EB) 458/2011, (EB) 65/2012, (EB) 130/2012, (EB) 347/2012, (EB) 351/2012, (EB)



19/2011, (UE) n.o 109/2011, (UE) n.o 458/2011, (UE) n.o 65/2012, (UE) n.o 130/2012, (UE) n.o 347/2012, (UE) n.o 351/2012, (UE) n.o 1230/2012 y (UE) 2015/166 de la Comisión ([DO L 325 de 16.12.2019, p. 1](#)).

(32) Reglamento (CE) n.o 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados) ([DO L 243 de 15.9.2009, p. 1](#)).

(33) Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para la concesión o la retirada de la protección internacional ([DO L 180 de 29.6.2013, p. 60](#)).

(34) Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política ([DO L 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj](#)).

(35) Directiva 2014/31/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de comercialización de instrumentos de pesaje de funcionamiento no automático ([DO L 96 de 29.3.2014, p. 107](#)).

(36) Directiva 2014/32/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de comercialización de instrumentos de medida ([DO L 96 de 29.3.2014, p. 149](#)).

(37) Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad») ([DO L 151 de 7.6.2019, p. 15](#)).

(38) Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público ([DO L 327 de 2.12.2016, p. 1](#)).

(39) Directiva 2002/14/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 2002, por la que se establece un marco general relativo a la información y a la consulta de los trabajadores en la Comunidad Europea ([DO L 80 de 23.3.2002, p. 29](#)).

1230/2012 eta (EB) 2015/166 erregelamenduak indargabetzen dituena ([2019/12/16ko EBAO, L 325, 1. or.](#)).

(32) (EE) 810/2009 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2009ko uztailaren 13koa, bisei buruzko erkidegoko kodea (bisen kodea) ezartzen duena ([2009/09/15eko EBAO, L 243, 1. or.](#)).

(33) 2013/32/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2013ko ekainaren 26koa, nazioarteko babesa emateko edo kentzeko prozedura komunei buruzkoa ([2013/06/29ko EBAO, L 180, 60. or.](#)).

(34) (EB) 2024/900 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2024ko martxoaren 13koa, publizitate politikoaren gardentasun eta segmentazioari buruzkoa ([2024/03/20ko EBAO, L 2024/900, ELI: http://data.europa.eu/eli/reg/2024/900/oj](#)).

(35) 2014/31/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko otsailaren 26koa, funtzionamendu ez-automatikoko pisatze-tresnak merkaturatzearen arloan estatu kideen legeria harmonizatzeari buruzkoa ([2014/03/29ko EBAO, L 96, 107. or.](#)).

(36) 2014/32/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko otsailaren 26koa, neurketa-tresnak merkaturatzearen arloan estatu kideen legeria harmonizatzeari buruzkoa ([2014/03/29ko EBAO, L 96, 149. or.](#)).

(37) (EB) 2019/881 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko apirilaren 17koa, ENISAr (Zibersegurtasunerako Europar Batasuneko Agentzia) eta informazioaren eta komunikazioaren teknologien zibersegurtasunaren ziurtapenari buruzkoa eta (EB) 526/2013 Erregelamendua («Zibersegurtasunari buruzko Erregelamendua») indargabetzen duena ([2019/06/07ko EBAO, L 151, 15. or.](#)).

(38) (EB) 2016/2102 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko urriaren 26koa, sektore publikoko organismoen webguneen eta gailu mugikorretarako aplikazioen erabilerraztasunari buruzkoa ([2016/12/02ko EBAO, L 327, 1. or.](#)).

(39) 2002/14/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2002ko martxoaren 11koa, langileen informazioari eta kontsultari buruzko esparru orokorra ezartzen duena Europako Erkidegoan ([2002/03/23ko EBAO, L 80, 29. or.](#)).



(40) Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE ([DO L 130 de 17.5.2019, p. 92](#)).

(41) Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo ([DO L 316 de 14.11.2012, p. 12](#)).

(42) Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) ([DO L 152 de 3.6.2022, p. 1](#)).

(43) Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) ([DO L 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>](#)).

(44) Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas ([DO L 124 de 20.5.2003, p. 36](#)).

(45) Decisión de la Comisión, de 24 de enero de 2024, por la que se crea la Oficina Europea de Inteligencia Artificial (C/2024/390).

(46) Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito, y por el que se modifica el Reglamento (UE) n.º 648/2012 ([DO L 176 de 27.6.2013, p. 1](#)).

(47) Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo ([DO L 133 de 22.5.2008, p. 66](#)).

(48) Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el

(40) (EB) 2019/790 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2019ko apirilaren 17koa, merkatu digital bakarreko egile-eskubideei eta antzeko eskubideei buruzkoa eta 96/9/EE eta 2001/29/EE zuzentaruak aldatzen dituen (2019/05/17ko EBAO, L 130, 92. or.).

(41) (EB) 1025/2012 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2012ko urriaren 25ekoa, Europaren normalizazioari buruzkoa, Kontseiluaren 89/686/EEE eta 93/15/EEE zuzentaruak eta Europako Parlamentuaren eta Kontseiluaren 94/9/EE, 94/25/EE, 95/16/EE, 97/23/EE, 98/34/EE, 2004/22/EE, 2007/23/EE, 2009/23/EE eta 2009/105/EE zuzentaruak aldatzen dituen eta Kontseiluaren 87/95/EEE Erabakia eta Europako Parlamentuaren eta Kontseiluaren 1673/2006/EE Erabakia indargabetzen dituen (2012/11/14ko EBAO, L 316, 12. or.).

(42) (EB) 2022/868 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2022ko maiatzaren 30ekoa, Europako datuen gobernantzari buruzkoa eta (EB) 2018/1724 Erregelamendua (Datuen Gobernantzari buruzko Erregelamendua) aldatzen duena (2022/06/03ko EBAO, L 152, 1. or.).

(43) (EB) 2023/2854 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2023ko abenduaren 13koa, datuetarako bidezko sarbidearen eta datuen erabileraren inguruko arau harmonizatuari buruzkoa eta (EB) 2017/2394 Erregelamendua eta (EB) 2020/1828 Zuzentaraua (Datuen Erregelamendua) aldatzen dituen (2023/12/22ko EBAO, L 2023/2854, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

(44) 2003/361/EE Gomendioa, Batzordearena, 2003ko maiatzaren 6koa, mikroenpresen, enpresa txikien eta enpresa ertainen definizioari buruzkoa (2003/05/20ko EBAO, L 124, 36. or.).

(45) Erabakia, Batzordearena, 2024ko urtarrilaren 24koa, Adimen Artifizialaren Europako Bulegoa sortzen duena (C/2024/390).

(46) (EB) 575/2013 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2013ko ekainaren 26koa, kreditu-entitateen zuhurtziazko betekizunei buruzkoa eta (EB) 648/2012 Erregelamendua aldatzen duena (2013/06/27ko EBAO, L 176, 1. or.).

(47) 2008/48/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2008ko apirilaren 23koa, kontsumorako kredituen kontratuei buruzkoa eta Kontseiluaren 87/102/EEE Zuzentaraua indargabetzen duena (2008/05/22ko EBAO, L 133, 66. or.).

(48) 2009/138/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2009ko azaroaren



acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) ([DO L 335 de 17.12.2009, p. 1](#)).

(49) Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE ([DO L 176 de 27.6.2013, p. 338](#)).

(50) Directiva 2014/17/UE del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, sobre los contratos de crédito celebrados con los consumidores para bienes inmuebles de uso residencial y por la que se modifican las Directivas 2008/48/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 ([DO L 60 de 28.2.2014, p. 34](#)).

(51) Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros ([DO L 26 de 2.2.2016, p. 19](#)).

(52) Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito ([DO L 287 de 29.10.2013, p. 63](#)).

(53) Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo ([DO L 135 de 23.5.2023, p. 1](#)).

(54) Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión ([DO L 305 de 26.11.2019, p. 17](#)).

(55) [DO L 123 de 12.5.2016, p. 1](#).

(56) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de

25ekoa, aseguru- eta berraseguru-jardueran hasteari eta horretan jarduteari buruzkoa (Kaudimena II) ([2009/12/17ko EBAO, L 335, 1. or.](#)).

(49) 2013/36/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2013ko ekainaren 26koa, kreditu-entitateak jardunean hasteari eta kreditu-entitateen zuhurtziazko gainbegiratzeari buruzkoa, zeinak 2002/87/EE Zuzentaraua aldatzen baitu eta 2006/48/EE eta 2006/49/EE zuzentzarauak indargabetzen baititu ([2013/06/27ko EBAO, L 176, 338. or.](#)).

(50) 2014/17/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko otsailaren 4koa, kontsumitzaileekin bizitegi-erabilerako ondasun higiezinatarako egindako kreditu-kontratuei buruzkoa eta 2008/48/EE eta 2013/36/EE zuzentzarauak eta (EB) 1093/2010 Erregelamendua aldatzen dituen ([2014/02/28ko EBAO, L 60, 34. or.](#)).

(51) (EB) 2016/97 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko urtarrilaren 20koa, aseguruen banaketari buruzkoa ([2016/02/02ko EBAO, L 26, 19. or.](#)).

(52) (EB) 1024/2013 Erregelamendua, Kontseiluarena, 2013ko urriaren 15ekoa, kreditu-entitateen zuhurtziazko gainbegiratzeari zerikusia duten eginkizun espezifikoak Europako Banku Zentralari agintzen dizkiona ([2013/10/29ko EBAO, L 287, 63. or.](#)).

(53) (EB) 2023/988 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2023ko maiatzaren 10ekoa, produktuen segurtasun orokorrari buruzkoa, Europako Parlamentuaren eta Kontseiluaren (EB) 1025/2012 Erregelamendua eta Europako Parlamentuaren eta Kontseiluaren (EB) 2020/1828 Zuzentaraua aldatzen dituen eta Europako Parlamentuaren eta Kontseiluaren 2001/95/EE Zuzentaraua eta Kontseiluaren 87/357/EEE Zuzentaraua indargabetzen dituen ([2023/05/23ko EBAO, L 135, 1. or.](#)).

(54) (EB) 2019/1937 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2019ko urriaren 23koa, Batasuneko zuzenbidearen arau-hausteei buruzko informazioa ematen duten pertsonak babesteari buruzkoa ([2019/11/26ko EBAO, L 305, 17. or.](#)).

(55) [2016/05/12ko EBAO, L 123, 1. or.](#)

(56) (EB) 182/2011 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2011ko otsailaren 16koa, Batzordeak betearazpen-eskumenak nola gauzatzen dituzten kontrolatzeko estatu kideen kontrol-



ejecución por la Comisión ([DO L 55 de 28.2.2011, p. 13](#)).

(57) Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas ([DO L 157 de 15.6.2016, p. 1](#)).

(58) Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE ([DO L 409 de 4.12.2020, p. 1](#)).

modalitateei buruzko arau eta printzipio orokorrak ezartzen dituen ([2011/02/28ko EBAO, L 55, 13. or.](#)).

(57) (EB) 2016/943 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko ekainaren 8koa, zabaldu gabeko ezagutza teknikoak eta enpresa-informazioa (merkataritza-sekretuak) babesteari buruzkoa, inork legez kontra ez eskuratzeko, ez erabiltzeko eta ez zabaltzeko ([2016/06/15eko EBAO, L 157, 1. or.](#)).

(58) (EB) 2020/1828 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2020ko azaroaren 25ekoa, kontsumitzaileen interes kolektiboak babesteko ordezkartza-ekintzei buruzkoa eta 2009/22/EE Zuzentaraua indargabetzen duena ([2020/12/04ko EBAO, L 409, 1. or.](#)).

ANEXO I

Lista de actos legislativos de armonización de la Unión

Sección A — Lista de actos legislativos de armonización de la Unión basados en el nuevo marco legislativo

1. Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE ([DO L 157 de 9.6.2006, p. 24](#))

2. Directiva 2009/48/CE del Parlamento Europeo y del Consejo, de 18 de junio de 2009, sobre la seguridad de los juguetes ([DO L 170 de 30.6.2009, p. 1](#))

3. Directiva 2013/53/UE del Parlamento Europeo y del Consejo, de 20 de noviembre de 2013, relativa a las embarcaciones de recreo y a las motos acuáticas, y por la que se deroga la Directiva 94/25/CE ([DO L 354 de 28.12.2013, p. 90](#))

4. Directiva 2014/33/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de ascensores y componentes de seguridad para ascensores ([DO L 96 de 29.3.2014, p. 251](#))

5. Directiva 2014/34/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de aparatos y sistemas de

I. ERANSKINA

Batasunaren harmonizazioko lege-egintzen zerrenda

A atala — Batasunaren legegitza-esparru berrian oinarritutako harmonizazioko lege-egintzen zerrenda

1. 2006/42/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2006ko maiatzaren 17koa, makinei buruzkoa eta 95/16/EE Zuzentaraua aldatzen duena ([2006/06/09ko EBAO, L 157, 24. or.](#))

2. 2009/48/EE Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2009ko ekainaren 18koa, jostailuen segurtasunari buruzkoa ([2009/06/30eko EBAO, L 170, 1. or.](#))

3. 2013/53/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2013ko azaroaren 20koa, aisiako ontziei eta uretako motoei buruzkoa eta 94/25/EE Zuzentaraua indargabetzen duena ([2013/12/28ko EBAO, L 354, 90. or.](#))

4. 2014/33/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko otsailaren 26koa, igogailuen eta igogailuetako segurtasun-osagaien arloan estatu kideen legeria harmonizatzei buruzkoa ([2014/03/29ko EBAO, L 96, 251. or.](#))

5. 2014/34/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko otsailaren 26koa, leherkorak izan daitezkeen atmosferetan erabiliko diren babeseko gailuen eta sistemen arloan



protección para uso en atmósferas potencialmente explosivas ([DO L 96 de 29.3.2014, p. 309](#))

6. Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE ([DO L 153 de 22.5.2014, p. 62](#))

7. Directiva 2014/68/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos a presión ([DO L 189 de 27.6.2014, p. 164](#))

8. Reglamento (UE) 2016/424 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a las instalaciones de transporte por cable y por el que se deroga la Directiva 2000/9/CE ([DO L 81 de 31.3.2016, p. 1](#))

9. Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a los equipos de protección individual y por el que se deroga la Directiva 89/686/CEE del Consejo ([DO L 81 de 31.3.2016, p. 51](#))

10. Reglamento (UE) 2016/426 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, sobre los aparatos que queman combustibles gaseosos y por el que se deroga la Directiva 2009/142/CE ([DO L 81 de 31.3.2016, p. 99](#))

11. Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo ([DO L 117 de 5.5.2017, p. 1](#))

12. Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión ([DO L 117 de 5.5.2017, p. 176](#))

Sección B — Lista de otros actos legislativos de armonización de la Unión

13. Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre

estatu kideen legeria harmonizatzeari buruzkoa ([2014/03/29ko EBAO, L 96, 309. or.](#))

6. 2014/53/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko apirilaren 16koa, ekipamendu erradioelektrikoak merkaturatzearen arloan estatu kideen legeria harmonizatzeari buruzkoa eta 1999/5/EE Zuzentaraua indargabetzen duena ([2014/05/22ko EBAO, L 153, 62. or.](#))

7. 2014/68/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko maiatzaren 15ekoa, presio-ekipamenduak merkaturatzearen arloan estatu kideen legeria harmonizatzeari buruzkoa ([2014/06/27ko EBAO, L 189, 164. or.](#))

8. (EB) 2016/424 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko martxoaren 9koa, kable bidezko garraioaren instalazioei buruzkoa eta 2000/9/EE Zuzentaraua indargabetzen duena ([2016/03/31ko EBAO, L 81, 1. or.](#))

9. (EB) 2016/425 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko martxoaren 9koa, norbera babesteko ekipamenduei buruzkoa eta Kontseiluaren 89/686/EEE Zuzentaraua indargabetzen duena ([2016/03/31ko EBAO, L 81, 51. or.](#))

10. (EB) 2016/426 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko martxoaren 9koa, gas-erregaiak erretzen dituzten aparatuei buruzkoa eta 2009/142/EE Zuzentaraua indargabetzen duena ([2016/03/31ko EBAO, L 81, 99. or.](#))

11. (EB) 2017/745 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2017ko apirilaren 5ekoa, osasun-produktuei buruzkoa, 2001/83/EE Zuzentaraua, (EE) 178/2002 Erregelamendua eta (EE) 1223/2009 Erregelamendua aldatzen dituen eta Kontseiluaren 90/385/EEE eta 93/42/EEE zuzentarauak indargabetzen dituen ([2017/05/05eko EBAO, L 117, 1. or.](#))

12. (EB) 2017/746 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2017ko apirilaren 5ekoa, in vitro diagnostikorako osasun-produktuei buruzkoa eta 98/79/EE Zuzentaraua eta Batzordearen 2010/227/EB Erabakia indargabetzen dituen ([2017/05/05eko EBAO, L 117, 176. or.](#))

B atala — Batasunaren harmonizazioko beste lege-gintza batzuen zerrenda

13. (EB) 300/2008 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2008ko



normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n.º 2320/2002 ([DO L 97 de 9.4.2008, p. 72](#))

14.Reglamento (UE) n.º 168/2013 del Parlamento Europeo y del Consejo, de 15 de enero de 2013, relativo a la homologación de los vehículos de dos o tres ruedas y los cuatriciclos, y a la vigilancia del mercado de dichos vehículos ([DO L 60 de 2.3.2013, p. 52](#))

15.Reglamento (UE) n.º 167/2013 del Parlamento Europeo y del Consejo, de 5 de febrero de 2013, relativo a la homologación de los vehículos agrícolas o forestales, y a la vigilancia del mercado de dichos vehículos ([DO L 60 de 2.3.2013, p. 1](#))

16.Directiva 2014/90/UE del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre equipos marinos, y por la que se deroga la Directiva 96/98/CE del Consejo ([DO L 257 de 28.8.2014, p. 146](#))

17.Directiva (UE) 2016/797 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, sobre la interoperabilidad del sistema ferroviario dentro de la Unión Europea ([DO L 138 de 26.5.2016, p. 44](#))

18.Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, sobre la homologación y la vigilancia del mercado de los vehículos de motor y sus remolques y de los sistemas, los componentes y las unidades técnicas independientes destinados a dichos vehículos, por el que se modifican los Reglamentos (CE) n.º 715/2007 y (CE) n.º 595/2009 y por el que se deroga la Directiva 2007/46/CE ([DO L 151 de 14.6.2018, p. 1](#))

19.Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, por el que se modifica el Reglamento (UE) 2018/858 del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 78/2009, (CE) n.º 79/2009 y (CE) n.º 661/2009 del Parlamento Europeo y del Consejo y los Reglamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012,

martxoaren 11koa, abiazio zibilaren segurtasunerako arau orokorre buruzkoa eta (EE) 2320/2002 Erregelamendua indargabetzen duena ([2008/04/09ko EBAO, L 97, 72. or.](#))

14.(EB) 168/2013 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2013ko urtarrilaren 15ekoa, bi edo hiru gurpileko ibilgailuak eta kuatrizikloak homologatzeari eta ibilgailu horien merkatua zaintzeari buruzkoa ([2013/03/02ko EBAO, L 60, 52. or.](#))

15.(EB) 167/2013 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2013ko otsailaren 5ekoa, nekazaritzako edo basogintzako ibilgailuak homologatzeari eta ibilgailu horien merkatua zaintzeari buruzkoa ([2013/03/02ko EBAO, L 60, 1. or.](#))

16.2014/90/EB Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2014ko uztailaren 23koa, itsas ekipamenduei buruzkoa eta Kontseiluaren 96/98/EE Zuzentaraua indargabetzen duena ([2014/08/28ko EBAO, L 257, 146. or.](#))

17.(EB) 2016/797 Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko maiatzaren 11koa, Europar Batasuneko trenbide-sistemen elkarrengarritasunari buruzkoa ([2016/05/26ko EBAO, L 138, 44. or.](#))

18.(EB) 2018/858 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko maiatzaren 30ekoa, ibilgailu motordunen eta haien atoiari eta ibilgailu horietarako sistemak, osagaiak eta unitate tekniko independenteen merkatuaren homologazioari eta zaintzari buruzkoa, (EE) 715/2007 eta (EE) 595/2009 erregelamenduak aldatzen dituen eta 2007/46/EE Zuzentaraua indargabetzen duena ([2018/06/14ko EBAO, L 151, 1. or.](#))

19.(EB) 2019/2144 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko azaroaren 27koa, ibilgailu motordunak eta haien atoiak, eta ibilgailu horietarako sistemak, osagaiak eta unitate tekniko independenteak homologatzeko betekizunei buruzkoa, haien segurtasun orokorrari eta ibilgailuko bidaiarien eta bide publikoko erabiltzaile kalteberen babesari dagokionez, eta Europako Parlamentuaren eta Kontseiluaren (EB) 2018/858 Erregelamendua aldatzen duena eta Europako Parlamentuaren eta Kontseiluaren (EE) 78/2009, (EE) 79/2009 eta (EE) 661/2009 erregelamenduak eta Batzordearen (EE) 631/2009, (EB) 406/2010, (EB) 672/2010, (EB) 1003/2010, (EB) 1005/2010, (EB) 1008/2010, (EB) 1009/2010, (EB) 19/2011, (EB) 109/2011, (EB) 458/2011, (EB) 65/2012, (EB) 130/2012, (EB) 347/2012, (EB) 351/2012, (EB) 1230/2012 eta (EB) 2015/166 erregelamenduak



(UE) n.o 351/2012, (UE) n.o 1230/2012 y (UE) 2015/166 de la Comisión ([DO L 325 de 16.12.2019, p. 1](#))

20.Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n.o 2111/2005, (CE) n.o 1008/2008, (UE) n.o 996/2010 y (UE) n.o 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.o 552/2004 y (CE) n.o 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.o 3922/91 del Consejo ([DO L 212 de 22.8.2018, p. 1](#)), en la medida en que afecte al diseño, la producción y la introducción en el mercado de aeronaves a que se refiere el artículo 2, apartado 1, letras a) y b), por lo que respecta a las aeronaves no tripuladas y sus motores, hélices, componentes y equipos para controlarlas a distancia

indargabetzen dituen ([2019/12/16ko EBAO, L 325, 1. or.](#))

20.(EB) 2018/1139 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko uztailaren 4koa, abiazio zibilaren arloko arau erkideei buruzkoa eta Aire Segurtasuneko Europar Batasuneko Agentzia bat sortzen duena, eta (EE) 2111/2005, (EE) 1008/2008, (EB) 996/2010 eta (EB) 376/2014 erregelamenduak eta 2014/30/EB eta 2014/53/EB zuzentarauak aldatzen dituen eta Europako Parlamentuaren eta Kontseiluaren (EE) 552/2004 eta (EE) 216/2008 erregelamenduak eta Kontseiluaren (EEE) 3922/91 Erregelamendua indargabetzen dituen ([2018/08/22ko EBAO, L 212, 1. or.](#)), baldin eta 2.1.a) eta 2.1.b) artikuluetan aipatutako aireontziak diseinatu, ekoitzi eta merkatuan jartzeari eragiten badie, tripulaziorik gabeko aireontziei eta haien motor, helize, osagai eta urrutitik kontrolatzeko ekipamenduei dagokienez

ANEXO II

Lista de los delitos a que se refiere el artículo 5, apartado 1, párrafo primero, letra h), inciso iii)

Delitos a que se refiere el artículo 5, apartado 1, párrafo primero, letra h), inciso iii):

- terrorismo,
- trata de seres humanos,
- explotación sexual de menores y pornografía infantil,
- tráfico ilícito de estupefacientes o sustancias psicotrópicas,
- tráfico ilícito de armas, municiones y explosivos,
- homicidio voluntario, agresión con lesiones graves,
- tráfico ilícito de órganos o tejidos humanos,
- tráfico ilícito de materiales nucleares o radiactivos,
- secuestro, detención ilegal o toma de rehenes,
- delitos que son competencia de la Corte Penal Internacional,

II. ERANSKINA

5.1.1.h.iii) artikuluan aipatzen diren delituen zerrenda:

Hauak dira 5.1.1.h.iii) artikuluan aipatutako delituak:

- terrorismoa;
- gizakien salerosketa;
- adingabeen sexu-esplotazioa eta haur-pornografia;
- estupefazianteen eta substantzia psikotropikoen legez kontrako trafikoa;
- armen, munizioen eta lehergailuen legez kontrako trafikoa;
- borondatezko giza hilketak eta lesio larriak eragiten dituen erasoak;
- giza organoen edo ehunen legez kontrako trafikoa;
- material nuklearren edo erradioaktiboen legez kontrako trafikoa;
- bahiketa, legearen aurkako atxiloketa eta bahituak hartzea;
- Nazioarteko Zigor Auzitegiaren eskumena diren delituak;



- secuestro de aeronaves o buques,
 - violación,
 - delitos contra el medio ambiente,
 - robo organizado o a mano armada,
 - sabotaje,
 - participación en una organización delictiva implicada en uno o varios de los delitos enumerados en esta lista.
- aireontziak eta ontziak bahitzea;
 - bortxaketa;
 - ingurumenaren kontrako delituak;
 - antolatutako lapurreta edo armak erabiliz egindakoak;
 - sabotajea;
 - zerrenda honetako delituen batean edo batzuetan inplikaturako antolakunde kriminal batean parte hartzea.

ANEXO III

Sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2

Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA que formen parte de cualquiera de los ámbitos siguientes:

1. Biometría, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:

a) Sistemas de identificación biométrica remota

Quedan excluidos los sistemas de IA destinados a ser utilizados con fines de verificación biométrica cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser

b) Sistemas de IA destinados a ser utilizados para la categorización biométrica en función de atributos o características sensibles o protegidos basada en la inferencia de dichos atributos o características

c) Sistemas de IA destinados a ser utilizados para el reconocimiento de emociones

2. Infraestructuras críticas: Sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o del suministro de agua, gas, calefacción o electricidad

3. Educación y formación profesional:

a) Sistemas de IA destinados a ser utilizados para determinar el acceso o la admisión de personas físicas a centros educativos y de formación profesional a todos

III. ERANSKINA

6.2 artikuluan aipatzen diren arrisku handiko AA-sistemak

Erregelamendu honen 6.2 artikulua araberako arrisku handiko AA-sistemak eremu hauetako edozeinetan dauden AA-sistemak dira:

1. Biometria, baldin eta aplikatzekoa den Batasuneko zuzenbideak edo zuzenbide nazionalak erabilera hori egiteko baimena ematen badu:

a) Urruneko identifikazio biometrikoko sistemak.

Kanpoan geratzen dira egiaztapen biometrikorako erabiliko diren AA-sistemak, zeinetan helburu bakarra baita ziurtatzea pertsona fisiko baten identitatea hark esandakoarekin bat datorrela.

b) Bereziki babestu beharreko atributu edo ezaugarrien araberako kategorizazio biometrikorako erabiliko diren AA-sistemak, atributu edo ezaugarri horien inferentzia oinarrituta.

c) Emozioak ezagutzeko erabiliko diren AA-sistemak.

2. Azpiegitura kritikoak: Azpiegitura digital kritikoen eta ibilgailuen trafikoaren edo ur-, gas-, berokuntza- edo elektrizitate-horniduraren kudeaketan eta funtzionamenduan segurtasun-osagai gisa erabiliko diren AA-sistemak.

3. Hezkuntza eta lanbide-heziketa:

a) Ikastetxeetan eta lanbide-heziketako zentroetan, maila guztietan, pertsona fisikoak sartzeko edo onartzeko moduak zehazteko zein pertsona fisikoak



los niveles o para distribuir a las personas físicas entre dichos centros

b) Sistemas de IA destinados a ser utilizados para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje de las personas físicas en centros educativos y de formación profesional a todos los niveles

c) Sistemas de IA destinados a ser utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles

d) Sistemas de IA destinados a ser utilizados para el seguimiento y la detección de comportamientos prohibidos por parte de los estudiantes durante los exámenes en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles

4. Empleo, gestión de los trabajadores y acceso al autoempleo:

a) Sistemas de IA destinados a ser utilizados para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos

b) Sistemas de IA destinados a ser utilizados para tomar decisiones que afecten a las condiciones de las relaciones de índole laboral o a la promoción o rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales o para supervisar y evaluar el rendimiento y el comportamiento de las personas en el marco de dichas relaciones

5. Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones:

a) Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución

b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su

ikastetxe horien artean banatzeko erabiliko diren AA-sistemak.

b) Ikastetxeetan eta lanbide-heziketako zentroetan, maila guztietan, ikaskuntzaren emaitzak ebaluatzeko erabiliko diren AA-sistemak, baita emaitza horiek pertsona fisikoen ikaskuntza-prozesua bideratzeko erabiltzen direnean ere.

c) Ikastetxeen eta lanbide-heziketako zentroen testuinguruan edo horien barruan, maila guztietan, pertsona batek jasoko duen edo eskuragarri izango duen hezkuntza-maila egokia ebaluatzeko erabiliko diren AA-sistemak.

d) Ikastetxeen eta lanbide-heziketako zentroen testuinguruan edo horien barruan, maila guztietan, azterketak egin bitartean ikasleek portaera debekatuak egiten ote dituzten zaintzeko eta detektatzeko erabiliko diren AA-sistemak.

4. Enplegua, langileen kudeaketa eta autoenplegurako sarbidea:

a) Pertsona fisikoak kontratatze edo hautatzeko erabiliko diren AA-sistemak, bereziki enplegurako iragarki espezifikoak argitaratzeko, enplegu-eskaerak aztertu eta iragazteko eta hautagaiak ebaluatzeko.

b) Lan-harremanen baldintzei eragiten dieten erabakiak hartzeko edo lan-izaerako kontratu-harremanak sustatzeko edo hutsaltzeko, zereginak esleitzeko portaera indibidualetatik edo bereizgarri edo ezaugarri pertsonaletatik abiatuta, edo pertsonen harreman horien esparruan duten errendimendua eta portaera gainbegiratzeko eta ebaluatzeko erabiliko diren AA-sistemak.

5. Funtsezko zerbitzu pribatuertako eta funtsezko zerbitzu eta prestazio publikoertako sarbidea izatea, eta zerbitzu eta prestazio horiez gozatzea:

a) Pertsona fisikoek laguntza publikoko funtsezko prestazio eta zerbitzuak —osasun-laguntzako zerbitzuak barne— erabili ahal izateko onargarritasuna ebaluatzeko, bai eta zerbitzu eta prestazio horiek emateko, murrizteko edo kentzeko edo itzultzea erreklamatzeko ere, agintaritza publikoek —edo haien izenean dihardutenek— erabiliko dituzten AA-sistemak.

b) Pertsona fisikoen kaudimena ebaluatzeko edo haien kreditu-kalifikazioa ezartzeko erabiliko diren AA-



calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes financieros

c) Sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud

d) Sistemas de IA destinados a ser utilizados para la evaluación y la clasificación de las llamadas de emergencia realizadas por personas físicas o para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo, policía, bomberos y servicios de asistencia médica, y en sistemas de triaje de pacientes en el contexto de la asistencia sanitaria de urgencia

6. Garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:

a) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho, o en su nombre, para evaluar el riesgo de que una persona física sea víctima de delitos

b) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho como polígrafos o herramientas similares

c) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para evaluar la fiabilidad de las pruebas durante la investigación o el enjuiciamiento de delitos

d) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito atendiendo no solo a la elaboración de perfiles de personas físicas mencionada en el artículo 3, punto 4, de la Directiva (UE) 2016/680 o para evaluar rasgos y características de la personalidad o comportamientos delictivos pasados de personas físicas o colectivos

sistemas, finantza-iruzurrak detektatzeko erabiltzen diren AA-sistemak izan ezik.

c) Bizi-aseguruen eta osasun-aseguruen kasuan, pertsona fisikoen arabera prezioak finkatzeko eta arriskuak ebaluatzeko erabiliko diren AA-sistemak.

d) Pertsona fisikoek egindako larrialdi-deiak ebaluatzeko eta sailkatzeko erabiliko diren AA-sistemak edo larrialdi-egoeretan lehen mailako eskuhartze-zerbitzuak bidaltzeko lehentasunak ezartzeko erabiliko direnak (polizia, suhiltzaileak eta laguntza medikoko zerbitzuak, esaterako), bai eta larrialdiko osasun-laguntzan pazienteak larritasunaren arabera sailkatzeko sistemak ere.

6. Zuzenbidea betearaztea, baldin eta aplikatzekoa den Batasuneko zuzenbideak edo zuzenbide nazionalak erabilera hori egiteko baimena ematen badu:

a) Pertsona fisiko batek delituen biktima izateko zer arrisku duen ebaluatzeko orduan, zuzenbidea betearazteko agintaritzek —edo haien izenean dihardutenek— edo zuzenbidea betearazteko agintaritzek laguntzeko Batasuneko instituzio, organo edo organismoek —edo haien izenean dihardutenek— erabiliko dituzten AA-sistemak.

b) Zuzenbidea betearazteko agintaritzek —edo haien izenean dihardutenek— edo zuzenbidea betearazteko agintaritzek laguntzeko Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak, esaterako poligrafoak eta antzeko beste tresna batzuk.

c) Delituak ikertzen edo epaitzen diren bitartean frogen fidagarritasuna ebaluatzeko orduan, zuzenbidea betearazteko agintaritzek —edo haien izenean dihardutenek— edo zuzenbidea betearazteko agintaritzek laguntzeko Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak.

d) Pertsona fisiko batek delitu bat egiteko edo delitu berean berrerortzeko nolako arriskua duen ebaluatzeko orduan —ez bakarrik (EB) 2016/680 Zuzentarauaren 3.4 artikuluan aipatutako pertsona fisikoen profilaketan edo pertsona fisikoen edo pertsona-taldeen nortasunaren bereizgarri edo ezaugarrien edo izandako delitu-portaeren ebaluazioan oinarrituta—, zuzenbidea betearazteko agintaritzek —edo haien izenean dihardutenek— edo zuzenbidea betearazteko agintaritzek laguntzeko Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak.



e) Sistemas de IA destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos y organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para elaborar perfiles de personas físicas, como se menciona en el artículo 3, punto 4, de la Directiva (UE) 2016/680, durante la detección, la investigación o el enjuiciamiento de delitos

7. Migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable:

a) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, como polígrafos o herramientas similares

b) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para evaluar un riesgo, por ejemplo, un riesgo para la seguridad, la salud o de migración irregular, que plantee una persona física que tenga la intención de entrar en el territorio de un Estado miembro o haya entrado en él

c) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado o permiso de residencia y las reclamaciones conexas con el fin de determinar si las personas físicas solicitantes reúnen los requisitos necesarios para que se conceda su solicitud, con inclusión de la evaluación conexa de la fiabilidad de las pruebas

d) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, en el contexto de la migración, el asilo o la gestión del control fronterizo, con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje

8. Administración de justicia y procesos democráticos:

a) Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios;

e) Delituak detektatu, ikertu edo epaitu bitartean pertsona fisikoen profilak egiteko orduan —(EB) 2016/680 Zuzentarauaren 3.4 artikuluan aipatzen den bezala—, zuzenbidea betearazteko agintaritzek —edo haien izenean dihardutenek— edo zuzenbidea betearazteko agintaritzei laguntzeko Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak.

7. Migrazioa, asiloa eta muga-kontrolaren kudeaketa, baldin eta aplikatzekoa den Batasuneko zuzenbideak edo zuzenbide nazionalak erabilera hori egiteko baimena ematen badu:

a) Agintaritza publiko eskudunek —edo haien izenean dihardutenek— edo Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak, esaterako poligrafoak eta antzeko beste tresna batzuk.

b) Estatu kide bateko lurraldean sartu den edo sartzeko asmoa duen pertsona fisiko batek ekar dezakeen arrisku bat ebaluatzeko orduan —esaterako segurtasunerako, osasunerako edo migrazio irregularrerako arrisku bat— agintaritza publiko eskudunek —edo haien izenean dihardutenek— edo Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak.

c) Asiloa, bisa eta bizileku-baimena eskuratzeko eskaerak, bai eta horiei lotutako erreklamazioak ere, aztertzeko orduan, agintaritza publiko eskudunek —edo haien izenean dihardutenek— edo agintaritza publiko eskudunei laguntzeko Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak, informazio horren bidez zehaztu ahal izateko ea pertsona fisiko eskatzaileek beren eskaerak onartzeko beharrezkoak diren betekizunak betetzen dituzten —frogen fidagarritasunari buruzko ebaluazioa barne hartuta—.

d) Migrazioaren, asiloaren edo muga-kontrolaren kudeaketari begira pertsona fisikoak detektatzeko, ezagutzeko edo identifikatzeko, agintaritza publiko eskudunek —edo haien izenean dihardutenek— edo Batasuneko instituzio, organo edo organismoek erabiliko dituzten AA-sistemak, salbuespen dela bidaia-agirien egiaztapena.

8. Justizia-administrazioa eta prozesu demokratikoak:

a) Egitateak eta legea ikertzeko zein interpretatzeko, egitate jakin batzuetan zuzenbidea betearazteko edo auziak bide ez-judizialek ebazteko, agintaritza judizial batek —edo haren izenean dihardutenek— agintaritza judizial bati laguntzeko erabiliko dituzten AA-sistemak.



b) Sistemas de IA destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de personas físicas que ejerzan su derecho de voto en elecciones o referendos. Quedan excluidos los sistemas de IA a cuyos resultados de salida no estén directamente expuestos las personas físicas, como las herramientas utilizadas para organizar, optimizar o estructurar campañas políticas desde un punto de vista administrativo o logístico.

b) Hauteskunde edo erreferendum baten emaitzan edo pertsona fisikoek hauteskundeetan edo erreferendumetan botoa ematean duten hauteskunde-portaeran eragiteko erabiliko diren AA-sistemak. AA-sistemen irteera-emaitzek pertsona fisikoengan zuzenean eragiten ez badute, sistema horiek sailkapen honetatik kanpo geratzen dira —adibidez, kanpaina politikoak ikuspegi administratibo eta logistikotik antolatzeko, optimizatzeko eta egituratzeko erabiltzen diren tresnak—.

ANEXO IV

IV. ERANSKINA

Documentación técnica a que se refiere el artículo 11, apartado 1

11.1 artikuluan aipatzen den dokumentazio teknikoak

La documentación técnica a que se refiere el artículo 11, apartado 1, incluirá como mínimo la siguiente información, aplicable al sistema de IA pertinente:

Dokumentazio teknikoak —11.1 artikuluan aipatzen da— dagokion AA-sistemari aplikatzekoa zaion informazio hau jasoko du gutxienez:

1. Una descripción general del sistema de IA que incluya:

1. AA-sistemaren deskribapen orokorra; alderdi hauek jasoko ditu:

a) su finalidad prevista, el nombre del proveedor y la versión del sistema de tal manera que se refleje su relación con versiones anteriores;

a) Helburu aurreikusia, hornitzailearen izena eta sistemaren bertsioa, aurreko bertsioekin duen lotura islatzeko moduan.

b) la manera en que el sistema de IA interactúa o puede utilizarse para interactuar con hardware o software, también con otros sistemas de IA, que no formen parte del propio sistema de IA, cuando proceda;

b) AA-sistemak nola elkarreragiten duen edo nola erabil daitekeen elkarreragiteko bai hardwarearekin edo softwarearekin, baita AA-sistemaren parte ez diren beste AA-sistema batzuekin ere, hala dagokionean.

c) las versiones de software o firmware pertinentes y todo requisito relacionado con la actualización de versiones;

c) Egoki diren software- edo firmware-bertsioak eta bertsioak eguneratzearekin lotutako betekizun guztiak.

d) la descripción de todas las formas en que el sistema de IA se introduce en el mercado o se pone en servicio, como paquetes de software integrados en el hardware, descargas o API;

d) AA-sistema merkatuan jartzeko edo zerbitzuan ipintzeko modu guztien deskribapena —esaterako, hardwarean integratutako software-paketea, deskargak edo APIak—.

e) la descripción del hardware en el que está previsto que se ejecute el sistema de IA;

e) AA-sistema exekutatzeko aurreikusi den hardwarearen deskribapena.

f) en el caso de que el sistema de IA sea un componente de un producto, fotografías o ilustraciones de las características exteriores, el marcado y la configuración interna de dicho producto;

f) Baldin eta AA-sistema kanpoko ezaugarriak azaltzen dituen produktu, argazki edo ilustrazio baten osagaia bada, produktu horren barne-konfigurazioa eta marka.

g) una descripción básica de la interfaz de usuario facilitada al responsable del despliegue;

g) Hedapenaren arduradunari eman zaion erabiltzaile-interfazearen oinarritzko deskribapena.

h) instrucciones de uso para el responsable del despliegue y una descripción básica de la interfaz de

h) Hedapenaren arduradunarentzako erabilera-jarraibideak eta hedapenaren arduradunari eman zaion



usuario facilitada al responsable del despliegue, cuando proceda.

2. Una descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo, incluidos:

a) los métodos y las medidas adoptados para el desarrollo del sistema de IA, incluido, en su caso, el recurso a sistemas o herramientas previamente entrenados facilitados por terceros y la manera en que han sido utilizados, integrados o modificados por el proveedor;

b) las especificaciones de diseño del sistema, a saber, la lógica general del sistema de IA y de los algoritmos; las decisiones clave de diseño, incluidos la lógica y los supuestos de los que se ha partido, también con respecto a las personas o colectivos de personas en relación con los que está previsto que se utilice el sistema; las principales decisiones de clasificación; aquello que el sistema está diseñado para optimizar y la pertinencia de los diversos parámetros; la descripción de los resultados de salida esperados del sistema y la calidad de dichos resultados; las decisiones adoptadas acerca de cualquier posible concesión con respecto a las soluciones técnicas adoptadas para dar cumplimiento a los requisitos establecidos en el capítulo III, sección 2;

c) la arquitectura del sistema, con una explicación de la manera en que los componentes del software se utilizan o enriquecen mutuamente y de la manera en que se integran en el procesamiento general; los recursos informáticos utilizados para desarrollar, entrenar, probar y validar el sistema de IA;

d) cuando proceda, los requisitos en materia de datos, en forma de fichas técnicas que describan las metodologías y técnicas de entrenamiento, así como los conjuntos de datos de entrenamiento utilizados, e incluyan una descripción general de dichos conjuntos de datos e información acerca de su procedencia, su alcance y sus características principales; la manera en que se obtuvieron y seleccionaron los datos; los procedimientos de etiquetado (p. ej., para el aprendizaje supervisado) y las metodologías de depuración de datos (p. ej., la detección de anomalías);

e) una evaluación de las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluida una evaluación de las medidas técnicas necesarias para facilitar la interpretación de los resultados de salida de los sistemas de IA por parte de los responsables del despliegue, con arreglo al artículo 13, apartado 3, letra d);

erabiltzaile-interfazearen oinarritzko deskribapena, hala dagokionean.

2. AA-sistemako elementuen eta horien garapen-prozesuaren deskribapen zehatza; datu hauek jasoko ditu:

a) AA-sistemak garatzeko erabili diren metodo eta neurriak, barnean hartuta, hala badagokio, hirugarrenek emandakoak diren eta aurretik entrenatuta dauden sistemak edo tresnak, eta nola erabili, integratu edo aldatu dituen hornitzaileak.

b) Sistemaren diseinuari buruzko zehaztapenak, hau da: AA-sistemaren eta algoritmoen logika orokorra; diseinuari buruzko funtsezko erabakiak, abiapuntutzat hartu diren kasuak eta logika barne, baita sistema erabiliko dutela aurreikusi den pertsona edo pertsona-taldeei dagokienez ere; sailkatzeko erabaki nagusiak; zer optimizatzeko diseinatu den sistema eta parametroen egokitasuna; sistematik espero diren irteera-emaizten deskribapena eta emaitza horien kalitatea; III. kapituluko 2. atalean ezarritako betekizunak betetzeko hartu diren soluzio teknikoei dagokienez egin daitekeen edozein emakidari buruz hartutako erabakiak.

c) Sistemaren arkitektura, softwarearen osagaiak elkarren artean nola erabiltzen edo aberasten diren eta prozesamendu orokorrean nola integratzen diren azalduz; AA-sistema garatu, entrenatu, probatu eta balioztatzeke erabili diren baliabide informatikoak.

d) Hala dagokionean, datuen arloko betekizunak, entrenamendu-metodologiak eta -teknikak deskribatzen dituzten fitxa teknikoen bidez, bai eta erabili diren entrenamendu-datuen multzoak ere, hauei buruzko deskribapen orokor bat ere emanez: nondik eskuratu diren, nolako irismena duten eta zein diren haien ezaugarri nagusiak; nola lortu eta hautatu ziren datuak; etiketatzeke zer prozedura erabili diren (adibidez, gainbegiraturako ikaskuntzarako), eta zer metodologia erabili den datuak arazteko (adibidez, anomaliak detektatzea).

e) 14. artikulua araberako beharrezkoak diren giza ikuskarpeneko neurrien ebaluazioa, barne hartuta hedapenaren arduradunek AA-sistemen irteera-emaizak errazago interpretatzeko beharrezkoak diren neurri teknikoen ebaluazioa, 13.3.d) artikulua araberako.



f) en su caso, una descripción detallada de los cambios predeterminados en el sistema de IA y su funcionamiento, junto con toda la información pertinente relativa a las soluciones técnicas adoptadas con el objetivo de garantizar la conformidad permanente del sistema de IA con los requisitos pertinentes establecidos en el capítulo III, sección 2;

g) los procedimientos de validación y prueba utilizados, incluida la información acerca de los datos de validación y prueba empleados y sus características principales; los parámetros utilizados para medir la precisión, la solidez y el cumplimiento de otros requisitos pertinentes establecidos en el capítulo III, sección 2, así como los efectos potencialmente discriminatorios; los archivos de registro de las pruebas y todos los informes de las pruebas fechados y firmados por las personas responsables, también en lo que respecta a los cambios predeterminados a que se refiere la letra f);

h) las medidas de ciberseguridad adoptadas.

3. Información detallada acerca de la supervisión, el funcionamiento y el control del sistema de IA, en particular con respecto a sus capacidades y limitaciones de funcionamiento, incluidos los niveles de precisión para las personas o colectivos de personas específicos en relación con los que está previsto que se utilice el sistema y el nivel general de precisión esperado en relación con su finalidad prevista; los resultados no deseados previsibles y las fuentes de riesgo para la salud y la seguridad, los derechos fundamentales y la discriminación, en vista de la finalidad prevista del sistema de IA; las medidas de supervisión humana necesarias de conformidad con el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de los resultados de salida de los sistemas de IA por parte de los responsables del despliegue; las especificaciones de los datos de entrada, según proceda.

4. Una descripción de la idoneidad de los parámetros de rendimiento para el sistema de IA concreto.

5. Una descripción detallada del sistema de gestión de riesgos con arreglo al artículo 9.

6. Una descripción de los cambios pertinentes realizados por el proveedor en el sistema a lo largo de su ciclo de vida.

7. Una lista de las normas armonizadas, aplicadas total o parcialmente, cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea; cuando no se hayan aplicado normas armonizadas, una descripción detallada de las soluciones adoptadas para

f) Hala badagokio, AA-sisteman aurrez zehaztutako aldaketen eta horien funtzionamenduaren deskribapen zehatza, beharrezko den informazio guztia emanaz AA-sistema III. kapituluko 2. atalean ezarritako betekizunekin etengabe bat datorrela bermatzeko hartu diren soluzio teknikoei buruz.

g) Balioztatzeko eta probak egiteko erabili diren prozedurak, balioztatze- eta proba-datuei buruzko informazioa eta haien ezaugarri nagusiak barne; zehaztasuna, sendotasuna eta III. kapituluko 2. atalean ezarritako beste betekizun batzuk betetzen direla neurtzeko erabili diren parametroak, bai eta diskriminatzaileak izan daitezkeen ondorioak ere; proben erregistro-artxiboak eta proben txosten guztiak, data jarrita eta arduradunek sinatuta, baita f) letran aipatu diren aurrez zehaztutako aldaketei dagokienez ere.

h) Zibersegurtasunari dagokionez hartu diren neurriak.

3. AA-sistemaren gainbegiratzeari, funtzionamenduari eta kontrolari buruzko informazio zehatza, bereziki haren funtzionamendu-gaitasun eta -mugei dagokienez, barnean hartuta sistema erabiliko dutela aurreikusi den pertsona edo pertsona-talde espezifikoentzako zehaztasun-mailak eta helburu aurreikusari dagokienez espero den zehaztasun-maila orokorra; aurreikus daitezkeen nahi gabeko emaitzak eta osasunerako, segurtasunerako, oinarritzko eskubideetarako eta diskriminaziorako arrisku-iturriak, AA-sistemaren helburu aurreikusia kontuan hartuta; 14. artikulua arabera beharrezkoak diren giza ikuskapeneko neurriak, barne hartuta hedapenaren arduradunek AA-sistemen irteera-emaitzak errazago interpretatzeko beharrezkoak diren neurri teknikoak; sarrera-datuen zehaztapenak, dagokionaren arabera.

4. Errendimendu-parametroek AA-sistema zehatzerako duten egokitasunaren deskribapena.

5. Arriskuak kudeatzeko sistemaren deskribapen zehatza, 9. artikulua arabera.

6. Sistemaren bizi-ziklo osoan hornitzaileak egin dituen aldaketa egokien deskribapena.

7. Guztiz edo zati batean aplikatu diren arau harmonizatuen zerrenda, horien erreferentziak Europar Batasunaren Aldizkari Ofizialean argitaratu direnean; arau harmonizaturik aplikatu ez denean, III. kapituluko 2. atalean ezarritako betekizunak betetzeko hartu diren



cumplir los requisitos establecidos en el capítulo III, sección 2, incluida una lista de otras normas y especificaciones técnicas pertinentes que se hayan aplicado.

8. Una copia de la declaración UE de conformidad de conformidad con el artículo 47.

9. Una descripción detallada del sistema establecido para evaluar el funcionamiento del sistema de IA en la fase posterior a la comercialización, de conformidad con el artículo 72, incluido el plan de vigilancia poscomercialización a que se refiere el artículo 72, apartado 3.

soluzioen deskribapen zehatza, aplikatu diren bestelako arau eta zehaztapen tekniko egokien zerrenda barne.

8. EB adostasun-adierazpenaren kopia bat, 47. artikuluaaren arabera.

9. Merkaturatu osteko fasean AA-sistemaren funtzionamendua ebaluatzeko ezarritako sistemaren deskribapen zehatza, 72. artikuluaaren arabera, 72.3 artikuluan aipatzen den merkaturatu osteko zaintza-plana barne.

ANEXO V

Declaración UE de conformidad

La declaración UE de conformidad a que se hace referencia en el artículo 47 contendrá toda la información siguiente:

1. El nombre y tipo del sistema de IA, y toda referencia inequívoca adicional que permita la identificación y trazabilidad del sistema de IA.
2. El nombre y la dirección del proveedor o, en su caso, de su representante autorizado.
3. La afirmación de que la declaración UE de conformidad con el artículo 47 se expide bajo la exclusiva responsabilidad del proveedor.
4. La declaración de que el sistema de IA es conforme con el presente Reglamento y, en su caso, con cualquier otra disposición de Derecho de la Unión pertinente que disponga la expedición de la declaración UE de conformidad con el artículo 47.
5. Cuando un sistema de IA implique el tratamiento de datos personales, la declaración de que el sistema de IA se ajusta al Reglamento (UE) 2016/679, al Reglamento (UE) 2018/1725 y a la Directiva (UE) 2016/680.
6. Referencias a todas las normas armonizadas pertinentes que se hayan aplicado o a cualquier otra especificación común respecto de la que se declara la conformidad.
7. En su caso, el nombre y el número de identificación del organismo notificado, una descripción del procedimiento de evaluación de la conformidad que se haya seguido y la identificación del certificado expedido.

V. ERANSKINA

EB adostasun-adierazpena

EB adostasun-adierazpenak —47. artikuluan dago aipatuta— informazio hau guztia jasoko du:

1. AA-sistemaren izena eta mota, eta AA-sistemaren identifikazioa eta trazabilitatea ahalbidetzen duen erreferentzia argi gehigarri oro.
2. Hornitzailearen izena eta helbidea, eta, hala badagokio, ordezkari baimenduarena.
3. Hau dioen adierazpen bat: 47. artikuluaaren arabera EB adostasun-adierazpenaren erantzukizun osoa hornitzailearena dela.
4. Hau dioen adierazpen bat: AA-sistema ados datorrela erregelamendu honekin eta, hala badagokio, 47. artikuluaaren arabera EB adostasun-adierazpena egitea xedatzen duen Batasuneko beste edozein zuzenbide-xedapenekin.
5. AA-sistema batek datu pertsonalen tratamendua eskatzen duenean, hau dioen adierazpen bat: AA-sistema bat datorrela (EB) 2016/679 Erregelamenduan, (EB) 2018/1725 Erregelamenduan eta (EB) 2016/680 Zuzentarauan ezarritakoarekin.
6. Adostasun-adierazpena egiteko aplikatu diren arau harmonizatu guztien edo bestelako zehaztapen komunen erreferentziak.
7. Hala badagokio, organismo jakinaraziaren izena eta identifikazio-zenbakia, adostasuna ebaluatzeko jarraitu den prozeduraren deskribapena eta emandako ziurtagiriaren identifikazioa.



8. El lugar y la fecha de expedición de la declaración, el nombre y el cargo de la persona que la firme, la indicación de la persona en cuyo nombre o por cuya cuenta firma la declaración y la firma.

8. Non eta noiz egin den adierazpena, sinatzen duen pertsonaren izena eta kargua, noren izenean egin edo sinatu den adierazpena eta sinadura.

ANEXO VI

Procedimiento de evaluación de la conformidad fundamentado en un control interno

1. El procedimiento de evaluación de la conformidad fundamentado en un control interno es el procedimiento de evaluación de la conformidad basado en los puntos 2, 3 y 4.
2. El proveedor comprueba que el sistema de gestión de la calidad establecido cumple los requisitos establecidos en el artículo 17.
3. El proveedor examina la información de la documentación técnica para evaluar la conformidad del sistema de IA con los requisitos esenciales pertinentes establecidos en el capítulo III, sección 2.
4. Asimismo, el proveedor comprueba que el proceso de diseño y desarrollo del sistema de IA y la vigilancia poscomercialización del mismo a que se refiere el artículo 72 son coherentes con la documentación técnica.

VI. ERANSKINA

Barne-kontrolean oinarritutako adostasuna ebaluatzeke prozedura

1. Barne-kontrolean oinarritutako adostasuna ebaluatzeke prozedura 2., 3. eta 4. puntuetan oinarritutako adostasuna ebaluatzeke prozedura da.
2. Hornitzaileak egiaztatuko du kalitatea kudeatzeko ezarritako sistemak 17. artikuluan ezarritako betekizunak betetzen dituela.
3. Hornitzaileak dokumentazio teknikoaren informazioa aztertuko du, ebaluatzeke ea AA-sistema bat datorren III. kapituluko 2. atalean ezarritako funtsezko betekizunekin.
4. Era berean, hornitzaileak egiaztatuko du ea AA-sistema diseinatu eta garatzeko prozesua eta 72. artikuluan aipatzen den merkaturatu osteko zaintza bat datozen dokumentazio teknikoarekin.

ANEXO VII

Conformidad fundamentada en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica

1. Introducción

La conformidad fundamentada en la evaluación del sistema de gestión de la calidad y la evaluación de la documentación técnica es el procedimiento de evaluación de la conformidad basado en los puntos 2 a 5.

2. Presentación general

El sistema de gestión de la calidad aprobado en relación con el diseño, el desarrollo y las pruebas de los sistemas de IA con arreglo al artículo 17 se examinará de conformidad con el punto 3 y será objeto de vigilancia con arreglo a lo establecido en el punto 5. La documentación técnica del sistema de IA se examinará de conformidad con el punto 4.

VII. ERANSKINA

Kalitatea kudeatzeko sistemaren ebaluazioan eta dokumentazio teknikoaren ebaluazioan oinarritutako adostasuna

1. Atariko

Kalitatea kudeatzeko sistemaren ebaluazioan eta dokumentazio teknikoaren ebaluazioan oinarritutako adostasuna 2.etik 5.era bitarteko puntuetan oinarritutako adostasuna ebaluatzeke prozedura da.

2. Aurkezpen orokorra

AA-sistemen diseinuari, garapenari eta probei dagokienez onartutako kalitatea kudeatzeko sistema — 17. artikuluan dago zehaztuta — 3. puntuaren arabera aztertuko da, eta 5. puntuan ezarritakoaren arabera zainduko da. AA-sistemaren dokumentazio teknikoa 4. puntuaren arabera aztertuko da.



3. Sistema de gestión de la calidad

3.1. La solicitud del proveedor incluirá:

a) el nombre y la dirección del proveedor y, si es el representante autorizado quien presenta la solicitud, también su nombre y dirección;

b) la lista de los sistemas de IA a los que se aplica el mismo sistema de gestión de la calidad;

c) la documentación técnica de cada sistema de IA al que se aplica el mismo sistema de gestión de la calidad;

d) la documentación relativa al sistema de gestión de la calidad, que cubrirá todos los aspectos enumerados en el artículo 17;

e) una descripción de los procedimientos establecidos para garantizar que el sistema de gestión de la calidad sigue siendo adecuado y eficaz;

f) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de gestión de la calidad será evaluado por el organismo notificado, que determinará si cumple los requisitos especificados en el artículo 17.

La decisión se notificará al proveedor o a su representante autorizado.

La notificación incluirá las conclusiones de la evaluación del sistema de gestión de la calidad y una decisión motivada sobre la evaluación.

3.3. El proveedor continuará aplicando y manteniendo el sistema de gestión de la calidad aprobado de forma que siga siendo adecuado y eficaz.

3.4. El proveedor comunicará al organismo notificado toda modificación prevista del sistema de gestión de la calidad aprobado o de la lista de sistemas de IA a los que este se aplica.

El organismo notificado examinará los cambios propuestos y decidirá si el sistema de gestión de la calidad modificado sigue cumpliendo los requisitos mencionados en el punto 3.2 o si es necesario realizar una nueva evaluación.

El organismo notificado notificará su decisión al proveedor. La notificación incluirá las conclusiones del

3. Kalitatea kudeatzeko sistema

3.1. Datu hauek jasoko dira hornitzailearen eskaeran:

a) Hornitzailearen izena eta helbidea, eta, ordezkari baimenduak aurkezten badu eskaera, haren izena eta helbidea.

b) Kalitatea kudeatzeko sistema bera aplikatzen zaien AA-sistemen zerrenda.

c) Kalitatea kudeatzeko sistema bera aplikatzen zaien AA-sistema guztien dokumentazio teknikoa.

d) Kalitatea kudeatzeko sistemaren dokumentazioa, 17. artikuluan zerrendatutako alderdi guztiak betez.

e) Kalitatea kudeatzeko sistemak egokia eta eraginkorra izaten jarraitzen duela bermatzeko ezarritako prozeduren deskribapena.

f) Hau dioen idatzizko adierazpen bat: ez zaiola eskaera bera aurkeztu beste organismo jakinarazi bati.

3.2. Organismo jakinaraziak ebaluatuko du kalitatea kudeatzeko sistema, eta hark zehaztuko du ea 17. artikuluan zehaztutako betekizunak betetzen dituen ala ez.

Erabakia hornitzaileari edo haren ordezkari baimenduari jakinaraziko zaio.

Jakinarazpenean, kalitatea kudeatzeko sistemaren ebaluazioaren ondorioak eta ebaluazioari buruzko erabaki arrazoitua jasoko dira.

3.3. Hornitzaileak onartu den kalitatea kudeatzeko sistema aplikatzen eta mantentzen jarraituko du, egokia eta eraginkorra izaten jarrai dezan.

3.4. Baldin eta onartu den kalitatea kudeatzeko sisteman edo sistema hori aplikatzen zaien AA-sistemetan aldaketaren bat egitea aurreikusten bada, hornitzaileak organismo jakinaraziari jakinaraziko dio.

Organismo jakinaraziak, orduan, proposatutako aldaketak aztertuko ditu, eta erabakiko du ea aldatu den kalitatea kudeatzeko sistemak oraindik betetzen dituen 3.2 puntuan aipatutako betekizunak edo beste ebaluazio bat egin behar den.

Organismo jakinaraziak hornitzaileari jakinaraziko dio bere erabakia. Jakinarazpenean, azterketaren ondorioak eta ebaluazioari buruzko erabaki arrazoitua jasoko dira.



examen de los cambios y una decisión motivada sobre la evaluación.

4. Control de la documentación técnica

4.1. Además de la solicitud a que se refiere el punto 3, el proveedor presentará una solicitud ante el organismo notificado de su elección para la evaluación de la documentación técnica relativa al sistema de IA que el proveedor pretenda introducir en el mercado o poner en servicio y al que se aplique el sistema de gestión de la calidad mencionado en el punto 3.

4.2. La solicitud incluirá:

- a) el nombre y la dirección del proveedor;
- b) una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado;
- c) la documentación técnica prevista en el anexo IV.

4.3. El organismo notificado examinará la documentación técnica. Cuando proceda, y en la medida en que sea necesario para el desempeño de sus tareas, se concederá al organismo notificado pleno acceso a los conjuntos de datos de entrenamiento, validación y prueba utilizados, también, cuando proceda y con sujeción a garantías de seguridad, a través de API u otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia.

4.4. Al examinar la documentación técnica, el organismo notificado podrá exigir que el proveedor facilite más pruebas justificativas o que lleve a cabo pruebas adicionales para que pueda evaluarse adecuadamente la conformidad del sistema de IA con los requisitos establecidos en el capítulo III, sección 2. Cuando el organismo notificado no quede satisfecho con las pruebas realizadas por el proveedor, efectuará él mismo directamente las pruebas adecuadas, según proceda.

4.5. Asimismo, se concederá al organismo notificado acceso al modelo de entrenamiento y al modelo entrenado del sistema de IA, con sus correspondientes parámetros, para, en caso necesario, una vez se hayan agotado y hayan demostrado ser insuficientes todas las demás vías razonables para verificar la conformidad, y previa solicitud motivada, evaluar la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2. Dicho acceso estará sujeto al Derecho de la Unión vigente relativo a la protección de la propiedad intelectual e industrial y los secretos comerciales.

4. Dokumentazio teknikoaren kontrola

4.1. Aipatutako eskaeraz gain —3. puntuan dago aipatuta—, hornitzaileak beste eskaera bat aurkeztuko dio berak hautatutako organismo jakinarazari, hornitzaileak merkatuan jarri edo zerbitzuan ipini nahi duen eta 3. puntuan aipatutako kalitatea kudeatzeko sistema aplikatzen zaion AA-sistemari buruzko dokumentazio teknikoa ebaluatu dezan.

4.2. Datu hauek jasoko dira eskaeran:

- a) Hornitzailearen izena eta helbidea.
- b) Hau dioen idatzizko adierazpen bat: ez zaiola eskaera bera aurkeztu beste organismo jakinarazi bati.
- c) IV. eranskinean aurreikusitako dokumentazio teknikoa.

4.3. Organismo jakinaraziak dokumentazio teknikoa aztertuko du. Hala dagokionean, eta bere zereginak betetzeko beharrezkoa den heinean, organismo jakinarazari sarbide osoa emango zaio erabili diren entrenamendu-, balioztatze- eta proba-datuen multzoetara, eta, hala dagokionean eta segurtasun-bermeei lotuta, APIaren edo urrutitik sartzea ahalbidetzen duten beste tresna eta bitarteko tekniko egoki batzuen bidez.

4.4. Dokumentazio teknikoa aztertzean, hornitzaileak frogagiri gehiago eman ditzala edo proba gehigarriak egin ditzala eskatu ahal izango du organismo jakinaraziak, behar bezala ebaluatu ahal izateko AA-sistema bat datorren III. kapituluko 2. atalean ezarritako betekizunekin. Organismo jakinaraziak uste badu hornitzaileak egindako probak ez direla nahikoak, berak egingo ditu proba egokiak, dagokionaren arabera.

4.5. Era berean, organismo jakinarazari sarbidea emango zaio AA-sistemaren entrenamendu-eredura eta eredu entrenatura, dagozkien parametroekin, ebaluatu ahal izan dezan, behar izanez gero, adostasuna egiaztatzeko gainerako arrazoizko bide guztiak agortu eta nahikoak ez direla frogatu ondoren, eta arrazoituta eskatuz gero, ea arrisku handiko AA-sistema bat datorren III. kapituluko 2. atalean ezarritako betekizunekin. Jabetza intelektuala eta industrial eta merkataritza-sekretuak babesteari buruz indarrean dagoen Batasuneko zuzenbidearen arabera da sarbide hori.



4.6. Se notificará la decisión del organismo notificado al proveedor o a su representante autorizado. La notificación incluirá las conclusiones de la evaluación de la documentación técnica y una decisión motivada sobre la evaluación.

Cuando el sistema de IA cumpla los requisitos establecidos en el capítulo III, sección 2, el organismo notificado expedirá un certificado de la Unión de evaluación de la documentación técnica. Dicho certificado indicará el nombre y la dirección del proveedor, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para identificar el sistema de IA.

El certificado y sus anexos contendrán toda la información pertinente para poder evaluar la conformidad del sistema de IA y permitir el control del sistema de IA mientras esté en uso, cuando proceda.

Cuando el sistema de IA no cumpla los requisitos establecidos en el capítulo III, sección 2, el organismo notificado denegará la expedición del certificado de la Unión de evaluación de la documentación técnica e informará de ello al solicitante, motivando detalladamente su decisión.

Cuando el sistema de IA no cumpla los requisitos relativos a los datos utilizados para su entrenamiento, será necesario llevar a cabo un nuevo entrenamiento del sistema antes de solicitar una nueva evaluación de la conformidad. En este caso, la decisión motivada sobre la evaluación del organismo notificado que deniegue la expedición del certificado de la Unión de evaluación de la documentación técnica contendrá consideraciones específicas relativas a la calidad de los datos utilizados para entrenar el sistema de IA, en particular acerca de los motivos del incumplimiento.

4.7. Todo cambio del sistema de IA que pueda afectar a su cumplimiento de los requisitos o su finalidad prevista será evaluado por el organismo notificado que haya expedido el certificado de la Unión de evaluación de la documentación técnica. El proveedor informará a dicho organismo notificado de su intención de introducir cualquiera de los cambios previamente mencionados o de si tiene constancia de que se hayan producido tales cambios. El organismo notificado evaluará los cambios previstos y decidirá si estos requieren una nueva evaluación de la conformidad con arreglo al artículo 43, apartado 4, o si pueden ser objeto de un suplemento al certificado de la Unión de evaluación de la documentación técnica. En este último caso, el organismo notificado evaluará los cambios, notificará su decisión al proveedor y, si aprueba los cambios, expedirá un suplemento al certificado de la Unión de evaluación de la documentación técnica.

4.6. Organismo jakinaraziaren erabakia hornitzaileari edo haren ordezkari baimenduari jakinaraziko zaio. Jakinarazpenean, dokumentazio teknikoaren ebaluazioaren ondorioak eta ebaluazioari buruzko erabaki arrazoitua jasoko dira.

Baldin eta AA-sistemak bete egiten baditu III. kapituluko 2. atalean ezarritako betekizunak, organismo jakinaraziak Batasunaren ziurtagiri bat egingo du dokumentazio teknikoaren ebaluazioari buruz. Datu hauek adieraziko dira ziurtagiri horretan: hornitzailearen izena eta helbidea, azterketaren ondorioak, baliozkotasun-baldintzak (hala badagokio) eta AA-sistema identifikatzeko behar diren datuak.

Ziurtagiriak eta haren eranskinek beharrezko den informazio guztia jasoko dute AA-sistemaren adostasuna ebaluatu eta AA-sistema kontrolatu ahal izateko erabiltzen ari den bitartean, hala dagokionean.

Baldin eta AA-sistemak ez baditu betetzen III. kapituluko 2. atalean ezarritako betekizunak, organismo jakinaraziak uko egingo dio dokumentazio teknikoaren ebaluazioari buruzko Batasunaren ziurtagiria egiteari, eta horren berri emango dio eskatzaileari, erabakia zehatz arrazoituz.

Baldin eta AA-sistemak ez baditu betetzen entrenamendurako erabilitako datuei buruzko betekizunak, sistemaren beste entrenamendu bat egin beharko da adostasuna berriro ebaluatzeko eskatu aurretik. Kasu horretan, organismo jakinaraziak uko egingo dio dokumentazio teknikoaren ebaluazioari buruzko Batasunaren ziurtagiria emateari, horren inguruko erabaki arrazoituak gogoeta espezifikoak jasoko ditu AA-sistema entrenatzeko erabilitako datuen kalitateari buruz, bereziki ez-betetzearen arrazoiei buruz.

4.7. AA-sistema aldatu nahi bada eta aldaketa horrek eragina izan badezake betekizunak betetzeari edo helburu aurreikusiari dagokionez, dokumentazio teknikoa ebaluatzeko Batasunaren ziurtagiria eman duen organismo jakinaraziak ebaluatuko du aldaketa. Hornitzaileak, aurretik aipatutako edozein aldaketa egiteko asmoa badu edo aldaketa horiek gertatu direla jakiten badu, organismo jakinarazi horri jakinaraziko dio. Organismo jakinaraziak aurreikusitako aldaketak ebaluatuko ditu, eta erabakiko du ea berriro ebaluatu behar den haren adostasuna 43.4 artikuluaaren arabera, edo osagarri bat gehitu dakiokeen dokumentazio teknikoa ebaluatzeko Batasunaren ziurtagiriari. Azken kasu horretan, organismo jakinaraziak aldaketak ebaluatuko ditu, bere erabakia hornitzaileari jakinaraziko dio eta, aldaketak onartzen baditu, osagarri bat gehituko dio dokumentazio teknikoa ebaluatzeko Batasunaren ziurtagiriari.



5. Vigilancia del sistema de gestión de la calidad aprobado

5.1. La finalidad de la vigilancia por parte del organismo notificado a que se refiere el punto 3 es asegurarse de que el proveedor cumple debidamente las condiciones del sistema de gestión de la calidad aprobado.

5.2. A efectos de la evaluación, el proveedor dará acceso al organismo notificado a las instalaciones donde se estén diseñando, desarrollando o probando los sistemas de IA. Además, el proveedor facilitará al organismo notificado toda la información necesaria.

5.3. El organismo notificado realizará auditorías periódicas para asegurarse de que el proveedor mantiene y aplica el sistema de gestión de la calidad, y le entregará un informe de la auditoría. En el marco de dichas auditorías, el organismo notificado podrá efectuar más pruebas de los sistemas de IA para los que se hayan expedido certificados de la Unión de evaluación de la documentación técnica.

5. Onartuta dagoen kalitatea kudeatzeko sistema zaintzea

5.1. Hauxe da organismo jakinaraziak 3. puntuan aipatzen den zaintza egitearen helburua: ziurtatzea hornitzaileak behar bezala betetzen dituela onartuta dagoen kalitatea kudeatzeko sistemaren baldintzak.

5.2. Ebaluazioa egiteko, AA-sistemak diseinatzen, garatzen edo probatzen ari diren instalazioetarako sarbidea emango dio hornitzaileak organismo jakinaraziori. Gainera, behar den informazio guztia emango dio hornitzaileak organismo jakinaraziori.

5.3. Organismo jakinaraziak, aldian behin, auditoretzak egingo ditu hornitzaileak kalitatea kudeatzeko sistema mantentzen eta aplikatzen duela ziurtatzeko, eta auditoretza-txostena emango dio. Auditoretza horien esparruan, organismo jakinaraziak AA-sistemen proba gehiago egin ahal izango ditu, baldin eta dokumentazio teknikoa ebaluatzeko Batasunaren ziurtagiriak eman badira horietarako.

ANEXO VIII

Información que debe presentarse para la inscripción en el registro de sistemas de IA de alto riesgo de conformidad con el artículo 49

Sección A — Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 1

Con respecto a los sistemas de IA de alto riesgo que vayan a inscribirse en el registro de conformidad con el artículo 49, apartado 1, se facilitará y se actualizará debidamente la información siguiente:

1. El nombre, la dirección y los datos de contacto del proveedor.
2. Cuando sea otra persona la que presente la información en nombre del proveedor, el nombre, dirección y datos de contacto de dicha persona.
3. El nombre, la dirección y los datos de contacto del representante autorizado, en su caso.
4. El nombre comercial del sistema de IA y toda referencia inequívoca adicional que permita su identificación y trazabilidad.

VIII. ERANSKINA

Arrisku handiko AA-sistemak erregistroan inskribatzeko aurkeztu behar den informazioa, 49. artikulua arabera

A atala — Arrisku handiko AA-sistemen hornitzaileek aurkeztu behar duten informazioa, 49.1 artikulua arabera

Erregistroan 49.1 artikuluari jarraikiz inskribatu behar diren arrisku handiko AA-sistemei dagokienez, informazio hau eman eta behar bezala eguneratuko da:

1. Hornitzailearen izena, helbidea eta harekin harremanetan jartzeko datuak.
2. Hornitzailearen izenean beste pertsona batek aurkezten duenean informazioa, haren izena, helbidea eta harekin harremanetan jartzeko datuak.
3. Hala badagokio, ordezkari baimenduaren izena, helbidea eta harekin harremanetan jartzeko datuak.
4. AA-sistemaren izen komertziala, eta identifikazioa eta trazabilitatea ahalbidetzen duen erreferentzia argi gehigarri oro.



5. La descripción de la finalidad prevista del sistema de IA y de los componentes y funciones que se apoyan a través del mismo.

6. Una descripción sencilla y concisa de la información que utiliza el sistema (datos, entradas) y su lógica de funcionamiento.

7. La situación del sistema de IA (comercializado o puesto en servicio, ha dejado de comercializarse o de estar en servicio, recuperado).

8. El tipo, el número y la fecha de caducidad del certificado expedido por el organismo notificado y el nombre o número de identificación de dicho organismo notificado, cuando proceda.

9. Una copia escaneada del certificado a que se refiere el punto 8, cuando proceda.

10. Todo Estado miembro en el que el sistema de IA se haya introducido en el mercado, puesto en servicio o comercializado en la Unión.

11. Una copia de la declaración UE de conformidad a que se refiere el artículo 47.

12. Las instrucciones de uso electrónicas. No se facilitará esta información en el caso de los sistemas de IA de alto riesgo en los ámbitos de la garantía del cumplimiento del Derecho o la migración, el asilo y la gestión del control fronterizo a que se refiere el anexo III, puntos 1, 6 y 7.

13. Una URL para obtener información adicional (opcional).

Sección B — Información que deben presentar los proveedores de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 2

Con respecto a los sistemas de IA que vayan a inscribirse en el registro de conformidad con el artículo 49, apartado 2, se facilitará y se actualizará debidamente la información siguiente:

1. El nombre, la dirección y los datos de contacto del proveedor.

2. Cuando sea otra persona la que presente la información en nombre del proveedor, el nombre, dirección y datos de contacto de dicha persona.

3. El nombre, la dirección y los datos de contacto del representante autorizado, en su caso.

5. AA-sistemaren, eta haren bidez bermatzen diren osagaien eta eginkizunen helburu aurreikusien deskribapena.

6. Sistemak erabiltzen duen informazioaren (datuak, sarrerak) eta haren funtzionamendu-logikaren deskribapen soil eta zehatza.

7. AA-sistemaren egoera (merkaturatu den edo zerbitzuan ipini den, merkaturatzeari edo zerbitzuan egoteari utzi zaion, berreskuratu den).

8. Organismo jakinaraziak emandako ziurtagiriaren mota, zenbakia eta iraungitze-data, eta organismo jakinarazi horren izena edo identifikazio-zenbakia, hala dagokionean.

9. Hala dagokionean, 8. puntuan aipatzen den ziurtagiriaren kopia eskaneatua.

10. Batasunean zein estatu kidean jarri den merkaturatu, ipini den zerbitzuan edo merkaturatu den AA-sistema, estatu kide guztiak zehaztuz.

11. EB adostasun-adierazpenaren kopia bat, 47. artikuluaaren arabera.

12. Erabilera-jarraibide elektronikoak. Informazio hori ez da emango III. eranskineko 1., 6. eta 7. puntuetan aipatzen diren arrisku handiko AA-sistemen kasuan, hau da, zuzenbidea betearaztearen, migrazioaren, asiloaren eta muga-kontrolaren kudeaketaren eremuetan.

13. Informazio gehigarria lortzeko URL bat (aukerakoa).

B atala — Arrisku handiko AA-sistemen hornitzaileek aurkeztu behar duten informazioa, 49.2 artikuluaaren arabera

Erregistroan 49.2 artikuluari jarraikiz inskribatu behar diren AA-sistemei dagokienez, informazio hau eman eta behar bezala eguneratuko da:

1. Hornitzailearen izena, helbidea eta harekin harremanetan jartzeko datuak.

2. Hornitzailearen izenean beste pertsona batek aurkezten duenean informazioa, haren izena, helbidea eta harekin harremanetan jartzeko datuak.

3. Hala badagokio, ordezkari baimenduaren izena, helbidea eta harekin harremanetan jartzeko datuak.



4. El nombre comercial del sistema de IA y toda referencia inequívoca adicional que permita su identificación y trazabilidad.
5. La descripción de la finalidad prevista del sistema de IA.
6. La condición o condiciones previstas en el artículo 6, apartado 3, con arreglo a las cuales se considera que el sistema de IA no es de alto riesgo.
7. Un breve resumen de los motivos por los que se considera que el sistema de IA no es de alto riesgo en aplicación del procedimiento previsto en el artículo 6, apartado 3.
8. La situación del sistema de IA (comercializado o puesto en servicio, ha dejado de comercializarse o de estar en servicio, recuperado).
9. Todo Estado miembro en el que el sistema de IA se haya introducido en el mercado, puesto en servicio o comercializado en la Unión.

Sección C — Información que deben presentar los responsables del despliegue de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 3

Con respecto a los sistemas de IA de alto riesgo que vayan a inscribirse en el registro de conformidad con el artículo 49, apartado 3, se facilitará y se actualizará debidamente la información siguiente:

1. El nombre, la dirección y los datos de contacto del responsable del despliegue.
2. El nombre, la dirección y los datos de contacto de la persona que presente la información en nombre del responsable del despliegue.
3. La URL de entrada del sistema de IA en la base de datos de la UE por parte de su proveedor.
4. Un resumen de las conclusiones de la evaluación de impacto relativa a los derechos fundamentales realizada de conformidad con el artículo 27.
5. Un resumen de la evaluación de impacto relativa a la protección de datos realizada de conformidad con el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680, tal como se especifica en el artículo 26, apartado 8, del presente Reglamento, cuando proceda.

4. AA-sistemaren izen komertziala, eta identifikazioa eta trazabilitatea ahalbidetzen duen erreferentzia argi gehigarri oro.
5. AA-sistemaren helburu aurrekusiaren deskribapena.
6. AA-sistema arrisku handikotzat ez jotzeko betetzen diren baldintzak —6.3 artikuluan daude aurreikusita—.
7. Azalpen labur bat, adieraziz zergatik uste den AA-sistema ez dela arrisku handikoa, 6.3 artikuluan aurreikusitako prozedura aplikatuz.
8. AA-sistemaren egoera (merkaturatu den edo zerbitzuan ipini den, merkaturatzeari edo zerbitzuan egoteari utzi zaion, berreskuratu den).
9. Batasunean zein estatu kidetan jarri den merkaturatu, ipini den zerbitzuan edo merkaturatu den AA-sistema, estatu kide guztiak zehaztuz.

C atala — Arrisku handiko AA-sistemen hedapenaren arduradunek aurkeztu behar duten informazioa, 49.3 artikulua arabera

Erregistroan 49.3 artikuluari jarraikiz inskribatu behar diren arrisku handiko AA-sistemei dagokienez, informazio hau eman eta behar bezala eguneratuko da:

1. Hedapenaren arduradunaren izena, helbidea eta harekin harremanetan jartzeko datuak.
2. Informazioa hedapenaren arduradunaren izenean aurkeztu duen pertsonaren izena, helbidea eta harekin harremanetan jartzeko datuak.
3. Hornitzaileak AA-sistema EBren datu-basean sartzeko baliatutako URLa.
4. Oinarritzko eskubideen gaineko inpaktuaren ebaluazioan —27. artikulua arabera egina— lortutako ondorioen laburpena.
5. Datuen babesaren gaineko inpaktuaren ebaluazioaren laburpena, (EB) 2016/679 Erregelamenduaren 35. artikulua edo (EB) 2016/680 Zuzentarauaren 27. artikulua arabera egina, erregelamendu honen 26.8 artikuluan zehazten den bezala, hala dagokionean.



ANEXO IX

Información que debe presentarse para la inscripción en el registro de los sistemas de IA de alto riesgo enumerados en el anexo III en relación con las pruebas en condiciones reales de conformidad con el artículo 60

Con respecto a las pruebas en condiciones reales que vayan a inscribirse en el registro de conformidad con el artículo 60, se facilitará y se actualizará debidamente la información siguiente:

1. El número de identificación único para toda la Unión de la prueba en condiciones reales.
2. El nombre y los datos de contacto del proveedor o proveedor potencial y de los responsables del despliegue que participen en la prueba en condiciones reales.
3. Una breve descripción del sistema de IA, su finalidad prevista y demás información necesaria para la identificación del sistema.
4. Un resumen de las principales características del plan de la prueba en condiciones reales.
5. Información sobre la suspensión o la conclusión de la prueba en condiciones reales.

IX. ERANSKINA

III. eranskinean zerrendatutako arrisku handiko AA-sistemak erregistroan inskribatzeko aurkeztu behar den informazioa, baldintza errealeko probei dagokienez —60. artikulua arabera—

Erregistroan 60. artikuluari jarraikiz inskribatu behar diren baldintza errealeko probei dagokienez, informazio hau eman eta behar bezala eguneratuko da:

1. Baldintza errealeko proben Batasun osorako identifikazio-zenbaki bakarra.
2. Baldintza errealeko probetan parte hartzen duten hornitzailearen edo hornitzaile potentzialaren eta hedapenaren arduradunen izena eta haiekin harremanetan jartzeko datuak.
3. AA-sistemaren deskribapen laburra, helburu aurreikusia eta sistema identifikatzeko beharrezkoa den gainerako informazioa.
4. Baldintza errealeko probaren planaren ezaugarri nagusien laburpena.
5. Baldintza errealeko proba eten edo amaitu izanaren inguruko informazioa.

ANEXO X

Actos legislativos de la Unión relativos a sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia

1. Sistema de Información de Schengen
 - a) Reglamento (UE) 2018/1860 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular ([DO L 312 de 7.12.2018, p. 1](#)).
 - b) Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 1987/2006 ([DO L 312 de 7.12.2018, p. 14](#)).

X. ERANSKINA

Magnitude handiko sistema informatikoei buruz Batasunak ezarritako lege-egintzak askatasun-, segurtasun- eta justizia-esparruan

1. Schengengo informazio-sistema
 - a) (EB) 2018/1860 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko azaroaren 28koa, egoera irregularrean dauden hirugarren herrialdeetako nazionalak itzultzeko Schengengo informazio-sistema erabiltzeko buruzkoa ([2018/12/07ko EBAO, L 312, 1. or.](#)).
 - b) (EB) 2018/1861 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko azaroaren 28koa, mugako ikuskapenen eremuko Schengengo informazio-sistemaren (SIS) ezarpenari, funtzionamenduari eta erabilerari buruzkoa, Schengengo Akordioa aplikatzeko hitzarmena aldatzen duena eta (EE) 1987/2006 Erregelamendua aldatzen eta indargabetzen duena ([2018/12/07ko EBAO, L 312, 14. or.](#)).



c) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión ([DO L 312 de 7.12.2018, p. 56](#)).

2. Sistema de Información de Visados

a) Reglamento (UE) 2021/1133 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (UE) n.º 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 y (UE) 2019/818 en lo que respecta al establecimiento de las condiciones para acceder a otros sistemas de información de la UE a efectos del Sistema de Información de Visados ([DO L 248 de 13.7.2021, p. 1](#)).

b) Reglamento (UE) 2021/1134 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se modifican los Reglamentos (CE) n.º 767/2008, (CE) n.º 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 y (UE) 2019/1896 del Parlamento Europeo y del Consejo y por el que se derogan las Decisiones 2004/512/CE y 2008/633/JAI del Consejo, a fin de reformar el Sistema de Información de Visados ([DO L 248 de 13.7.2021, p. 11](#)).

3. Eurodac

a) Reglamento (UE) 2024/1358 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la creación del sistema «Eurodac» para la comparación de datos biométricos a efectos de la aplicación efectiva de los Reglamentos (UE) 2024/1315 y (UE) 2024/1350 del Parlamento Europeo y del Consejo y de la Directiva 2001/55/CE del Consejo y de la identificación de nacionales de terceros países y apátridas en situación irregular, y sobre las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de garantía de cumplimiento del Derecho, por el que se modifican los Reglamentos (UE) 2018/1240 y (UE) 2019/818 del Parlamento Europeo y del Consejo y se deroga el Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo ([DO L, 2024/1358, 22.5.2024, ELI: <http://data.europa.eu/eli/reg/2024/1358/oj>](#)).

c) (EB) 2018/1862 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko azaroaren 28koa, polizia-lankidetzaren eta zigor-arloko lankidetzaren eremuko Schengengo informazio-sistemaren (SIS) ezarpenari, funtzionamenduari eta erabilerari buruzkoa, Kontseiluaren 2007/533/JAI Erabakia aldatzen eta indargabetzen duena eta Europako Parlamentuaren eta Kontseiluaren (EE) 1986/2006 Erregelamendua eta Batzordearen 2010/261/EB Erabakia indargabetzen dituen ([2018/12/07ko EBAO, L 312, 56. or.](#)).

2. Bisen informazio-sistema

a) (EB) 2021/1133 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2021eko uztailaren 7koa, (EB) 603/2013, (EB) 2016/794, (EB) 2018/1862, (EB) 2019/816 eta (EB) 2019/818 erregelamenduak aldatzen dituen bisen informazio-sistemaren ondorioetarako EBko beste informazio-sistema batzuetara sartzeko baldintzak ezartzeari dagokionez ([2021/07/13ko EBAO, L 248, 1. or.](#)).

b) (EB) 2021/1134 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2021eko uztailaren 7koa, Europako Parlamentuaren eta Kontseiluaren (EE) 767/2008, (EE) 810/2009, (EB) 2016/399, (EB) 2017/2226, (EB) 2018/1240, (EB) 2018/1860, (EB) 2018/1861, (EB) 2019/817 eta (EB) 2019/1896 erregelamenduak aldatzen dituen eta Kontseiluaren 2004/512/EE eta 2008/633/JAI erabakiak indargabetzen dituen bisen informazio-sistema erreformatzeko ([2021/07/13ko EBAO, L 248, 11. or.](#)).

3. Eurodac

a) (EB) 2024/1358 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2024ko maiatzaren 14koa, datu biometrikoak konparatzeko «Eurodac» sistema sortzei buruzkoa, Europako Parlamentuaren eta Kontseiluaren (EB) 2024/1315 eta (EB) 2024/1350 erregelamenduak eta Kontseiluaren 2001/55/EE Zuzentaraua eraginkortasunez aplikatzeko, eta egoera irregularrean dauden hirugarren herrialdeetako nazionalak eta aberriak identifikatzeko, eta estatu kideetako segurtasun-zerbitzuek eta Europolek aurkeztutako Eurodac-eko datuekin konparatzeko eskaerei buruzkoa, zuzenbidea betetzeko, Europako Parlamentuaren eta Kontseiluaren (EB) 2018/1240 eta (EB) 2019/818 erregelamenduak aldatzen dituen eta Europako Parlamentuaren eta Kontseiluaren (EB) 603/2013 Erregelamendua indargabetzen duena ([2024/05/22ko EBAO, L, 2024/1358, ELI: <http://data.europa.eu/eli/reg/2024/1358/oj>](#)).



4. Sistema de Entradas y Salidas

a) Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n.º 767/2008 y (UE) n.º 1077/2011 ([DO L 327 de 9.12.2017, p. 20](#)).

5. Sistema Europeo de Información y Autorización de Viajes

a) Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establece un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226 ([DO L 236 de 19.9.2018, p. 1](#)).

b) Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV) ([DO L 236 de 19.9.2018, p. 72](#)).

6. Sistema Europeo de Información de Antecedentes Penales en relación con los nacionales de terceros países y apátridas

Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN) a fin de complementar el Sistema Europeo de Información de Antecedentes Penales, y por el que se modifica el Reglamento (UE) 2018/1726 ([DO L 135 de 22.5.2019, p. 1](#)).

7. Interoperabilidad

a) Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo, y las

4. Sarrera-irteeren sistema

a) (EB) 2017/2226 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2017ko azaroaren 30ekoa, sarrera-irteeren sistema bat ezartzen duena estatu kideetako kanpo-mugak zeharkatzen dituzten hirugarren herrialdeetako herritarrei dagozkien sarrera-eta irteera-datuak eta sarrera-ukapeneko datuak erregistratzeko, sistema horretara polizia-helburuekin sartzeko baldintzak ezartzen dituena eta Schengengo Akordioa aplikatzeko hitzarmena eta (EE) 767/2008 eta (EB) 1077/2011 erregelamenduak aldatzen dituena ([2017/12/09ko EBAO, L 327, 20. or.](#)).

5. Bidaien informazio eta baimenen Europako sistema

a) (EB) 2018/1240 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko irailaren 12koa, bidaien informazio eta baimenen Europako sistema ezartzen duena eta (EB) 1077/2011, (EB) 515/2014, (EB) 2016/399, (EB) 2016/1624 eta (EB) 2017/2226 erregelamenduak aldatzen dituena ([2018/09/19ko EBAO, L 236, 1. or.](#)).

b) (EB) 2018/1241 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2018ko irailaren 12koa, (EB) 2016/794 Erregelamendua aldatzen duena bidaien informazio eta baimenen Europako sistema ezartzeko ([2018/09/19ko EBAO, L 236, 72. or.](#)).

6. Hirugarren herrialdeetako nazionalen eta aberrigabeen aurrekari penalei buruzko Europako informazio-sistema

(EB) 2019/816 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko apirilaren 17koa, hirugarren herrialdeetako nazionalen eta aberrigabeen kondenei buruzko informazioa duten estatu kideak identifikatzeko sistema zentralizatu bat ezartzen duena, aurrekari penalei buruzko Europako informazio-sistema osatzeko, eta (EB) 2018/1726 Erregelamendua aldatzen duena ([2019/05/22ko EBAO, L 135, 1. or.](#)).

7. Elkarrengarritasuna

a) (EB) 2019/817 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko maiatzaren 20koa, EBko informazio-sistemen elkarrengarritasunerako esparru bat ezartzen duena mugen eta bisen eremuan eta Europako Parlamentuaren eta Kontseiluaren (EE) 767/2008, (EB) 2016/399, (EB) 2017/2226, (EB) 2018/1240, (EB) 2018/1726 eta (EB) 2018/1861 erregelamenduak eta



Decisiones 2004/512/CE y 2008/633/JAI del Consejo ([DO L 135 de 22.5.2019, p. 27](#)).

b) Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativo al establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 ([DO L 135 de 22.5.2019, p. 85](#)).

Kontseiluaren 2004/512/EE eta 2008/633/JAI erabakiak aldatzen dituenak ([2019/05/22ko EBAO, L 135, 27. or.](#)).

b) (EB) 2019/818 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2019ko maiatzaren 20koa, EBko informazio-sistemen elkarrengarritasunerako esparru bat ezartzen duena polizia-lankidetzaren, lankidetzak judizialaren, asiloaren eta migrazioaren eremuan eta (EB) 2018/1726, (EB) 2018/1862 eta (EB) 2019/816 erregelamenduak aldatzen dituenak ([2019/05/22ko EBAO, L 135, 85. or.](#)).

ANEXO XI

Documentación técnica a que se refiere el artículo 53, apartado 1, letra a) — documentación técnica para proveedores de modelos de IA de uso general

Sección 1

Información que deben presentar los proveedores de modelos de IA de uso general

La documentación técnica a que se refiere el artículo 53, apartado 1, letra a), incluirá como mínimo la siguiente información en función del tamaño y perfil de riesgo del modelo:

1. Una descripción general del modelo de IA de uso general que incluya:

a) las tareas que el modelo vaya a realizar y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;

b) las políticas de usos aceptables aplicables;

c) la fecha de lanzamiento y los métodos de distribución;

d) la arquitectura y el número de parámetros;

e) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;

f) la licencia.

2. Una descripción detallada de los elementos del modelo a que se refiere el punto 1 e información pertinente sobre el proceso de desarrollo que incluya los siguientes elementos:

XI. ERANSKINA

53.1.a) artikuluan aipatutako dokumentazio teknikoak — Erabilera orokorreko AA-ereduen hornitzaileentzako dokumentazio teknikoak

1. atala

Erabilera orokorreko AA-ereduen hornitzaileek aurkeztu behar duten informazioa

Erregelamendu honen 53.1.a) artikuluan aipatzen den dokumentazio teknikoak informazio hau jasoko du, gutxienez, ereduaren tamainaren eta arrisku-profilaren arabera:

1. Erabilera orokorreko AA-ereduaren deskribapen orokorra; datu hauek jasoko ditu:

a) zer-nolako lanak egingo dituen ereduak eta nolako AA-sistemetan integratu ahal izango den —mota eta izaera—;

b) aplikatzekoak diren erabilera onargarrien politikak;

c) zein egunetan atera den eta nola banatu den;

d) arkitektura eta parametro-kopurua;

e) sarrera-irteeren modalitatea (adibidez, testua, irudia) eta formatua;

f) lizentzia.

2. Eranskin honen 1. puntuan aipatzen den ereduaren elementuen deskribapen zehatza eta garapen-prozesuari buruz beharrezko den informazioa; elementu hauek jasoko ditu:



a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para integrar el modelo de IA de uso general en los sistemas de IA;

b) las especificaciones de diseño del modelo y el proceso de entrenamiento, incluidos los métodos y las técnicas de entrenamiento, las decisiones clave de diseño, incluidas la justificación lógica y los supuestos de los que se ha partido; aquello que el modelo está diseñado para optimizar y la pertinencia de los diversos parámetros, según proceda;

c) información sobre los datos utilizados para el entrenamiento, las pruebas y la validación, cuando proceda, incluidos el tipo y la procedencia de los datos y los métodos de gestión (por ejemplo, limpieza, filtrado, etc.), el número de puntos de datos, su alcance y sus principales características; cómo se obtuvieron y seleccionaron los datos, así como cualquier otra medida que permita detectar que las fuentes de datos no son idóneas y los métodos para detectar sesgos identificables, cuando proceda;

d) los recursos computacionales utilizados para entrenar el modelo (por ejemplo, número de operaciones de coma flotante, el tiempo de entrenamiento y otros detalles pertinentes relacionados con el mismo;

e) el consumo de energía conocido o estimado del modelo.

A propósito de la letra e), cuando se desconozca el consumo de energía del modelo, podrá hacerse una estimación del consumo de energía a partir de la información relativa a los recursos computacionales utilizados.

Sección 2

Información adicional que deben presentar los proveedores de modelos de IA de uso general con riesgo sistémico

1. Una descripción detallada de las estrategias de evaluación, con los resultados de la misma, sobre la base de los protocolos y herramientas de evaluación públicos disponibles o de otros métodos de evaluación. Las estrategias de evaluación incluirán los criterios de evaluación, los parámetros y el método de detección de limitaciones.

2. Cuando proceda, una descripción detallada de las medidas adoptadas para realizar pruebas adversarias internas o externas (por ejemplo, utilización

a) Zer baliabide tekniko behar den (adibidez, erabilera-jarraibideak, azpiegitura, tresnak) erabilera orokorreko AA-eredua AA-sistemetan integratzeko;

b) Eredua diseinatzeko zehaztapenak eta entrenamendu-prozesua —entrenamendu-metodoak eta -teknikak barne—, diseinuaren funtsezko erabakiak —justifikazio logikoa eta abiapuntuko kasuak barne—; eredua zer optimizatzeko diseinatu den eta parametro ezberdinen egokitasuna, dagokionaren arabera;

c) Entrenamendurako, probetarako eta balioztatze erabili diren datuei buruzko informazioa, hala dagokionean, datu hauek adierazita: datuen mota eta jatorria, eta horiek kudeatzeko metodoak (adibidez, garbiketa, iragazketa, etab.); datu-puntuen kopurua, irismena eta ezaugarri nagusiak; datuak lortzeko eta hautatzeko modua, datu-iturriak egokiak ez direla detektatzea ahalbidetzen duen beste edozein neurri eta, hala badagokio, alborapen identifikagarriak detektatzeko metodoak;

d) Eredua entrenatzeko erabili diren baliabide konputazionalak (adibidez, koma mugikorrek eragiketa-kopurua), entrenamendu-denbora eta horrekin lotutako beste xehetasun batzuk;

e) Ereduren energia-kontsumo ezaguna edo zenbatetsia.

e) letrari dagokionez, ereduren energia-kontsumoa ezagutzen ez denean, erabilitako baliabide konputazionalak buruzko informazioan oinarrituta egin ahal izango da energia-kontsumoaren zenbatespena.

2. atala

Arrisku sistemikoa dakarten erabilera orokorreko AA-ereduen hornitzaileek aurkeztu behar duten informazio gehigarria

1. Ebaluazio-estrategien deskribapen zehatza, emaitzak adierazita, eskura dauden ebaluazio-protokolo eta -tresna publikoetan edo beste ebaluazio-metodo batzuetan oinarrituta. Ebaluazio-estrategien artean, ebaluazio-irizpideak, parametroak eta mugak hautemateko metodoa jasoko dira.

2. Hala dagokionean, deskribapen zehatz bat barneko edo kanpoko aurkaritza-probak egiteko hartutako neurriei buruz (adibidez, «ekipo gorriak»



de «equipos rojos») y adaptaciones de los modelos, incluida su alineación y puesta a punto.

3. Cuando proceda, una descripción detallada de la arquitectura del sistema, con una explicación de la manera en que se incorporan o enriquecen mutuamente los componentes del software y de la manera en que se integran en el procesamiento general.

erabiltzea) eta ereduaren egokitzapenei buruz, lerrokatzea eta doikuntza barne.

3. Hala dagokionean, sistemaren arkitekturaren deskribapen zehatza, behar bezala azalduz nola txertatzen edo aberasten diren softwarearen osagaiak elkarren artean eta nola integratzen diren prozesamendu orokorrean.

ANEXO XII

Información sobre transparencia a que se refiere el artículo 53, apartado 1, letra b) — documentación técnica de los proveedores de modelos de IA de uso general para los proveedores posteriores que integren el modelo en su sistema de IA

La información a que se refiere el artículo 53, apartado 1, letra b), incluirá como mínimo la siguiente información:

1. Una descripción general del modelo de IA de uso general que incluya:
 - a) las tareas que el modelo vaya a realizar y el tipo y la naturaleza de los sistemas de IA en los que puede integrarse;
 - b) las políticas de usos aceptables aplicables;
 - c) la fecha de lanzamiento y los métodos de distribución;
 - d) la manera en que el modelo interactúa o puede utilizarse para interactuar con el hardware o el software que no formen parte del propio modelo, cuando proceda;
 - e) las versiones del software pertinente relacionadas con el uso del modelo de IA de uso general, cuando proceda;
 - f) la arquitectura y el número de parámetros;
 - g) la modalidad (por ejemplo, texto, imagen) y el formato de las entradas y salidas;
 - h) la licencia del modelo.
2. Una descripción de los elementos del modelo y de su proceso de desarrollo, incluidos:

XII. ERANSKINA

53.1.b) artikuluan aipatzen den gardentasunari buruzko informazioa — Erabilera orokorreko AA-ereduen hornitzaileek eredia haien AA-sisteman integratuko duten ondorengo hornitzaileentzat aurkeztu behar duten dokumentazio teknikoa

Erregelamendu honen 53.1.b) artikuluan aipatzen den informazioak informazio hau jasoko du, gutxienez:

1. Erabilera orokorreko AA-ereduaren deskribapen orokorra; datu hauek jasoko ditu:
 - a) zer-nolako lanak egingo dituen ereduak eta nolako AA-sistemetan integratu ahal izango den —mota eta izaera—;
 - b) aplikatzekoak diren erabilera onargarrien politikak;
 - c) zein egunetan atera den eta nola banatu den;
 - d) ereduak nola elkarreragiten duen edo nola erabil daitekeen ereduaren parte ez diren hardwarearekin edo softwarearekin elkarreragiteko, hala dagokionean;
 - e) erabilera orokorreko AA-ereduaren erabilerarekin lotutako softwarearen bertsioak, hala dagokionean;
 - f) arkitektura eta parametro-kopurua;
 - g) sarrera-irteeren modalitatea (adibidez, testua, irudia) eta formatua;
 - h) ereduaren lizentzia.
2. Ereduko elementuen eta horien garapen-prozesuaren deskribapena; datu hauek jasoko ditu:



a) los medios técnicos (por ejemplo, instrucciones de uso, infraestructura, herramientas) necesarios para integrar el modelo de IA de uso general en los sistemas de IA;

b) la modalidad (por ejemplo, texto, imagen, etc.) y el formato de las entradas y salidas y su tamaño máximo (por ejemplo, longitud de la ventana de contexto, etc.);

c) información sobre los datos utilizados para el entrenamiento, las pruebas y la validación, cuando proceda, incluidos el tipo y la procedencia de los datos y los métodos de gestión.

a) Zer baliabide tekniko behar den (adibidez, erabilera-jarraibideak, azpiegitura, tresnak) erabilera orokorreko AA-eredua AA-sistemetan integratzeko;

b) Sarrera-irteeren modalitatea (adibidez, testua, irudia, etab.) eta gehieneko tamaina (adibidez, testuinguru-leihoaren luzera, etab.);

c) Entrenamendurako, probetarako eta balioztatze erabili diren datuei buruzko informazioa, hala dagokionean, datu hauek adierazita: datuen mota eta jatorria, eta horiek kudeatzeko metodoak.

ANEXO XIII

Crterios para la clasificaci3n de los modelos de IA de uso general con riesgo sist3mico a que se refiere el art3culo 51

Con el fin de determinar si un modelo de IA de uso general tiene unas capacidades o unos efectos equivalentes a los contemplados en el art3culo 51, apartado 1, letra a), la Comisi3n tendr3 en cuenta los siguientes criterios:

- a) el n3mero de par3metros del modelo;
- b) la calidad o el tama1o del conjunto de datos, por ejemplo medidos a trav3s de criptofichas;
- c) la cantidad de c3lculo utilizada para entrenar el modelo, medida en operaciones de coma flotante o indicada con una combinaci3n de otras variables, como el coste estimado del entrenamiento, el tiempo estimado necesario o el consumo de energ3a estimado para el mismo;
- d) las modalidades de entrada y salida del modelo, como la conversi3n de texto a texto (grandes modelos de lenguaje), la conversi3n de texto a imagen, la multimodalidad y los umbrales punteros para determinar las capacidades de gran impacto de cada modalidad, y el tipo concreto de entradas y salidas (por ejemplo, secuencias biol3gicas);
- e) los par3metros de referencia y las evaluaciones de las capacidades del modelo, tambi3n teniendo en cuenta el n3mero de tareas sin entrenamiento adicional, la adaptabilidad para aprender tareas nuevas distintas, su nivel de autonom3a y capacidad de ampliaci3n y las herramientas a las que tiene acceso;
- f) si sus repercusiones para el mercado interior son importantes debido a su alcance, lo que se dar3 por

XIII. ERANSKINA

Arrisku sistemikoa dakarten erabilera orokorreko AA-ereduak sailkatzeko irizpideak —51. artikuluan aipatzen dira—

Erabilera orokorreko AA-eredu batek 51.1.a) artikuluan jasotako gaitasunak edo ondorio baliokideak dituen zehazteko, irizpide hauek hartuko ditu kontuan Batzordeak:

- a) ereduaren parametro-kopurua;
- b) datuen multzoaren kalitatea edo tamaina, adibidez kriptofitxen bidez neurtuta;
- c) eredia entrenatzeko erabili den kalkulu-kopurua, koma mugikorrek eragiketetan neurtua edo beste aldagai batzuen konbinazio baten bidez adierazia, hala nola entrenamenduaren kostu zenbatetsia, behar den gutxi gorabeherako denbora edo horretarako zenbatetsitako energia-kontsumoa;
- d) ereduaren sarrera- eta irteera-modalitateak, hala nola testua testu bihurtzea (lengoaia-eredu handiak), testua irudi bihurtzea, multimodalitatea eta modalitate bakoitzaren inpaktu handiko gaitasunak zehazteko puntako atalaseak, eta sarrera- eta irteera-mota zehatza (adibidez, sekuentzia biologikoak);
- e) ereduaren gaitasunen erreferentzia-parametroak eta ebaluazioak, kontuan hartuta, halaber, entrenamendu gehigarririk gabeko ariketa-kopurua, zeregin berri desberdinak ikasteko moldagarritasuna, autonomia-maila eta zabaltzeko gaitasuna, eta eskura dituen tresnak;
- f) barne-merkatuan izango dituen ondorioak ea garrantzitsuak izango diren irismenagatik; garrantzitsuak



supuesto cuando se haya puesto a disposición de al menos 10 000 usuarios profesionales registrados establecidos en la Unión;

g) el número de usuarios finales registrados.

ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>

ISSN 1977-0685 (electronic edition)

izango direla ulertuko da Batasunean ezarrita dauden erregistratutako gutxienez 10.000 erabiltzaile profesionalen esku jarri denean;

g) erregistratutako azken erabiltzaileen kopurua.

ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>

ISSN 1977-0685 (electronic edition)